HERZOG FOX & NEEMAN
LAW OFFICE

December 2015

HFN AdTech & Technology Compliance Client Update

Dear Clients and Friends,

In this HFN AdTech & Technology Compliance Client Update, you can read about:

- Google Play's new **"ad-supported" label requirement**;
- New **legal challenges for the mobile browser ad-blocker**;
- The extension of **Safe Browsing to Chrome for mobile**;
- Privacy enforcement regarding **targeted native ads**;
- The DAA's Self-Regulatory Principles regarding **cross-device data**;
- The FTC's approval of **parental consent under COPPA ,using "selfies"**;

and a few other industry, compliance and regulatory developments in the fields of digital advertising, technology compliance and information privacy regulations.

Kind regards,

Ariel Yosefi, Partner
Head of AdTech and Technology Compliance
Herzog Fox & Neeman

Quick Navigation

Industry Compliance Developments

"Ad Supported" label requirement for apps in Google Play

Google has recently announced that as from early 2016, all apps published on Google Play and which contain ads (including any promotional material delivered through third-party ad networks, native ads, display ads, banner ads and more), **will be required to carry an "ad-supported" label in the Google Play store listing**. Google originally launched the "ad-supported" tag in April 2015 in its kid-friendly Play Store, as part of the Designed for Families program

In practice, all app developers are required by 11 January 2016, to sign-in to the Play Developer Console and declare whether their apps contain ads. After that date, developers will be required to declare whether or not the app contains ads in order to implement updates.

Any developer misrepresenting the ad presence in their apps, may result in the suspension of the developer account.

Firefox will allow users to block online trackers

Mozilla has announced that the latest version of its Firefox browser will allow users to choose if they prefer to **block online trackers, which follow internet users from site to site**. The new tool, called "Tracking Protection", will be implemented into the Firefox Private Browsing (which until now has only managed locally stored content), for the purpose of deleting cookies whilst allowing third-party scripts to run as intended on the site.

Under the browser's new setup, the Private Browsing mode will block any script that could be used to identify a user, including ads, analytic trackers, and features, such as the Facebook Like button that can be tied back to social networks. The result is a more anonymous kind of browsing that will load pages faster and cut off advertising networks. Users will have the option to turn it on or off, as they do with Private Browsing.

This decision follows the trend of improving the users' control over the data and content presented to them, as we reported in our recent client updates. Very recently, Apple iOS 9 introduced similar changes which allow users to use Content Blocking Safari Extensions on their iPhone apps, which block cookies, images, resources, pop-ups, and other content.

Safe Browsing extends to Chrome users on mobile devices

Google has recently announced that it will **enable Safe Browsing by default on Chrome for Android**, starting with Chrome version 46. Google noted that this step would protect Chrome users on Android from certain types of malware, unwanted software, phishing attacks, and other

cybersecurity threats. It should also be noted that this feature would also be available for Chrome users on iOS devices, but not as default.

In practice, **Google's Safe Browsing systems will now block by default Android Chrome users from navigating to sites that were flagged as hosting or encouraging the download of unwanted software**, phishing, social engineering and malware, through Chrome's "Red Warning".

It is also important to note that Google is releasing the Safe Browsing feature **as part of Google Play Services** (starting with version 8.1), meaning that it is expected that it will come to other in-house mobile apps and services in the future.

Windows 10 update to block code injection

Microsoft has announced that a new Windows 10 update will strengthen the **enforcement against loading unauthorized DLLs onto the Edge browser**.

When Microsoft first announced Edge back in May, it was reported that the browser would have some hidden, built-in security features. This recent update will prevent the loading of unsigned DLLs in order to stop the running of unwanted binary extensions and software. The recent update will upgrade the browser's engine to "EdgeHTML13", which will protect against code injection. This mechanism will block DLL injections on the browser unless they are Microsoft components or signed device drivers.

DLLs that are Microsoft signed (i.e., Edge components, Microsoft supplied features, Widows components, etc.) or Windows Hardware Quality Lab (WHQL) signed (i.e., device drivers), will be allowed to load and others will be blocked.

Notable Legal and Regulatory Actions

iOS ad blocking extension at the center of a new legal challenge

Publishers are struggling with the increasing popularity of ad-blockers. According to a recent report by PageFair, ad-blocking services grew by 41% globally in the last 12 months and are estimated to cost publishers nearly $22 billion during 2015. More and more publishers around the world redirect readers using ad-blocker to a subscription page, asking them to sign up to newsletters, or disable their ad-blocking software. In addition it seems as though the "legal battle" between publishers and ad-blockers is far from over.

Blockr - one of new iOS 9 ad-blocking extensions that allow users to block ads in Safari - is facing a lawsuit filed by the Springer family, the publisher of one of Europe's biggest daily newspapers, "BILD".

The lawsuit, which has been filed to the German District Court of Stuttgart, has as its objective, to prohibit Blockr's developers from being able to "*offer, advertise, maintain and distribute the service*" which can be currently used to block ads. According to the plaintiff's statement, ad-blocking interferes with the constitutionally protected position of publishing houses and endangers their profit model, and in the long run, the existence of professional online journalism.

Although the final ruling is due to be published later this month, at a Court hearing held on 19 November 2015, **the Court dismissed the plaintiff's petition for a preliminary injunction**. According to Blockr's lawyers' statement, the court specifically considered that "*it is the users' independent decision to use content blocking software and that publishers like DIEWELT can adequately react to users who block certain content, for example by banning users of content or ad blockers. A measure already implemented by BILD regarding its online content can be found on www.bild.de.*"

As we previously reported, this is not the first time ad-blocking software faces a "legal battle" in Germany. The previous two cases, in which publishers filed legal claims against ad-blocking browser extension ("Adblock Plus"), were **dismissed by the respective courts which concluded that there is nothing inadmissible or anti-competitive in the service, or with its operators' activities**.

