29/04/15

NOTA DE FUTURO 2015

INTERNET DE LAS COSAS

CENTRO DE ANÁLISIS Y PROSPECTIVA
GABINETE TÉCNICO DE LA GUARDIA CIVIL

INTERNET DE LAS COSAS

PRIVACIDAD Y SEGURIDAD EN UN MUNDO CONECTADO

El Internet de las Cosas (IoT) se refiere a la capacidad de los objetos cotidianos para conectarse a Internet y enviar y recibir datos. Incluye, por ejemplo, las cámaras conectadas a Internet que permiten publicar fotos en línea con un solo clic; o las pulseras que comparten con tus amigos lo lejos que has andado en bicicleta o has corrido durante el día.

Hace seis años, por primera vez, el número de "cosas" conectadas a Internet superó al número de personas. Sin embargo todavía estamos en el comienzo de esta tendencia tecnológica. Los expertos estiman que a partir de este año habrá 25.000 millones de dispositivos conectados y, en 2020, 50.000 millones.

FTC Staff Report

JANUARY 2015

Ante estos hechos, la Comisión Federal de Comercio (FCT) organizó un taller, el pasado 19 de noviembre de 2013, titulado *El Internet de las Cosas: Privacidad y seguridad en un mundo conectado*. Este informe resume el taller citado y ofrece recomendaciones en este área.

En consonancia con la misión de la FTC para proteger a los consumidores en el ámbito comercial, nuestro debate se limita a los dispositivos IoT que son vendidos o utilizados por los consumidores. En consecuencia, el informe no habla de dispositivos vendidos en un contexto de negocio a negocio, ni se ocupa de las comunicaciones máquina a máquina más amplias, que permiten a las empresas realizar un seguimiento de inventario, funcionalidad o eficiencia.

Beneficios y riesgos

Los participantes en el taller hablaron sobre los beneficios y riesgos asociados al IoT. En cuanto a los beneficios, proporcionaron numerosos ejemplos, muchos de los cuales ya están en uso:

- En el campo de la salud, los dispositivos médicos conectados pueden permitir a los consumidores con problemas médicos graves trabajar con sus médicos para tratar sus enfermedades.

- En el hogar, los medidores inteligentes pueden permitir a los proveedores de energía analizar su uso por parte de los consumidores e identificar problemas con electrodomésticos, por ejemplo, además de permitir que estos consumidores sean más conscientes con el uso de la energía.

- En la carretera, los sensores de un coche pueden notificar a los conductores las condiciones peligrosas de un determinado tramo y las actualizaciones de software pueden realizarse de forma inalámbrica, obviando la necesidad de los consumidores de visitar el concesionario.

En general, los participantes coincidieron en que el IoT ofrecerá numerosos y revolucionarios beneficios para los consumidores.

En cuanto a los riesgos, los participantes señalaron que el IoT presenta una variedad de riesgos de seguridad potenciales que podrían ser explotados para perjudicar a los consumidores, como por ejemplo:

- El acceso no autorizado y el uso indebido de la información personal.
- La facilitación de ataques a otros sistemas.
- La creación de riesgos para la seguridad personal.

También indicaron que los riesgos de privacidad pueden fluir desde la recogida de datos personales, hábitos, lugares y las condiciones físicas en el tiempo. En particular, algunos comentaron que las empresas pueden utilizar estos datos para tomar decisiones de crédito, de seguros y de empleo.

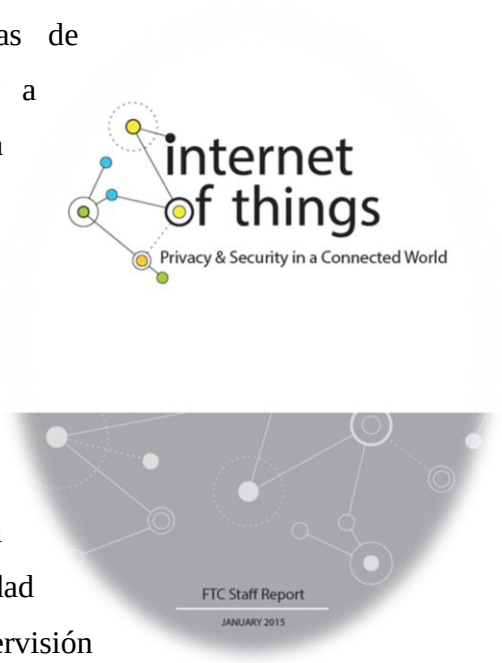
Además, los integrantes del taller reflexionaron sobre cómo los Principios de Buenas Prácticas de la Información (FIPPs), que incluyen máximas tales como avisos, alternativas, acceso, precisión, minimización de los datos, seguridad y rendición de cuentas, son de aplicación al espacio IoT. Los principales debates se centraron en cuatro FIPPs en particular: la seguridad, la minimización de los datos, el aviso y la elección. Igualmente se abordó el tema de cómo los enfoques basados en el uso podrían ayudar a proteger la privacidad del consumidor.

