Documento Desordenado – Sociedad Vigilada

# Advertencias sobre una sociedad vigilada

El Relator de Libertad de Expresión de la ONU, Frank La Rue, expresó días atrás que “el derecho a la privacidad es habitualmente entendido como un requisito esencial para la realización del derecho a la libertad de expresión”. Los individuos tienen derecho a mantener buena parte de sus vidas, comunicaciones, pensamientos y movimientos en privado, y si lo desean en forma anónima. El derecho a la privacidad implica además que tenemos derecho a determinar quién tiene información sobre nosotros y cómo se usa.

Las advertencias de la ONU no llegan fuera de tiempo. Son fruto de la masificación de tecnologías de información y vigilancia que, con costos cada vez más bajos, permiten retener datos, monitorear, vigilar y procesar información de los ciudadanos de modos nunca antes vistos. Con la aplicación del sistema Sibios, Argentina entra de lleno en la política de mantener a todos sus ciudadanos vigilados. Para que podamos ejercer nuestros plenos derechos, los Estados deben asegurar que contamos con la libertad de circular, recibir y expresar información, respetando nuestra privacidad. Por eso cualquier avance sobre la privacidad tiene consecuencias sobre la vida, pero aún más sobre el estado de libertad en una democracia.

<http://www.clarin.com/sociedad/Advertencias-sociedad-vigilada_0_926307509.html>

La publicidad necesita libertad de expresión para cumplir sus objetivos. La libertad de expresión es el oxígeno de la comunicación comercial, de su creatividad, de su impacto.

<http://elmundo.com.sv/ix-reunion-conared-2015-el-salvador/>

# Google, ¿lo sabe todo sobre ti?

Muchos de nosotros, no somos conscientes de la cantidad de información que compartimos al conectarnos a internet: Información personal, datos bancarios… Esta información nos es requerida en los procesos de registro de las cuentas que usamos en Internet, por eso es conveniente leer los**términos y condiciones** que se aceptan al crear una nueva cuenta o perfil.

Google sabe más acerca de nuestra vida que nosotros mismos, casi. Debemos tener presente que toda la **información que facilitamos a Google**, queda almacenada en sus servidores. Cuando realizamos búsquedas en Chrome, cuando enviamos mails a través de Gmail, cuando viajamos y utilizamos su servicio Google Maps para orientarnos y llegar a nuestro destino… Toda esa información que tiene sobre ti, es utilizada para ofrecerte publicidad y convertirte en un cliente potencial; ya que sabe todo acerca de ti y tus gustos.

<http://blog.tiendas-jazztel.com/google-lo-sabe-todo-sobre-ti/>

# Google Wants Search to Know What You Know

A revamped search engine might return different results depending on whether you’ve researched a subject before.

Google seems to have developed almost an almost preternatural ability to divine what users are really looking for when they enter a search term. Its engine often returns useful results for even the most egregiously misspelled queries. But Google’s user experience team hopes to give search an additional layer of intelligence—the power to grow with users over time, returning different results depending on whether users are just beginning to investigate a subject or have become old hands.

Google’s user experience team has two branches: designers and researchers. The design group builds the visual experience, and the researchers test it to see if it works, says Dan Russell, lead researcher for the team. Designers come up with possible changes, which the researchers test by inserting them into live search results for selected groups of everyday users and gathering data about their responses.

<http://www.technologyreview.com/news/425244/google-wants-search-to-know-what-you-know/>

# Now Television Advertisers Know You’re Tweeting

If you tweet about a TV show or its ads, don’t be surprised if the advertisers “sponsored tweet” you back.

People love to tweet about television shows they are watching; this much, we know. But now the analytics technologies are producing the payback: televsion advertisers will find out and tweet them back.

This new possibility comes thanks to Twitter having bought the MIT startup Bluefin labs (see “[A Social Media Decoder](http://www.technologyreview.com/featuredstory/425787/a-social-media-decoder/)”). Bluefin measures people’s reaction to specific airings of TV shows and ads, which it tracks and aligns with the tweets it captures. It also keeps track of what individual tweeters are talking about over time.

