Ad Blockers y Publicidad en Internet

Fabrizio Pezzino
fpezzino.13@gmail.com

Universidad Católica Nuestra Señora de la Asunción
Facultad de Ciencias y Tecnología
Departamento de Electrónica e Informática
http://www.uca.edu.py

Resumen El modelo comercial de la web esta basado en las interacciones entre los usuarios, los editores y los anunciantes. El aumento del uso de bloqueadores de contenido significa un cambio importante en el ecosistema de Internet.

Keywords: ads, ad blockers, trackers, fingerprinting, mobile, native

1. Introducción

Internet ha sido el canal de publicidad de mayor crecimiento en los últimos años. El efecto de la publicidad en el desempeño de los negocios siempre se ha considerado difícil de medir. Los medios tradicionales como la televisión, la radio, los periódicos y las carteleras tienen capacidades limitadas de impacto. Internet permite orientar mejor los anuncios a usuarios que estén interesados en los mismos y la tecnología permite medir variables asociadas con la efectividad de un anuncio.

Los anunciantes pagan a los editores de contenido para que muestren entre el contenido que generan el material promocional. Los editores utilizan este ingreso para mitigar la necesidad de que los usuarios paguen directamente por el contenido que consumen. Una compañía compra anuncios para promover la imagen de un producto o para lograr ventas directas.

Existen dos modelos para auto-solventar un portal web: un modelo de ventas de suscripción o mercaderías; y un modelo basado en publicidad. El esfuerzo comercial de la Web se puede dividir en dos tipos: sitios de comercio electrónico; y sitios de contenido. Los sitios de e-commerce producen ganancias vendiendo productos. Los sitios de contenido crean o recolectan texto, imágenes, videos, etc. y producen ganancias por medio de la publicidad.

Las tres partes del ecosistema de publicidad son: los anunciantes, los editores y los lectores. Los anunciantes compran espacio de los editores para vender productos o servicios a los lectores, pero los editores venden espacio para ganar dinero, no para ayudar a vender. Los lectores quieren el contenido de los editores.

La desconfianza entre los anunciantes y los editores ha causado el surgimiento de los ad counters. Son compañías que ofrecen el servicio independiente de contar el número de veces que los editores muestran la publicidad de los anunciantes

por medio de balizas web. Ofrecen este servicio a bajo costo porque les da la oportunidad de recolectar datos sobre los hábitos de navegación.

1.1. Ads[5]

Los primeros anuncios fueron banners, imágenes de 728x90 píxeles que se encontraban en la parte superior de las páginas Web. Los anuncios sidebar son similares a los banners, pero están orientados de manera vertical y son de 120x600 píxeles. Los banners y sidebars tienen tamaños estándares, pero se pueden encontrar en distintas formas y colocaciones.

Los pop-ups son anuncios que se abren en una ventana separada cuando se carga la página y se ubican sobre el contenido de la misma. Los pop-unders son similares pero se abren en segundo plano. Los floating ads son los anuncios animados que "flotan" o "vuelan" sobre la página. Un anuncio Unicast es básicamente un comercial de televisión que se ejecuta en su propia ventana. Son animados y tienen sonido.

Existen otras configuraciones y formatos, todas buscando llamar la atención del usuario y lograr mejores tasas de click.

Search Engine Marketing[4] A diferencia de los banners que aparecen en los sitios web que el usuario visita, SEM coloca anuncios que directamente se relacionan con los términos introducidos en los motores de búsqueda como *Google*, *Bing* y *Yahoo*. Es decir, estos anuncios son más relevantes por ser una respuesta a una acción del usuario.

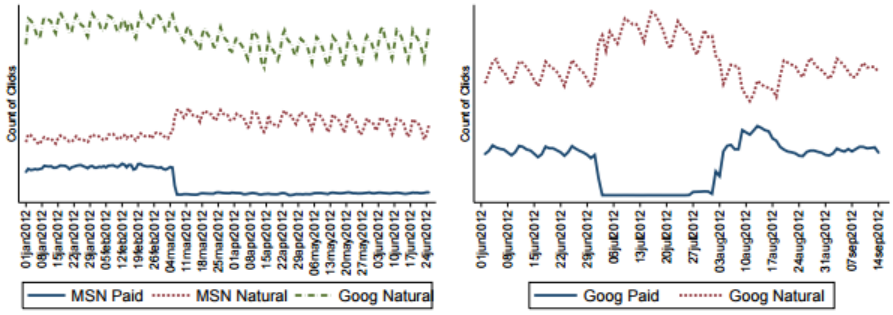
Los resultados de la búsqueda se dividen en dos categorías: patrocinados y orgánicos. El orden de los resultados orgánicos es determinado por el algoritmo del motor de búsqueda, mientras que el orden de los patrocinados dependen de la puja hecha por los anunciantes para aparecer cuando se busca un término en particular.

