

Mercadeo Relacional -vs- protección y privacidad de los datos

Si visita la web de Amazon pensando en adquirir un libro online, encontrará en su página de bienvenida sugerencias de otros libros que tal vez sean también de su gusto, inclusive el último lanzamiento de sus autores preferidos, todo gracias a su historial de compras anteriores.

¿Cómo reaccionaría si, al visitar una página web de inversiones, se encontrara con mensajes sugiriendo terapias para un problema de corazón que le ha sido diagnosticado recientemente? Su reacción, probablemente, sería la misma que la de Fran Maier, directora ejecutiva de TrustE, organización sin ánimo de lucro que actúa en defensa de la privacidad online, que describió su experiencia como "escalofriante", cuando tuvo la sensación de que alguien estaba espiando una parte de su vida que debería permanecer en la intimidad.

Maier es directora ejecutiva de TrustE, una organización sin fines de lucro que fija directrices para la preservación de la privacidad online y otorga un sello de aprobación a las empresas que las siguen. Ella fue una de las oradoras presentes en el congreso Supernova, realizado en San Francisco, un evento anual de tecnología organizado por el profesor de Ética empresarial de Wharton, Kevin Werbach, en asociación con la propia Wharton.

Escalofríos

El factor de "escalofrío" es un riesgo inherente al llamado enfoque en el comportamiento. Esa práctica se basa en la actitud de los profesionales de marketing que observan el comportamiento del usuario en Internet elaborando a continuación su perfil según los intereses y el comportamiento del internauta: las webs que visitó, las investigaciones realizadas, los artículos leídos, e incluso los correos escritos y recibidos. Con base a esos datos, el usuario recibe anuncios dirigidos específicamente a él, sin importar por qué webs navegue.

Para los defensores de los consumidores, la recogida de datos online y el seguimiento que se hace de la navegación del usuario han llegado demasiado lejos. Los ejecutivos de marketing responden diciendo que el consumidor se beneficia de una publicidad orientada a sus intereses y afirman que la renuncia que hacen a parte de sus datos personales es un cambio razonable por el acceso gratuito al contenido de Internet, que se sostiene, en gran medida, por la publicidad.

Explorando datos

En el fondo de toda esa preocupación por la privacidad individual está la velocidad con que Internet entró en el día a día de las personas a lo largo de los últimos diez o veinte años. Quince años atrás, la Web era una novedad usada por poca gente. Hoy en día, es utilizada por millones de personas que buscan información, para la adquisición de bienes y servicios e intercambio de ideas en foros de discusiones. El rápido desarrollo de la

tecnología proporcionó a las empresas unas condiciones fantásticas y cada vez mayores de recolectar, almacenar y analizar un número colosal de datos de los consumidores.

"Todo lo que hacemos online crea un historial de transacciones, y todos los datos tienen algún valor", dijo Bruce Schneier, especialista en seguridad muy conocido y director de tecnología de BT Counterpane, proveedora de soluciones de seguridad corporativa. "A medida que el almacenamiento de datos y los costos de procesamiento van haciéndose prácticamente gratuitos, los datos que normalmente borraríamos pasan a ser guardados".

El almacenamiento y la prospección de datos, es decir, el proceso del descubrimiento de correlaciones, o patrones, entre decenas de campos en vastos bancos de datos relacionales permiten la ejecución de expedientes minuciosos de rastreo y de elaboración de perfiles, sea por el gobierno, sea por las empresas, lo que tiene serias implicaciones para la privacidad. Algunos analistas dicen que a los usuarios de Internet, de modo general, no les importa que se haga esa recogida de informaciones y prefieren anuncios que reflejen sus intereses. Dicen también que la preocupación por la cuestión de la privacidad es un problema generacional, ya que los usuarios más jóvenes no se sienten tan incómodos con la recogida de información sobre ellos como los usuarios más mayores.

Schneier y Maier, entre otros, aseguran que la mayor parte de las personas, independientemente de la edad, no tienen ni idea del volumen de información que está siendo recolectada y analizada. Tampoco esas personas se pararon a pensar en las posibles implicaciones negativas de tales actividades como, por ejemplo, la mayor probabilidad de que les persigan en la Web y de que les roben su identidad.

De acuerdo con recientes investigaciones de TrustE, la mayor parte de los consumidores online es consciente, en cierta manera, de que las informaciones online que él busca pueden ser utilizadas para fines publicitarios. Pero no comprenden muy bien lo que es el enfoque en el comportamiento, y no les gusta la idea de que su historial de navegación pueda ser utilizado para el envío de publicidad específica.

Paradójicamente, cerca de dos tercios preferirían encontrarse con publicidad de anunciantes que conocen y en quienes confían, lo que exigiría el seguimiento online de esas personas. De acuerdo con una investigación hecha por la agencia de investigaciones globales TNS, basada en una encuesta realizada con una muestra de 1.015 americanos adultos, la gran mayoría (un 91%) dijo que, si tuviera la oportunidad, utilizaría herramientas online para controlar el seguimiento online de su navegación. Maier dijo que los datos apuntan hacia "una indicación bastante concreta de que el consumidor quiere que encontremos un medio de proporcionarle acceso a anuncios de su interés. Para eso, el enfoque en el comportamiento es uno de los métodos más prometedores. Sin embargo, es preciso que sea transparente en los mínimos detalles, permita hacer elecciones y proporcione valor real".