So don’t be surprised, next time you tweet about a great Super Bowl play, when the Doritos tweet you back. The plan was announced and explained [here](http://advertising.twitter.com/2013/05/Amplify-TV-commercials-on-Twitter-Premiering-TV-ad-targeting.html?m=1), in a Twitter blog written by the Bluefin cofounder Michael Fleischman, who is now a Twitter product manager for revenue.

<http://www.technologyreview.com/view/515371/now-television-advertisers-know-youre-tweeting/>

# Can You Improve Your E-Mails by Analyzing Recipients’ Personalities?

Startup Crystal claims it can help you write better e-mails by mining recipients’ online data for clues to their personality.

The websites and apps we use collect ever-growing mountains of data about us that are being used to tailor all kinds of content to our preferences.

It can be hard to figure out just what to say in an e-mail to someone you don’t know very well. A startup wants to make this easier by correcting messages as you type, suggesting changes that may make the recipient more receptive to what you’re saying. These suggestions are gleaned from data gathered about the recipients online.

[Crystal](https://www.crystalknows.com/), which launched in an invite-only beta in March, attempts to show you the best and worst ways to converse with people, in messages and in person, by scrutinizing publicly available data from LinkedIn, Twitter, blogs, and other online sources.

While Crystal might sound creepy, at its core it’s not all that different from what huge technology companies like Facebook and Netflix already do when mining your user data to figure out what ads to show you or movies to suggest.

“I could see why people are put off at first, as a small segment of people are,” says Crystal creator Drew D’Agostino. “They see it as an invasion of privacy, but it’s just using public data.”

And if it can accurately depict people’s personalities, it could be helpful for interactions ranging from sales and recruiting to dating.

<http://www.technologyreview.com/news/537256/can-you-improve-your-e-mails-by-analyzing-recipients-personalities/>

# AT&T Brings Online Ad Targeting Tactics to TV Commercials

Experiments suggest that monitoring viewer behavior via set-top boxes could help make TV commercials much more effective.

Sophisticated targeting techniques could change viewers’ experiences and TV networks’ bottom lines.

Few cable subscribers realize it, but each time they switch channels, their TV provider makes a note of it. Today, that data is primarily used for internal research and to inform ratings. But newly published work from researchers at AT&T shows how it could also be used to make TV advertising more compelling.

The methods tested by researchers at AT&T Labs in Florham Park, New Jersey, are detailed in a paper that was presented at the [International Conference on Data Mining](http://icdm2012.ua.ac.be/) last month. While they don’t allow for ads to be targeted to individual viewers, they could make TV commercials more effective—and more valuable.

TV advertising is today bought and sold in much the same way it has been for decades. A company that wants to advertise works out who it wants to see its message, and tells that to a TV station, where experts use ratings information from surveys, and their own judgment, to decide when best to run the commercial and how much to charge.

Data from the set-top boxes of an unspecified “major television provider” (presumably AT&T) was used in the new research. The data—anonymized to remove identifying data such as names—included details of channel changes and volume adjustments plus some demographic information. By assuming that someone was watching a channel any time a TV stayed tuned to it for more than 20 seconds but less than one and a half hours, the researchers built up a record of which subscribers had watched what channels, and when. That was used to predict when different demographic segments would be watching TV in the future—predictions that could be used to plan when to show commercials.

Most people don’t know that their TV provider tracks channel changes. Some advocacy groups may protest the possible privacy implications of such techniques, but Way believes viewers will likely be even less concerned than they are about online ad targeting. “It’s a medium that consumers are just more comfortable with,” she says.

AT&T is not the only company exploring new uses for set-top-box data, says Way, although most efforts are focused on replacing the use of ratings based on surveys to guess at viewing figures. “They’re all looking to mine that set-top-box data and use it better and use it for audience profiles,” she says.

AT&T declined to respond to questions about its TV targeting research and so it is unknown whether this might become more than just a research project. But the company last year launched a new service called [AdWorks](http://www.adworks.att.com/) that offers advertisers ways to measure TV campaigns using set-top-box data and to make TV ads interactive via a subscriber’s remote.

<http://www.technologyreview.com/news/510186/att-brings-online-ad-targeting-tactics-to-tv-commercials/>

# Web Ads That Know Too Much

Ads that follow you from one website to another are increasingly common, but in the rush for more tailored advertising, age-old wisdom may be lost.