En la figura 1 se observa que el SEM no es muy efectivo cuando los resultados pagados son similares a los resultados orgánicos. Si una persona introduce *"eBay"* como término de búsqueda, es porque ya conoce lo que está buscando y probablemente haga click en la página *eBay*.

El SEM es más efectivo cuando se utilizan términos genéricos que describen un sitio en particular. Por ejemplo la búsqueda *"subastas on-line"* captará nuevos usuarios al sitio *eBay*.

1.2. Trackers[19]

Tracking es un mecanismo para identificar a una persona y su comportamiento de navegación. Esto puede ocurrir por medio de un dominio de tracking que aparece en múltiples sitios web o por el uso de *cookies*. Se conoce como *cookies* a los archivos de texto almacenados en una computadora (en una ubicación accesible al navegador) que almacenan todo tipo de datos sobre el usuario y los pasan de sitio en sitio.



(a) MSN Test (b) Google Test

Figura 1. Resultados de un experimento hecho en eBay sobre la efectividad de los anuncios de búsqueda pagados.[4]

Los servicios Web pueden rastrear a sus usuarios por varios motivos. Los sitios web y compañías de analítica buscan saber cuántos visitantes únicos tienen sus sitios o aprender cómo navegan sus usuarios dentro de los sitios. Las redes de publicidad buscan medir el nivel de efectividad de los anuncios que distribuyen o para crear un perfil del usuario destinado a anuncios personalizados. Un anunciante de aplicaciones móviles busca entender cuál de sus anuncios resultan en descargas de la aplicación.

Tracking también se utiliza para prevenir fraude. Se puede determinar que un navegador está intentando acceder a una cuenta desde una ubicación desconocida. Una red de publicidad puede determinar clicks falsos producidos por bots.

Los trackers se utilizan para producir anuncios dirigidos que se venden a tasas mayores por ser más efectivos que los anuncios tradicionales. Las redes de anuncios colocan los *cookies* cuando el usuario visita una página que participa en la red.

Do Not Track[12][18] Es una propuesta de política que permite a los usuarios optar por no ser rastreados por sitios web que no visitan, incluyendo servicios de analítica, redes de publicidad y plataformas sociales. Indica la preferencia del usuario por medio de una cabecera HTTP.

Todavía no existe un acuerdo sobre cómo las compañías deben interpretar un pedido DNT. La mayoría de los sitios no cambian sus prácticas cuando reciben la señal. Algunas compañías evitan personalizar los anuncios que muestran. Otras limitan las maneras de recolectar información sobre los hábitos de navegación del usuario.

El *World Wide Web Consortium* (W3C) *"Tracking Protection Working Group"* es un grupo internacional de defensores políticos, expertos técnicos y compañías

que esta intentando crear un consenso sobre la interpretación y propósito del DNT así como una definición apropiada de *"tracking"*.

1.3. Browser Fingerprinting[10][11]

La manera más común de asociar las actividades de navegación entre distintos sitios a un navegador en particular es por medio de los *cookies* HTTP. Estos cookies pueden ser necesarios para que funcionen ciertas características del sitio, pero al mismo tiempo se pueden utilizar como trackers. A diferencia de los *cookies*, el *fingerprinting* no deja evidencia persistente del etiquetado de la computadora del usuario.

El *fingerprinting* consiste en identificar un dispositivo a partir de las configuraciones y/o comunicaciones del mismo. En el caso de los navegadores se utilizan las características que los mismos hacen disponibles a los sitios web como versión del navegador, versión del Sistema Operativo, idioma, toolbars instalados, resolución de pantalla, zona horaria, plugins instalados, fuentes, entre otros.

La cantidad matemática utilizada para medir que tanto un dato permite identificar a un dispositivo se conoce como entropía y se mide en bits. El *fingerprinting* intenta generar suficientes bits de información para contrarrestar los bits de entropía y unívocamente identificar a un navegador.