Seguridad

No parece haber un acuerdo generalizado sobre el hecho de que las empresas que desarrollan productos IoT deban implementar una seguridad razonable. Por supuesto, lo que constituye una garantía acertada para un dispositivo determinado dependerá de una serie de factores, incluyendo la cantidad y la sensibilidad de los datos recogidos y los costes de la reparación de las vulnerabilidades de seguridad. El personal de la FCT anima a las empresas a considerar la adopción de las mejores prácticas destacadas por los participantes del taller, incluyendo las que se describen a continuación:

- ***Primero.*** Las empresas deberían crear seguridad en sus dispositivos desde el principio y no como una ocurrencia tardía. Como parte de la garantía con el proceso de diseño, las compañías tendrían que realizar una evaluación de la privacidad o del riesgo para la seguridad; reducir al mínimo los datos que recogen y conservan; y hacer pruebas de sus medidas de seguridad antes de lanzar sus productos.

- ***Segundo.*** Con respecto a las prácticas de personal, las empresas deberían formar a todos los empleados en una buena política de seguridad y asegurarse de que los problemas de seguridad se abordan en el nivel apropiado de responsabilidad dentro de la organización.



- ***Tercero***. Las empresas deberían retener los proveedores de servicios que son capaces de mantener una seguridad considerable y proporcionarles una supervisión razonable.

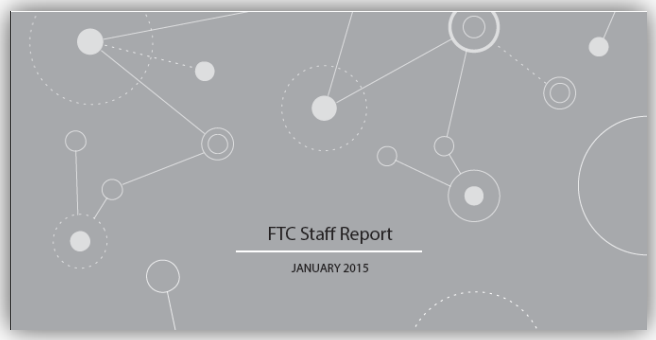
- ***Cuarto.*** Cuando las empresas identifiquen riesgos significativos dentro de sus sistemas deberían aplicar un enfoque de defensa en profundidad, considerando la implementación de las medidas de seguridad en varios niveles.

- ***Quinto.*** Las empresas deberían contemplar la implementación de medidas de control de acceso razonables para limitar la capacidad de una persona no autorizada a acceder a los dispositivos, los datos de un consumidor o, incluso, a la red de consumidores.

- ***Sexto.*** Las empresas tendrían que continuar monitoreando productos y, en la medida de lo posible, arreglar las vulnerabilidades conocidas.

Minimización de datos

La minimización de datos se refiere a la idea de que las empresas deben limitar los datos que recogen y retienen y disponer de ellos cuando ya no los necesiten. Aunque algunos participantes expresaron su preocupación por que la exigencia de minimización de los datos podría limitar sus usos innovadores, en este sentido el personal estuvo de acuerdo con los participantes que afirmaron que las empresas deberían considerar razonablemente la limitación de su recolección y conservación de los datos de consumo.



La minimización de datos puede ayudar a proteger contra dos riesgos relacionados con la privacidad. En primer lugar, los almacenes de datos más grandes presentan un objetivo más atractivo para los ladrones de datos, tanto fuera como dentro de la empresa, y aumenta el daño potencial para los consumidores de tal evento. En segundo lugar, si una empresa recoge y retiene grandes cantidades de datos, existe un mayor riesgo de que sean utilizados de una forma que se aparte de las expectativas razonables de los consumidores.