Online advertising is the foundation of many business models on PCs and mobile devices.

All over the Web, ads are getting more personal. They follow you from one site to the next and know your browsing history. But are such ads really effective? The answer may not be as obvious as digital marketers assume.

The practice of serving ads that match past online behavior, generally called “retargeting,” is growing more important for many online businesses, which are making increasing use of fine-grained data about products or pages that a person has viewed or searched. Last month, even Facebook said it would allow marketers to retarget ads in people’s News Feeds based on their browsing history.

<http://www.technologyreview.com/news/512921/web-ads-that-know-too-much/>

### La creciente popularidad de Android ayuda a Google a hacer crecer su sistema de vigilancia del tráfico

*Los movimientos de los usuarios de Android permiten a Google hacer un seguimiento del tráfico en directo, un servicio que ahora se extiende a nuevos países y otras ciudades de EE.UU.*

Google anunció el lunes de la semana pasada que sus mapas móviles ofrecerán datos en tiempo real del tráfico en 130 nuevas ciudades de Estados Unidos, entre ellas Kalamazoo, Michigan, Tuscaloosa o Alabama, así como en las capitales de Colombia, Costa Rica y Panamá. La cobertura en directo del tráfico en China y muchos países europeos también se verá incrementada. Google ofrece en la actualidad datos de tráfico en más de 50 países, y la mayoría de ellos fueron añadidos durante el último año.

Gracias al sistema operativo que utilizan casi 400 millones de teléfonos móviles, Google ha logrado construir la red de vigilancia de atascos de tráfico más grande del mundo. Pocas personas se dan cuenta, pero al utilizar la función de mapas en un dispositivo con Android de Google se envían datos anónimos sobre nuestra posición y velocidad, que se utilizan para calcular los flujos de tráfico. Si vamos por una autopista a 60 millas por hora (96 km/hora), pero repente reducimos hasta apenas movernos, Google sabe que probablemente estamos en un atasco. El nuevo anuncio de Google pone de relieve la potencia de este enfoque de *crowdsourcing* móvil.

"Lo que realmente permite ampliar el servicio de esta manera son los datos anónimos procedentes de los usuarios de Android", asegura Stephan Seyboth, gerente de producto de Google para tráfico, tránsito y características de direcciones en Google Maps.

Tradicionalmente, las autoridades locales se han encargado de reunir datos sobre los flujos de tráfico utilizando detectores instalados en la superficie de la carretera. "Son caros de instalar, por lo que solo cubren tramos limitados de carreteras", indica Seyboth. "Nuestro *crowdsourcing* proporciona datos anónimos desde el teléfono y nos permite llegar a países sin este tipo tradicional de servicio de tráfico".

Seyboth afirma que Google decidió lanzar su servicio de tráfico en tiempo real en nuevas ciudades basándose en las medidas de calidad y cantidad de sus datos sobre los flujos de tráfico. "Esta función es posible gracias al uso y la adopción de Android", indica, aunque se niega a decir cuántos usuarios de Android necesita una ciudad para conseguir una buena imagen de los flujos de tráfico.

La información enviada a la compañía solo especifica la ubicación y la velocidad, y no puede ser asociada a un usuario o dispositivo en particular, señala Seyboth. Los puntos de inicio y fin de una ruta no se cargan. "No se puede identificar a usuarios o teléfonos individuales siguiéndoles la pista".

Las aplicaciones de mapeo de Google en la actualidad escogen las rutas para los usuarios basándose en su conocimiento de las condiciones del tráfico al iniciar su viaje. Otras empresas están empezando a explorar la posibilidad de que un servicio de direcciones de conducción pudiera tratar de organizar a todos sus usuarios para evitar la creación de atascos en cualquier lugar.

<http://www.technologyreview.es/internet/41059/la-creciente-popularidad-de-android-ayuda-a/>

### La colaboración de Microsoft en la vigilancia electrónica: ¿ayuda voluntaria o nueva táctica legal?

*Microsoft rediseñó sus sistemas para ayudar a los programas de vigilancia de Estados Unidos, pero no se sabe si lo hizo voluntariamente o bajo presión.*

En julio de el año pasado, Microsoft empezó a hacer pruebas públicas de un servicio de correo electrónico y chat llamado Outlook.com. Poco después, según el periódico británico *The Guardian*, la empresa lo rediseñó de tal forma que permitía al programa de vigilancia de la Agencia Nacional de Seguridad (NSA por sus siglas en inglés) llamado PRISM recoger datos del chat antes de que fueran encriptados.