Ejemplo Supongamos que existen 4 computadoras en una red. Entonces existen $\log_2 4 = 2$ bits de entropía. Si todos las máquinas utilizan el mismo sistema operativo, no obtengo ningún bit de información. Si 2 de las computadoras tienen una resolución de pantalla 16:9 y las otras dos 4:3, obtengo 1 bit de información que puedo utilizar para clasificar las computadoras pero todavía no identificarlas porque me queda 1 bit de entropía. Si dos de las computadoras utilizan *Firefox* y las otras dos *Chrome*, de nuevo obtengo 1 bit de información. Pero si combino estos datos y resulta que sólo una tiene una resolución de 16:9 y utiliza *Firefox*, entonces finalmente reduzco la entropía lo suficiente como para unívocamente identificar una computadora.

Utilizando solamente el *User-Agent sting*, el cual es enviado a todos los sitios que un navegador visita, se pueden obtener usualmente 10.5 bits de información. Lo cual significa que si se elige un navegador al azar, la probabilidad de que otro usuario de Internet comparta ese string es uno en 1500.

1.4. Ad Blockers

Muchos sitios web y aplicaciones proveen un servicio gratuito, contenido gratuito o software gratuito porque alguien más los está pagando. Los proveedores de contenido tienen que mostrar anuncios para obtener los ingresos que solventan su operación. El usuario obtiene los beneficios de usar el producto gratuitamente. Pero algunas veces los anuncios pueden ser molestos, empeorando la experiencia del usuario.

Las extensiones de bloqueo de publicidad funcionan como un *firewall* entre el navegador web y los servidores de anuncios. La mayoría de los anuncios son

bloqueados por extensiones open-source para los navegadores web, instaladas por los usuarios. La base de datos de los servidores de anuncios es mantenida por la comunidad de usuarios. Una vez instaladas, esta extensiones automáticamente bloquean anuncios de terceros en todos los sitios web.

Desde junio de 2015 existen 198 millones de usuarios activos de bloqueadores de publicidad en el mundo. El uso global de bloqueadores creció en un 41 % entre Abril de 2014 y Abril de 2015 [21].

Estas herramientas solo defienden contra las redes de publicidad de terceros que entregan los anuncios por medio del sitio web del editor. Bloquean todos los pedidos de terceros, ya sean redes de publicidad, redes sociales o compañías de analítica. No bloquean anuncios directos del sitios del editor. Algunos también eliminan los *cookies* que se pueden utilizar como trackers. Ninguno de ellos puede evitar el *fingerprinting*.

Los usuarios lo utilizan para evitar ver anuncios, protegerse contra rastreadores, mejorar la velocidad de carga y reducir el consumo de datos. Los usuarios quieren control sobre la manera que consumen contenido web.

2. Debate

Los bloqueadores de contenido pueden ser dañinos para la web. El bloqueo de contenido crea nuevos porteros que pueden elegir quien obtiene el espacio publicitario, favoreciendo a algunos sobre otros, disminuyendo la competencia y la innovación. El modelo comercial de la web se ve amenazado por los mismos. Pero al mismo tiempo, el surgimiento de los bloqueadores y su aumento en popularidad se debe al ambiente tóxico que el usuario percibe producto de la cantidad excesiva de anuncios.

2.1. Legitimidad

No es la primera vez que las compañías con un modelo basado en publicidad recurren a las cortes para eliminar productos que permiten a los consumidores bloquear anuncios. Ocurrió con la demanda contra la VCR en 1979 y contra *ReplayTV* en 2001. En la década de los 90, *ClearWay Technologies* canceló el proyecto *AdScreen* luego de ser boicoteada por los editores de sitios soportados por anuncios. La firma de seguridad *PGP Corp* discontinuó su programa *Internet Fast Forward* luego de ser amenazada con demandas de copyright por modificar los sitios de los editores sin el permiso de los mismos[6].

