Panel I - Smart Data

James Dempsey inicia sus palabras estableciendo que se escucha muchísimo la palabra “smart” en el mundo, smartphones, smart devices, smart grid, smart meters, smart automóviles, y será un término que se oirá de forma creciente en la próxima década en lo que respecta al desarrollo de la tecnología y protección de datos.

Uno de los objetivos principales del panel es introducir al concepto de Smart Data y hablar de diferentes aspectos vinculados con smart data o smart devices o smart networks.

Ken Anderson desarrolla una introducción del video en el cual hablan los Sres. Ann Cavoukian, Comisionada de Ontario y George Tomko, creador de un concepto particular de Smart Data, el que sería inmediatamente proyectado.

Ann Cavoukian sostiene que Smart Data es el concepto de privacidad para el futuro, dejando a los datos o a la información que piense por ella misma y el programa que se adapte siendo el contexto, la clave. La privacidad se trata del contexto, nadie sabe mejor que el propio usuario cómo deben usarse sus datos dependiendo del contexto.

Lo bueno de smart data es la personificación del concepto de Privacy by Design. La razón por la cual Privacy by Design es una herramienta muy efectiva, es que es proactiva, previene y se anticipa a los daños que puedan afectar a la privacidad.

El usuario lleva el control, conoce el contexto, da las instrucciones que se verán reflejadas en el mundo Smart data siendo que está integrada por agentes virtuales que actuarán conforme a las instrucciones que les haya dado el usuario. La data vive en línea y refleja las preferencias de los usuarios en cuanto al uso y la divulgación de los datos personales.

George Tomko comienza definiendo la Smart data como un agente

inteligente basado en web, que sirve de representante del titular de los datos, para asegurar y controlar la emisión y usos de sus datos personales, en función del contexto y las preferencias del interesado.

Es autónomo y aprende de la experiencia, respondiendo correctamente a situaciones nuevas, va a funcionar en un mundo 3-D virtual cuando ésta se convierta en la próxima evolución de la web.

Es una tecnología basada en la Web que permite a la persona interesada estar en completo control de los usos de sus datos personales todo el tiempo.

Comienza con la Fantasía Científica, cada uno tiene información en su cabeza que quiere mantener en privacidad, entonces cada uno de nosotros somos la versión humana de smart data. Ahora, si la imaginación permitiera que fuera posible digitalizar el propio cuerpo y mente en un sistema binario y luego almacenarlo en la nube, y cuando alguien tiene una solicitud acerca de los datos personales de un tercero, se pudiera descargar un sistema binario en una máquina clonadora y que ésta, a su vez, pudiera reconstruir una copia de nosotros, un clon. Dicho clon representaría el interés en cuanto a la privacidad de los datos concernidos. O sea que si alguien le solicita al clon determinada información, el clon solo se la entregará si reunió los criterios adecuados. Pero además, queremos que ese clon de vueltas por ahi, observe lo que se hace con los datos personales, controlar que no se haya hecho nada incorrecto, por ejemplo que hayas mandado datos a personas que no quisiste mandarlos.

Lo anterior parece de ciencia ficción, pero no lo es. En primer lugar, si se sustituye al clon por un agente inteligente, a ese agente se lo llamará Smart Data. Luego, sustituír la máquina de clonación por un procesador, de manera que cuando se descargue la cadena binaria en un dispositivo se configura y activa un agente inteligente de datos.

En cuanto a la seguridad, los datos personales estarán divididos, anónimos, encriptados y ubicados en cajas bloqueadas almacenadas en la nube.

¿Qué va a controlar Smart data? Quién está autorizado a acceder a los datos. ¿Qué pueden hacer con los datos? ¿Cuándo y dónde pueden acceder a los datos?

Stefano Nolfi relata que sin perjuicio de que las personas no proporcionan voluntariamente sus datos personales, la revelación de información ocurre, sin embargo, por varios factores:

Los seres humanos no siempre toman decisiones racionales. Las recompensas a corto plazo hacen que las personas tiendan a aceptar riesgos a largo plazo. Los beneficios del intercambio de información son por lo general mucho más evidentes.

Los comportamientos de protección de la privacidad consumen tiempo y conocimiento.

Falta de conocimiento. El usuario no es consciente de la cantidad de datos personales que se recolecta y la manera en que dichos datos pueden ser analizados.

Falta de alternativas. En muchas ocasiones el usuario está obligado a elegir entre privacidad y seguridad pública, entre privacidad y mejor servicio al cliente, por ejemplo.

Estos factores producen consecuencias negativas no sólo para los usuarios sino tambien para los proveedores de servicios. Para ser efectivos se necesita tecnología para poder eliminar estos factores o las consecuencias de los mismos. La idea es empoderar al usuario con herramientas tecnológicas, en particular con un representante o agente virtual que proteja sus datos personales.