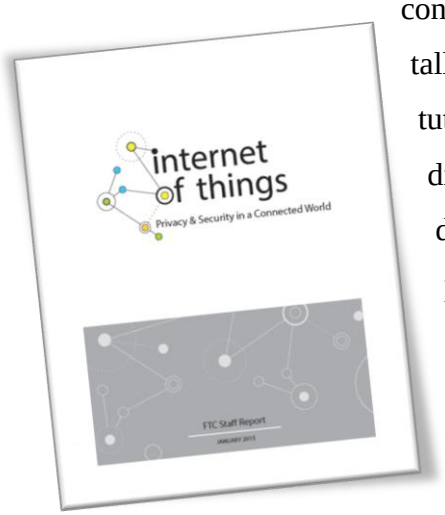
Para minimizar estos riesgos, las empresas deberían examinar sus prácticas de datos y necesidades de negocio, así como desarrollar políticas y prácticas que impongan límites razonables a la recogida y conservación de los datos de consumo. Sin embargo, se reconoce la necesidad de equilibrar el futuro y los usos beneficiosos de los datos con protección de la privacidad. La recomendación del personal en la minimización de los datos es un uso flexible que ofrece a las empresas muchas opciones. Estas pueden decidir no recoger datos; recoger solo los campos de datos necesarios en el producto o servicio que se ofrece; recopilar datos que son menos sensibles; o identificar los datos que recogen. Si una empresa determina que ninguna de estas opciones va a cumplir sus objetivos de negocio, se puede solicitar el consentimiento de los consumidores para la recogida de categorías adicionales inesperadas de datos, tal como se explica a continuación.

Notificación y opción

El personal de la FCT considera que la opción de los consumidores sigue desempeñando un papel importante en el IoT. Algunos participantes sugirieron que la oferta de notificación y opción es un reto en el IoT debido a la ubicuidad de la recopilación de datos y los obstáculos prácticos para el suministro de información sin una interfaz de usuario. Sin embargo, el personal cree que la provisión de notificación y de opción sigue siendo importante.

Esto no quiere decir que todas las colecciones de datos requieran una opción. La FCT ha reconocido que la provisión de opciones para cada instancia de recolección de datos no es necesaria para proteger la privacidad. En su Informe de Privacidad 2012, recomendado en las mejores prácticas, la FCT señaló que no se debe obligar a las empresas a proporcionar la opción, antes de la recolección y el uso de datos de los consumidores, de las prácticas que sean coherentes con el contexto de una transacción o relación de la empresa con el consumidor. De hecho, debido a que estos usos de datos son generalmente inherentes a las expectativas razonables de los consumidores, el coste para los consumidores y las empresas de dar notificación y opción será probablemente mayor que los beneficios. Este principio se aplica igualmente al Internet de las Cosas.

Asimismo se reconoce la dificultad práctica de proporcionar una opción cuando no hay contacto con el consumidor y también se admite que no hay una talla única para todos. Algunas opciones incluyen el desarrollo de tutoriales en vídeo, la colocación de los códigos QR en los dispositivos y proporcionar opciones en el punto de venta, dentro de asistentes de configuración, o en un tablero de privacidad. Independientemente del enfoque que una empresa decida tomar, las opciones de privacidad que ofrezca deberían ser claras y prominentes. Incluso algunas empresas podrían querer considerar el uso de una combinación de enfoques.



Algunos participantes mostraron su preocupación por que las empresas ofrecieran opciones a los consumidores solo en los casos en que la recopilación o el uso fueran incompatibles con el contexto; un enfoque que podría restringir nuevos usos inesperados de datos con beneficios sociales potenciales. Por eso instaron a que las limitaciones de uso se consideraran como un suplemento a, en lugar de un aviso u opción. Con un enfoque basado en el uso, los legisladores, reguladores, organismos de autorregulación o empresas individuales fijarían como "admisibles" e "inadmisibles" los usos de determinados datos de los consumidores.