Anunciantes alemanes han demandado a *AdBlock Plus* argumentando que la extensión del navegador es anti-competitiva y amenaza la habilidad de ofrecer contenido a los usuarios "gratuitamente". La decisión de la corte de Munich se basó en la poca cantidad de usuarios del producto que no justificaba una intervención por anti-monopolio[15].No es la primera demanda contra la compañía, otra con el mismo resultado se presentó ante la corte de Hamburg[30]. Ambas demandas no se centraron en el software mismo, sino en en el modelo de negocios de *AdBlock Plus*; la lista de "Anuncios Aceptables" ha sido calificada por los demandantes como extorsión[28].

2.2. Principios[9]

Mozilla desarrolló unos principios sobre bloqueo de contenido para asegurar que la Web siga siendo abierta y segura para los usuarios.

Content Neutrality El software se debe enfocar en potenciales necesidades del usuario (como desempeño, seguridad y privacidad) en lugar de bloquear ciertos tipos de contenido (como publicidad).

Transparenct & Control El software debe proveer a los usuarios de transparencia y control significativo sobre las necesidades que intenta cubrir.

Openness El bloqueo debe operar sobre los mismos principios independientemente del origen del contenido. Se debe proveer a los anunciantes y a otros proveedores de contenido métodos de participar en un ecosistema Web abierto, en lugar de marcarlos permanentemente en falta y cerrar la Web a sus productos y servicios.

2.3. Privacidad

El uso principal de los bloqueadores de contenido es eliminar los anuncios molestos de los sitios web. Pero una preocupación creciente es la venta de las actividades de navegación de los usuarios. Los anuncios son el enemigo visible que combaten los bloqueadores, pero los trackers que atacan la privacidad de los usuarios son más peligrosos.

Cuando un usuario ve un anuncio, entiende que esta siendo persuadido por el mismo para actuar de cierta forma. El usuario tolera ciertos anuncios porque permiten que su contenido favorito siga siendo gratuito.

Pero cuando las redes de analítica utilizan los hábitos de navegación para mostrar anuncios más específicos, se viola la privacidad del usuario. En ningún momento el mismo accedió a que se utilice su información. Los sitios de analítica venden la información que recolectan sin el consentimiento de los usuarios a los anunciantes.

2.4. Desempeño

Con el auge de la web móvil, los bloqueadores de contenido buscan mejorar el desempeño de la misma. Los usuarios móviles tienen una cantidad limitada de datos. Por tanto quieren evitar desperdiciarlos con la carga de contenido no deseado. Esta reducción del consumo de datos también trae un impacto sobre la batería del móvil, al haber menos datos que transmitir se ahorra energía.

3. Apps

3.1. AdBlock[1]

Creado por Michael y Katie Gundlach en 2009 es una extensión gratuita para *Chrome* y *Safari* utilizada para filtrar contenido en la red. Se inspiró en la extensión *Adblock Plus*, pero no está relacionado con ellos. *AdBlock* esta financiado a

través de donaciones de sus usuarios. *AdBlock* no necesita información personal para funcionar y no rastrea la navegación. Permite administrar excepciones en una página o en todo un dominio permanentemente.

3.2. AdBlock Plus[2]

Creado por Wladimir Palant en 2006 es una extensión open-source y gratuita que permite bloquear anuncios molestos, deshabilitar rastreadores y bloquear dominios que propagan malware. Esta disponible para *Android*, *Chrome*, *Firefox*, *Internet Explorer*, *Maxthon*, *Opera*, *Safari* y *Yandex*. Utiliza listas de filtros, un conjunto de reglas que indican cuales elementos de un sitio web deben ser bloqueados.

Dos listas de filtros vienen activadas por defecto: *EasyList* y *Acceptable Ads*. *EasyList* esta orientado a deshabilitar anuncios que son considerados intrusivos por la comunidad de usuarios. *Acceptable Ads* es una lista de anuncios que cumplen con los criterios de publicidad aceptable de la comunidad de usuarios. Es posible eliminar y agregar otras listas. *AdBlock Plus* recauda dinero a partir de donaciones de los usuarios y a través del programa de Anuncios Aceptables.

Acceptable Ads[3] Es una iniciativa para apoyar a los sitios web que dependen de la publicidad pero que lo hacen de una manera no intrusiva. Es una opción que viene activada por defecto, pero puede ser deshabilitada en cualquier momento. Las entidades que quieran participar en esta iniciativa deben pagar por el servicio de soporte. Se consideran aceptables a los anuncios estáticos, sólo de texto sin imágenes que llamen la atención, a los que no ocultan contenido de la página, los que no interrumpen el flujo de la lectura, anuncios marcados claramente como tales, entre otros. Estos criterios no son definitivos.