¿Qué funcionalidad debería tener esta tecnología? Permitir a los usuarios adoptar por defecto un comportamiento para proteger la privacidad. Por otra parte, el Agente virtual debe ser capaz de reducir el esfuerzo cognitivo requerido por el usuario para controlar sus datos personales. Y monitorear y proveer retroalimentación pertinente a los usuarios.

¿Cuáles son los desafíos a los que hay que enfrentarse? Generar una interacción entre el agente y el usuario de forma natural y efectiva; transformar conceptos abstractos en operaciones que se pueden automatizar y crearr agentes confiables y competentes capaces de adquirir sus conocimientos mediante la interacción con los usuarios.

Noah Lang propone la siguiente interrogante: ¿Cómo se puede llegar a una "bóveda" de Smart data?

En su oportunidad se intentó con, por ejemplo, Microsoft Passport, y las lecciones aprendidas fueron básicamente que no había confianza del consumidor y ésta debe existir si se desea obtener intercambio de datos, pudiendo obtenerse mediante la demostración de la habilidad de eliminar datos. En aquel momento había falta de escala y no era un negocio auto sustentable.

Afirmó a su vez, que se debe detener la fuga de datos, para que funcione no deben haber datos brutos al descubierto. Esto pasa debido a que por ejemplo: el ecosistema actual de base de datos se basa en la venta de la persona; en el caso los "Documentos públicos" el gobierno recolecta y libera los datos; es posible la identificación del comportamiento en línea del consumidor y de los datos de salud.

Las piezas necesarias son: los datos y hay distintos tipos: datos (ofrecidos, observados y deducidos); penetración y contratos y permisos (la confianza y la centralidad del usuario son la clave).

Existen dos partes que deben comprometerse con la protección de los datos personales: los consumidores y las empresas que realizan tratamiento de datos.

En este sentido, los consumidores deben: contar con acceso rápido a sus datos durante y después de la obtención; tener control demostrado sobre sus datos, corregir, añadir y eliminar sus datos, lo que genera confianza y demostrar un valor monetario legítimo por compartir los datos.

Por otra parte, para conseguir que el sector empresarial participe, se debe reducir la exposición, tener precisión, calidad y oportunidad, abrir o desbloquear nuevas fuentes de datos en la regulación actual y debe existir una participación global masiva de los consumidores.

En relación con cuáles son las claves para impulsar la adopción en ambos sectores, se estableció que éstas remiten a: usuario compartido, el valor del usuario, valor del mercado, facilidad y eficiencia, disminución de los riesgos basados en los costos de hacer negocios y suma positiva no negativa, para todas las partes involucradas.

Finalmente, concluye que para crear un negocio autosustentable se requiere la confianza de los consumidores y contar con una escala a nivel masivo para proporcionar grandes saltos en la inteligencia de los consumidores.

La pregunta es entonces, quién está trabajando en esto ahora, dado que se requieren aplicaciones específicas, como: Open Identity Exchange, Personal Data Ecosystem Consortium, Project VRM, entre otros.

Rainer Knyrim, establece que la idea de un smart meter es muy buena para tener valores remotos diarios pero se plantean las siguientes cuestiones:

Bajo la ley australiana de protección de datos, los datos pueden ser usados si es necesario para el establecimiento, ejercicio o defensa de reclamaciones legales, y si los datos fueron recolectados de forma legítima.

Quién es el controlador, el sistema operador de distribución o el consumidor.

Si originariamente es el sistema operador de distribución, ¿el uso en la Corte, sería un uso legítimo?

El riesgo podría ser que el consumidor pueda obtener una contrademanda o una multa administrativa por haber quebrantado la ley de protección de datos aun habiendo ganado en vía civil.

Podría ser una cuestión del modelo a seguir en el futuro del mercado de redes inteligentes.

Otros posibles riesgos de los Smart meters son: la alta frecuencia y la intensidad de la recolección de los datos de consumo permite sacar conclusiones sobre los hábitos y patrones de comportamiento de las personas viviendo en el mismo lugar. En segundo lugar, el gran interés de personas e instituciones con respecto a esos datos detallados de consumo: propietario (la falta de uso de la vivienda como la razón válida para terminar el contrato), industria publicitaria (segmentación por comportamiento del consumidor), autoridad impositiva (calificación de una residencia como principal o secundaria) e investigaciones penales ("CSI Smart meter").

Concluye brindando recomendaciones estratégicas prácticas, entre las cuales recomienda la lectura del borrador de la regulación de privacidad de la Unión Europea y la Recomendación de la Comisión para la instalación de Smart meters de marzo de 2012.