Ahora, los defensores de la privacidad y los expertos en vigilancia se preguntan si las acciones de Microsoft fueron forzadas por una táctica legal anteriormente desconocida, o si la empresa llevó a cabo los cambios de forma voluntaria para ayudar a la vigilancia. El[artículo de *The Guardian*](http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data)es la primera descripción que existe de que una gran empresa de Internet modifique sus sistemas para permitir la vigilancia por parte del Gobierno, y no simplemente proporcionar acceso a datos que ya posee.

El informe de *The Guardian*afirma que además de modificar el funcionamiento de Outlook.com, Microsoft trabajó con el FBI para permitir el acceso a datos en su sistema de almacenaje en nube, SkyDrive, y a aumentar el acceso del Gobierno a las llamadas a través de Skype, que es propiedad de Microsoft. El FBI actúa como intermediario entre las agencias de inteligencia, incluyendo la NSA, y las empresas de Internet. Los cambios llevados a cabo por Microsoft formaban parte de un programa de la NSA llamado PRISM que también recoge datos de Facebook, Google, Yahoo y Apple. Los datos de PRISM se pasan de la NSA a la FBI y la CIA.

<http://www.technologyreview.es/informatica/43478/la-colaboracion-de-microsoft-en-la-vigilancia/>

Como en casi cualquier debate complejo, las respuestas nunca son en blanco y negro. El anonimato en Internet tiene, por lo menos, dos caras.

Por un lado, y en esto se basó mi respuesta en la charla del miércoles, está el uso perverso del anonimato, el apelar a este recurso para ocultar delitos. Muchas personas han sido víctimas de agravios y acoso por parte de sujetos anónimos. Esta es la cara oscura del anonimato, la que me hace sostener que las personas debemos hacernos cargo de lo que decimos en la Red.

Pero hay otra cara, una que, lejos de amenazar el buen nombre y la vida de las personas, los protege

Hay un montón de casos de corrupción que no pueden terminar de procesarse porque la gente no puede hacer la denuncia sin perder el empleo, no cuentan con formas anónimas de comunicar sus denuncias. Cualquier caso donde ir a testificar te cause una pérdida de empleo, es un espacio donde el anonimato por Internet es válido y útil, y lo es en todos los niveles: de gobiernos nacionales y municipales, y de empresas privadas

Todo el asunto viene a complicarse porque, además, el anonimato es extremadamente difícil de lograr en la Red. Cada vez que nos conectamos a Internet se le asigna al dispositivo que usemos (sí, incluso tablets, smartphones, smartwatches y los Glass) un número IP, una cadena numérica que identifica al equipo y, por ende, a nuestra cuenta. Los sitios registran lo que hacemos y, de hecho, saben una gran cantidad de cosas acerca de nosotros. Por ejemplo, el lugar desde el que nos conectamos.

Así que nuestras actividades online son cualquier cosa menos anónimas. Internet es como una ciudad donde hubiera 100 cámaras de seguridad por cada metro cuadrado, dentro y fuera de las casas, y donde no existiera límite en cuanto a lo que se puede registrar, primero porque hay una batalla legal en este sentido, y además porque no se graba video, se guardan archivos llamados logs (registros, en inglés) que, al estar basados en texto, ocupan muy poco espacio.

También creo que el factor humano influye tanto como cualquier tecnología; encuentro difícil imaginar un mundo donde no existan corruptos que facilitan contraseñas, entregan nombres de disidentes o instalan software de espionaje a cambio de dinero. La digitalización no hará que este mundo se vuelva menos imperfecto. Pero esto no cambia el hecho de que una conectividad cada vez más omnipresente y nuevas y mejores tecnologías de cifrado podrán traer alivio a miles de situaciones individuales y colectivas en las que el solo hecho de hacer una búsqueda en Facebook puede atraer una catástrofe.

<http://www.lanacion.com.ar/1619730-las-dos-caras-del-anonimato-en-internet>