3.3. Crystal[8]

Creada por Dean Murphy en 2015. Es un bloqueador de contenido de terceros para *iPhone* y *iPad* totalmente nativo orientado a la web móvil. Bloquea la descarga de anuncios y el seguimiento de sus usuarios. Se integra directamente a *Safari*. Actualmente los bloqueadores de contenido sólo funcionan dentro del navegador y en las aplicaciones de terceros que utilizan el *Safari View Controller*. No almacena datos sobre los sitios que se visitan. Es una aplicación de pago.

3.4. Ghostery[13]

Es un complemento gratuito que muestra los trackers de un sitio y permite elegir cuáles bloquear. Esta disponible para *Firefox*, *Safari*, *Chrome*, *Internet Explorer*, *Opera*, *iOS* y *Android*. Ofrece también los perfiles de los trackers, permitiendo a los usuarios aprender sobre las compañías que recopilan sus datos. Su funcionalidad Click-to-Play permite acceder al contenido y las funcionalidades de la web aunque estén bloqueadas. Recopila información de los usuarios para mejorar sus servicios, esta funcionalidad puede ser desactivada.

3.5. Privacy Badger[24]

Es un proyecto de la *Electronic Frontier Foundation* creado en 2014 disponible para *Chrome* y *Firefox*. *Privacy Badger* es una herramienta de privacidad, no un bloqueador de anuncios. Es una extensión gratuita para navegadores web que evita que los trackers rastreen la actividad en Internet del usuario. Automáticamente analiza y bloquea cualquier tracker o anuncio que viola el principio de consentimiento del usuario, a diferencia de otras aplicaciones que requieren ser configuradas para bloquear a los rastreadores no consensuales. Se enfoca en no permitir que scripts de terceros, que aparentemente están rastreando al usuario, se ejecuten. No utiliza una lista negra, en cambio bloquea los dominios si detecta que están recolectando identificadores únicos luego de recibir un mensaje DNT.

3.6. Purify[25]

Creada por Chris Aljoudi en 2015. Es un bloqueador de anuncios y trackers para iOS. Mantiene una lista blanca de sitios permitidos mantenida por el usuario. Es una aplicación de pago.

3.7. Readability[26]

Es una plataforma web y móvil gratuita que convierte cualquier página web en una versión más limpia para ser leída en la computadora, teléfono o tablet. En 2009 comenzó como una herramienta Javascript que convertía cualquier página en una vista personalizada de lectura. El código original es parte de otras aplicaciones, como Safari 5, Amazon Kindle, Flipboard y Reeder. Esta disponible para *iOS* y *Android* como aplicación. Se puede acceder desde cualquier dispositivo con acceso web en el portal de *Readability*. No comparte la información personal con terceros.

3.8. Tracking Protection[16]

Es una característica del navegador *Firefox* que activamente bloquea dominios y sitios conocidos por rastrear usuarios. Previene cualquier comunicación entre el navegador y sitios de terceros de orígenes inseguros. Filtra los pedidos HTTP salientes y cancela los dirigidos a dominios de rastreo. Depende de una lista de bloqueo curada por los desarrolladores.

3.9. uBlock[27] y uBlock Origin

Es una extensión gratuita y open-source disponible para Chrome y Firefox lanzada en 2014 basadas en la sintaxis de filtros de *AdBlock Plus*. El desarrollador original del proyecto bifurco en dos versiones. *uBlock* es mantenida por el equipo dirigido por Chris Aljoudi mientras que *uBlock Origin* es un build personal del creador original Raymond Hill. *uBlock* acepta donaciones para cubrir costos de hosting, mientras que *uBlock Origin* es un hobby y no acepta donaciones o sugerencias. Utilizan listas de bloqueo mantenidas por la comunidad.

4. Futuro

No es la primera vez que los usuarios actúan para contrarrestar la publicidad en Internet. Cuando la web se encontraba plagada de pop-ups que irrumpían la experiencia de navegación, surgieron programas para evitar que se ejecute el código que crea una nueva ventana. Eventualmente los navegadores se sumaron a la iniciativa incluyendo por defecto la opción de evitar que los sitios muestren pop-ups.