El equilibrio correcto

Maier y los demás participantes de Supernova reconocieron que tanto el consumidor como el profesional de marketing necesitan llegar al equilibrio correcto entre la recolección de datos y la privacidad del usuario, así como descubrir formas más adecuadas de atender a las necesidades de anunciantes y usuarios.

Se puede tomar como ejemplo el caso de Facebook, la conocida web de relaciones sociales. El año pasado, Facebook lanzó un sistema llamado Beacon, que monitorizaba las compras de los miembros en otras webs y compartía la información con todos los usuarios de su círculo social. Pasado un mes, los usuarios, al sentirse invadidos, obligaron a la web a reconsiderar la iniciativa puesta en práctica sin previo aviso. La empresa se disculpó y lanzó enseguida nuevas opciones de privacidad que exigían el consentimiento del usuario para activar Beacon.

Así como en muchas otras áreas, la posibilidad de monitorizar lo que se pasa en la Web, gracias a la tecnología, supera con creces la capacidad de la sociedad de gestionarla. Las políticas públicas de privacidad actuales se remontan a 1973, cuando el Departamento de Salud, Educación y Bienestar de EEUU fijó directrices básicas para la utilización apropiada de informaciones personales computarizadas como, por ejemplo, la comunicación anticipada a los consumidores sobre la recolecta de datos, la posibilidad de no optar por tal recolecta, acceso a los datos obtenidos y la garantía de que no serán utilizados sin autorización previa del usuario. "¿Tendrá eso sentido en 2008?", se preguntó Maier, observando que tales medidas son insuficientes para el ambiente actual de Internet, en que se recolecta todo en todas partes.

En realidad, dijo Maier que "nuestro concepto de privacidad se basa en la idea de quién es usted. Pero tenemos que pensar ahora también en lo que usted hace. El debate en torno a la privacidad y la estructura básica de la cuestión cambiaron para siempre".

¿Significa esto que necesitamos una ley nacional de privacidad? Las realidades políticas y sociales llevan a muchos analistas a creer que una ley como esa todavía debería tardar en llegar, y que EEUU, probablemente, no seguirá la orientación de los países europeos en lo que concierne a la privacidad online. En Europa, la privacidad es entendida como derecho fundamental, una obligación del Estado para con sus ciudadanos. En EEUU, la privacidad es un derecho individual del consumidor que puede ser intercambiada por un beneficio como, por ejemplo, la utilización gratuita de Internet.

Transparencia frente a simulación

Mientras tanto, no se puede negar el apetito insaciable de las empresas para obtener más y más informaciones sobre los usuarios de Internet, esto porque las posibilidades financieras son muy grandes en ese segmento. Conforme dijo Jonathan Swartz, consejero delegado de Sun Microsystems: "Existe la voluntad de obtener toda información posible del usuario, cada ítem, por menor que sea. Pero es preciso que el usuario sepa qué tipo de información está cosechando. Es preciso ser transparente, la menor simulación puede acabar en desastre".

De acuerdo con Joe Kraus, director de gestión del producto de Google, "la buena privacidad comienza por la utilización de una tecnología que permita la filtración de datos, es decir, una tecnología que posibilite a un tercero tener acceso solamente a aquello que yo quiera que él visite. Tenemos que dar a los usuarios un control mayor sobre el tipo específico de información compartida". Se trata de una medida de enorme importancia, añadió Kraus, "ya que Internet trabaja en conjunto con varios aparatos móviles".

Cuando le preguntaron lo que más le preocupaba, Schneier hizo referencia a la consolidación y a la correlación cruzada de datos por empresas como Choicepoint, y también por agencias del Gobierno. "Hay datos cuya recolecta por el Gobierno es ilegal,

entonces éste se los compra a las empresas y viceversa. Todas esas informaciones se juntan después y pueden ser usadas de maneras inesperadas". (Choicepoint tiene fuerte presencia en la industria de comercio de datos comerciales; en 2005, la empresa informó del robo de datos personales de 145.000 consumidores de su banco de datos).

Maier también dijo que estaba preocupada "con la forma en la que somos monitorizados por Internet, es decir, con base a informaciones específicas. ¿Cuánta de esa información está al alcance del Gobierno?" Ella ve, sin embargo, señales positivas, inclusive tentativas de desarrollar mejores prácticas entre algunas empresas de Internet y una generación más joven y más habituada a usar la Web en beneficio propio.

Como cualquier tecnología, la recolecta de datos online, el procesamiento y el seguimiento tienen fines positivos y negativos, dijo Gerard Lewis, vicepresidente, consultor jurídico y encargado del área de privacidad de Comcast. "El desafío consiste en conseguir el equilibrio justo mediante la fiscalización correcta. Para eso, es preciso que toda la comunidad, todos los que están involucrados en los sectores públicos y privados: consumidores, usuarios, empresas, especialistas en políticas públicas, gobierno, participen en la discusión".