Reconociendo la inquietud por que un aviso y el enfoque de la opción pudieran restringir nuevos usos beneficiosos de los datos, el personal ha incorporado algunos elementos del modelo basado en su enfoque. Por ejemplo, la idea de las opciones está acuñada en el contexto que tiene en cuenta cómo se utilizarán los datos: si un uso es coherente con el contexto de la interacción, es decir, si se trata de un uso previsto la empresa no tendría que ofrecer una opción para el consumidor. En cambio, para usos incompatibles con el contexto de la interacción (usos inesperados), las empresas deberían ofrecer opciones claras y evidentes. Así, si una empresa recopila los datos de un consumidor y los identifica de forma inmediata y efectiva no es necesario que ofrezca opciones a los consumidores acerca de esta colección. Además, la FCT protege la privacidad a través de un enfoque basado en el uso, en algunos casos. Por ejemplo, se hace cumplir la Fair Credit Reporting Act (FCRA), una ley que restringe los usos permisibles de información del crédito del consumidor en determinadas circunstancias. La FCT también aplica su autoridad a la injusticia para desafiar ciertos usos nocivos de datos de los consumidores.

El personal se preocupa, sin embargo, acerca de la adopción de un modelo basado en el uso puro del Internet de las Cosas. En primer lugar, porque las limitaciones basadas en el uso no se articulan exhaustivamente en la legislación, las normas o códigos ampliamente adoptados de conducta, no está claro quién decide qué usos adicionales son beneficiosos o perjudiciales. En segundo lugar, porque las limitaciones de uso no abordan por sí solas los riesgos de privacidad y seguridad creados por la recopilación y retención de datos. Por último, un modelo basado en el uso puro del IoT no tendría en cuenta las preocupaciones de los consumidores sobre la recopilación de información sensible.

El establecimiento de marcos legislativos o ampliamente aceptados por las partes interesadas podría abordar potencialmente algunas de estas preocupaciones. Por ejemplo, un marco podría establecer los usos permitidos o prohibidos. Ante la falta de consenso sobre esos marcos, sin embargo, el enfoque establecido aquí (dando a los consumidores la información y decisiones sobre sus datos) sigue siendo el más viable para el IoT en un futuro previsible.

Legislación

Los participantes también hablaron de si la legislación sobre el IoT era apropiada, con algunos mostrando su apoyo y otros oponiéndose a la misma. El personal de la FCT está de acuerdo con aquellos que declararon que existe un gran potencial para la innovación en este área y que establecer una legislación específica en esta etapa sería prematuro. También está de acuerdo en que el desarrollo de los programas de autorregulación diseñados para determinadas industrias sería útil como medio para fomentar la adopción de prácticas de privacidad y seguridad.

Sin embargo, a la luz de las continuas amenazas a la seguridad de los datos y el riesgo de que las nuevas tecnologías del Internet de las Cosas pudieran hacer que se incrementasen estas amenazas, la FCT reitera la recomendación de que el Congreso apruebe una legislación federal fuerte, flexible y tecnológicamente neutral, para fortalecer sus herramientas de aplicación de seguridad de datos existentes y para notificar a los consumidores cuando exista un fallo de seguridad. La legislación general de seguridad de datos debería proteger contra el acceso no autorizado a información personal y la funcionalidad del dispositivo en sí. Por ejemplo, si un marcapasos no se asegura correctamente, el problema no es solo que la información de salud pudiera verse comprometida, sino que la persona que lo lleva también podría ser dañada seriamente.

Además, la omnipresencia de la recopilación de información y su uso, que hace posible el IoT, refuerza la necesidad de asentar una serie de normas de privacidad básicas, que la FCT ya recomendó anteriormente en su informe de privacidad de 2012. Aunque la FCT tiene actualmente autoridad para tomar medidas en contra de algunas prácticas relacionadas con el Internet de las Cosas, no puede obligar a adoptar ciertas protecciones básicas de privacidad, como revelaciones de privacidad o de opción de los consumidores, ante la ausencia de pruebas específicas de engaño o falta de equidad. El personal de la FCT recomienda por tanto, una vez más, que el Congreso promulgue una base amplia en la legislación sobre la privacidad (en oposición a una legislación específica). Esta legislación debería ser flexible y tecnológicamente neutral, que también proporcione reglas claras para las empresas sobre cuestiones tales como la forma de proporcionar opciones a los consumidores acerca de la recopilación de datos y las prácticas de uso.

Mientras tanto, la FCT va a seguir utilizando sus herramientas para garantizar que las empresas del IoT sigan considerando cuestiones de seguridad y privacidad a medida que desarrollan nuevos dispositivos.