Los anunciantes y los editores entendieron el mensaje. Algunos buscaron crear iniciativas de publicidad no intrusiva que el usuario toleraría para que la web siga siendo gratuita. Otros se adaptaron creando nuevos tipos de publicidad.

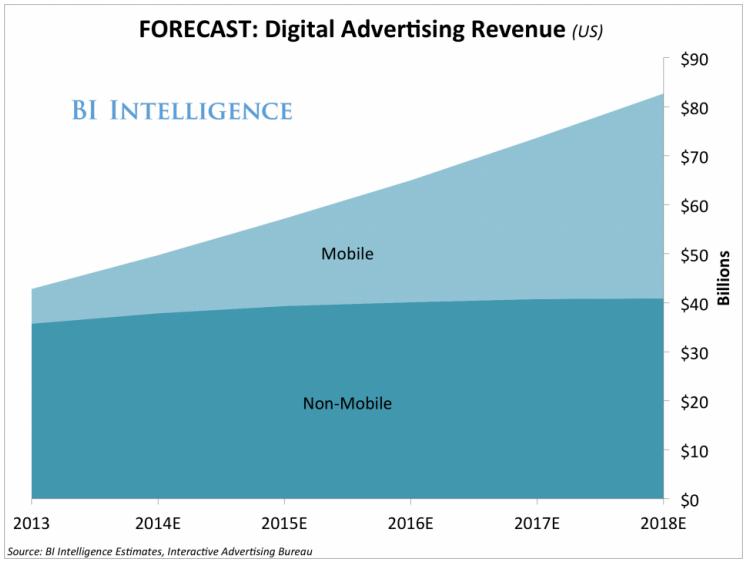


Figura 2. Estimaciones de los ingresos de publicidad digital.[14]

En la figura 2 se observa una proyección del crecimiento de la publicidad en móviles. La mayor parte de los ingresos proyectados se deben a búsquedas y redes sociales. La publicidad dentro de las aplicaciones tiene un mejor retorno que la publicidad en la web móvil.

4.1. Native

La publicidad nativa es aquella que aparece junto al contenido editorial y está formateada para parecerse a ese contenido, aunque etiquetado como un anuncio. Desde la perspectiva de los bloqueadores de contenido, no son publicidad. El contenido patrocinado es el futuro de la publicidad en una web donde se bloquea el contenido de las redes de anuncios.

4.2. Mobile

Los medios móviles de publicidad son: web móvil, mensajes, aplicaciones y video. La Web Móvil se caracteriza por presentar texto y gráficos optimizados para coincidir con la resolución de pantalla y capacidades específicas del navegador de cada teléfono móvil. Existen aplicaciones que albergan anuncios dentro del diseño y la lógica de la misma. Durante el segundo cuatrimestre de 2015, la navegación móvil representó el 38 % de toda la navegación web[22].

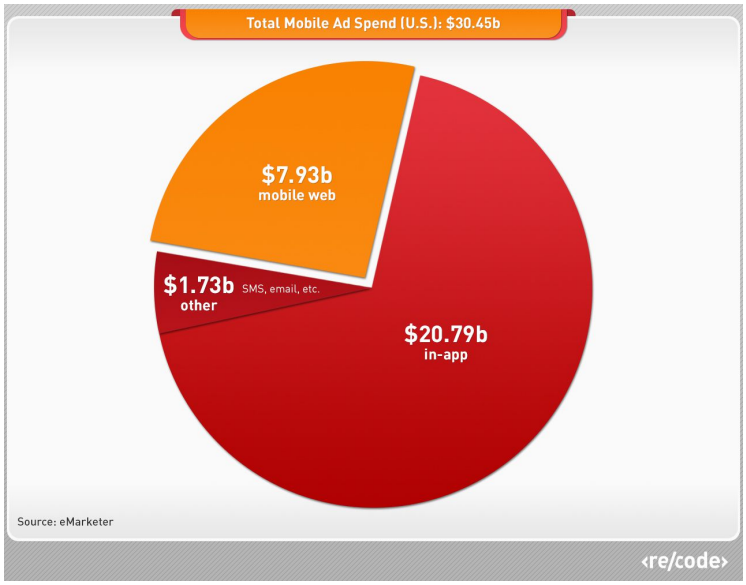


Figura 3. Gráfico circular del gasto en publicidad para móviles en el año 2015.[29]

Los bloqueadores de contenido no eliminaran la publicidad en los dispositivos móviles. Como se observa en la figura 3, el impacto de los bloqueadores de contenido para móviles amenaza a un 25 % del gasto total en publicidad. Esto se debe a la transición de la publicidad en los navegadores a la publicidad dentro de las aplicaciones, por ser más efectiva. La aparición de los bloqueadores de contenido acelerará esta transición.

De la misma manera que *Google* monetizó la web a través de publicidad dentro de su motor de búsqueda, el futuro de la publicidad móvil son las plataformas que incorporan publicidad dentro de su contenido; como *Facebook* y sus *Instant Articles* o *Apple News*.

In-App Blocking *Android* permitía aplicaciones que bloquean publicidad dentro de aplicaciones en la *Play Store*, como *AdBlock Plus* y *AdAway*. Pero estas

aplicaciones fueron removidas de la tienda oficial luego de que Google determinara que violaban el acuerdo de desarrolladores. Específicamente la sección que indica que una aplicación no debe interferir con la funcionalidad de otra aplicación[7].

También es posible editar el archivo **hosts** de manera manual en dispositivos con acceso root para bloquear los sitios de publicidad de terceros[17].

Luego del anuncio de *Apple* de que a partir de *iOS 9* soportaría tecnología de bloqueo de contenido, han aparecido aplicaciones que bloquean anuncios en *Safari* como dentro de otras aplicaciones. Se han aprobado las aplicaciones que se integran al navegador, pero una aplicación llamada *Been Choice* fue removida de la tienda *iTunes*. El creador afirmaba que la aplicación podía bloquear anuncios dentro de *Facebook* y *Apple News*[23].

Been Choice utilizaba una técnica que redirigía el tráfico web a través de una VPN donde se inspeccionaban los paquetes para remover los anuncios dentro de las aplicaciones. *Apple* eliminó la aplicación de la tienda luego de determinar el grave problema de privacidad que causa este método, ya que permite registrar todo lo que un usuario esta haciendo en línea[20].

Referencias

[1] AdBlock. URL: `https://getadblock.com/` (visitado 21-09-2015).

[2] AdBlock Plus. URL: `https://adblockplus.org/` (visitado 15-09-2015).

[3] AdBlock Plus. *Acceptable Ads Criteria*. URL: `https://adblockplus.org/en/acceptable-ads#criteria` (visitado 15-09-2015).

[4] Tom Blake, Chris Nosko y Steven Tadelis. «Consumer Heterogeneity and Paid Search Effectiveness: A Large Scale Field Experiment». Mayo de 2014. URL: `http://www.nber.org/papers/w20171.pdf` (visitado 15-09-2015).

[5] Marshall Brain. *How Web Advertising Works*. Ed. por HowStuffWorks. 8 de abr. de 2002. URL: `http://computer.howstuffworks.com/web-advertising.htm` (visitado 15-09-2015).

[6] Anne Broache. *Web ad blocking may not be (entirely) legal*. Ed. por CNET. 14 de sep. de 2007. URL: `http://www.cnet.com/news/web-ad-blocking-may-not-be-entirely-legal/` (visitado 13-10-2015).

[7] Business Wire, ed. *Adblock Plus Reports Removal from Google Play Store; Android Customers Forced to Watch Ads*. 14 de mar. de 2013. URL: `http://www.businesswire.com/news/home/20130314005784/en/Adblock-Reports-Removal-Google-Play-Store-Android#.VVwoDDY4nTY` (visitado 13-10-2015).

[8] Crystal. URL: `http://crystalapp.co/` (visitado 23-09-2015).

[9] Denelle Dixon-Thayer. *Proposed Principles for Content Blocking*. Ed. por The Mozilla Blog. 7 de oct. de 2015. URL: `https://blog.mozilla.org/blog/2015/10/07/proposed-principles-for-content-blocking/` (visitado 10-10-2015).

[10] Peter Eckersley. *A Primer on Information Theory and Privacy*. Ed. por EFF. 26 de ene. de 2010. URL: https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy (visitado 28-09-2015).

[11] Peter Eckersley. *How Unique Is Your Web Browser?* Inf. téc. Proceedings of the Privacy Enhancing Technologies Symposium, 2010. URL: https://panopticlick.eff.org/browser-uniqueness.pdf (visitado 28-09-2015).

[12] Future of Privacy Forum, ed. *All About Do Not Track*. URL: http://www.allaboutdnt.com/ (visitado 26-09-2015).

[13] Ghostery. URL: www.ghostery.com (visitado 21-09-2015).

[14] Mark Hoelzel. *Mobile advertising is exploding and will grow much faster than all other digital ad categories*. Ed. por Business Insider. 3 de abr. de 2015. URL: http://www.businessinsider.com/mobile-is-growing-faster-than-all-other-ad-formats-2014-10 (visitado 21-09-2015).

[15] Leo Kelion. *AdBlock Plus secures another court victory in Germany*. Ed. por BBC. 27 de mayo de 2015. URL: http://www.bbc.com/news/technology-32903235 (visitado 21-09-2015).

[16] Georgios Kontaxis y Monica Chew. *Tracking Protection in Firefox For Privacy and Performance*. Inf. téc. Columbia University y Mozilla Corporation, 2015. URL: http://ieee-security.org/TC/SPW2015/W2SP/papers/W2SP_2015_submission_32.pdf (visitado 21-09-2015).

[17] Ashutosh KS. *How To Block Ads In Android Apps, Games And Browsers*. Ed. por Hongkiat. URL: http://www.hongkiat.com/blog/blocking-ads-in-android/ (visitado 12-10-2015).

[18] Jonathan Mayer y Arvind Narayanan. *Do Not Track*. URL: http://donottrack.us/ (visitado 26-09-2015).

[19] Robert L. Mitchell. *Ad tracking: Is anything being done?* Ed. por Computerworld. 2 de abr. de 2015. URL: http://www.computerworld.com/article/2489106/data-privacy/ad-tracking--is-anything-being-done-.html (visitado 24-09-2015).

[20] Lara O'Reilly. *Apple has dumped the ad blocker that blocked in-app ads from the App Store*. Ed. por Business Insider. 9 de oct. de 2015. URL: http://www.businessinsider.com/apple-removes-been-choice-and-other-ad-blockers-from-its-app-store-2015-10 (visitado 12-10-2015).

[21] PageFair. *The 2015 Ad Blocking Report*. 10 de ago. de 2015. URL: http://blog.pagefair.com/2015/ad-blocking-report/ (visitado 15-09-2015).

[22] PageFair y Adobe. *The cost of ad blocking. PageFair and Adobe 2015 Ad Blocking Report*. Report. The PageFair Team, 10 de ago. de 2015. URL: http://downloads.pagefair.com/reports/2015_report-the_cost_of_ad_blocking.pdf (visitado 15-09-2015).

[23] Sarah Perez. *Apple Approves An App That Blocks Ads In Native Apps, Including Apple News*. Ed. por techcrunch. 6 de oct. de 2015. URL: http://techcrunch.com/2015/10/06/apple-approves-an-app-that-blocks-ads-in-native-apps-including-apple-news/#.8k6v2h:gDv3 (visitado 12-10-2015).

[24] Privacy Badger. Ed. por Electronic Frontier Foundation. 22 de jul. de 2015. URL: https://www.eff.org/privacybadger (visitado 26-09-2015).
[25] Purify. URL: https://www.purify-app.com/ (visitado 23-09-2015).
[26] Readability. URL: https://www.readability.com/ (visitado 21-09-2015).
[27] uBlock. URL: https://www.ublock.org/ (visitado 21-09-2015).
[28] Jeevan Vasagar y Henry Mance. *Adblocking group wins fresh legal round in media fight*. Ed. por The Financial Times. 27 de mayo de 2015. URL: http://www.ft.com/cms/s/0%2Fef6fe54e-046d-11e5-a5c3-00144feabdc0.html#axzz3bMyPvlCW (visitado 13-10-2015).
[29] Kurt Wagner. *Good News, Publishers! Mobile Ad Blockers Will not Actually Block Much Revenue*. Ed. por Re/Code. 21 de sep. de 2015. URL: http://recode.net/2015/09/21/good-news-publishers-mobile-ad-blockers-wont-actually-block-much-revenue/ (visitado 21-09-2015).
[30] Ben Williams. *Restating the obvious: adblocking declared legal*. 21 de abr. de 2015. URL: https://adblockplus.org/blog/restating-the-obvious-adblocking-declared-legal (visitado 13-10-2015).