Enforcement of privacy principles in targeted native ads

As we previously reported, the Online Interest-Based Advertising Accountability Program ("**the OIBAAP**") has issued a general compliance warning concerning the enforcement of the Digital Advertising Alliance self-regulatory privacy and disclosure principles ("**the Principles**") with respect to **online behavioral advertising in native ads**. These principles highlight the requirement to deliver transparency and control to users when engaging in online behavioral advertising.

Following the compliance warning, the OIBAAP has recently issued two decisions against Outbrain and Gravity, which concerned the requirement to provide a "*clear, meaningful, and prominent*" link to a compliant disclosure (an "enhanced notice" link) anywhere **on webpages where data is collected, or where an interest-based ad is served** (in practice, in or around the companies' recommendation widgets).

In the Gravity decision, the OIBAAP highlighted the **importance of effectively collaborating with web publishers to ensure that enhanced notice links are in fact provided**, in order to satisfy the obligation to provide enhanced notice on non-affiliate websites. The OIBAAP stressed, in this regard, the importance of the enhanced notice requirement, is deemed as "*the most innovative, privacy-enhancing component of the Principles*". However, the OIBAAP has noted that Gravity has demonstrated that it is committed to remedying the compliance issues.

In the Outbrain disposition, the OIBAAP noted that concerning the initial compliance issues with regard to the effective provision of an enhanced notice, due to the proactive steps taken by it to remedy the compliance issues, Outbrain is now in full compliance with the Principles.

These decisions demonstrate the **importance of complying with the industry's privacy and disclosure codes with respect to delivering online behavioral advertising, and in particular, regarding native advertising and cross-device tracking**. We encourage our clients and friends to consider the implementation of these requirements and to contact us with any questions concerning this issue.

Twitter rejects accusations for illegally Intercepting messages

A lawsuit filed in against Twitter in a Federal Court in San Francisco accused Twitter of violating the Wiretap Act, the Electronic Communications Privacy Act and California privacy law.

According to the plaintiffs, when Twitter users send links to each other, the company transforms the URLs into short links for the purpose of having traffic directed through its own system in order to obtain improved advertising rates. The plaintiffs claim that despite Twitter's assurances that users are allowed to talk privately, the company is eavesdropping on direct messages being sent by users through the social network, without having obtained the consent of its users, and without their knowledge.

In a motion to dismiss, Twitter argued that the Wiretap Act should be applied narrowly and neither the Act nor the Electronic Communications Privacy Act applies to its "processing" of direct messages. Twitter added that shortening URLs allows users to share more without encountering character limits. In addition, Twitter addresses its terms of service and privacy policy disclosures which prove, according to the motion, that users are informed that Twitter "may modify or adapt content… (and) may keep track of how you interact with links across our services...by redirecting clicks or through other means".

Standards and Best Practice Guidance

DAA's Self-Regulatory Principles on Cross-Device Data

The Digital Advertising Alliance ("**DAA**") released initial guidance to assist companies apply the current DAA's Self-Regulatory Principles (in particular, Online Behavioral Advertising Principles, Multi-Site Data Principles, and Mobile Principles) in the rapidly growing cross-device environment. The guidance, titled "Application of the DAA Principles of Transparency and Control to Data Used across Devices", aims to help participants in the digital advertising ecosystem better understand their **obligations regarding cross-device data**.

The guidance makes clear that **the transparency and choice obligations in the existing Self-Regulatory Principles apply to cross-device data practices,** which are also subject to the DAA's independent enforcement.

The DAA recommends that entities should include **notifications** on their websites or apps which describe their data collection and use practices, as well as the fact that data collected from a particular browser or device may be used with another computer or device. This notification should also include the fact that exercising choice through user choice mechanisms, may limit such collection and use. In addition, when data is collected or used on a website or through an application, the website or the application should provide **a clear, meaningful, and prominent link** to a disclosure that **either links to a choice based mechanism, that provides control consistent with the Self-Regulatory Principles, or lists third-party entities which are engaged in the collection of multi-site or cross-app data through its website or application**.

Regulatory and Legislative Developments

FTC allows selfies to verify parental consent for kids under COPPA

The U.S. Federal Trade Commission ("**FTC**") has allowed the use of a **new method involving the facial recognition of parents to verify that the person providing consent for a child to use an online service is indeed the child's parent**.

The Rules promulgated under the Children's Online Privacy Protection Act ("**COPPA Rule**"), require websites and online services directed to children to obtain the consent of a child's parent before collecting personal information from the child. The COPPA Rule allows parties to request the FTC's approval of methods not currently provided for in the Rule. This provision seeks to encourage the development of new methods that provide businesses with more flexibility while ensuring parents are providing consent before collecting personal information from the children.

The COPPA Rule currently allows parents to email, fax or send electronic scans of consent forms, call specified toll-free numbers with their consent, or use their bank or credit cards for payments. One method in use involves checking government-issued identification documents submitted by parents against databases with such information. In contrast to this, the new system performs the verification entirely by face recognition technology.

The approved new system, called "face match to verified photo identification" (FMVPI), requires the parent to submit a snap of a personal photo ID (e.g. a driver's license, passport, etc.) which is verified using image forensics technology, in order to ensure that it is a genuine government-issued document. The parent then submits a selfie, taken with a phone camera or webcam, which the system then compares using facial recognition technology to ascertain whether the person on the photo is the same person as in the second photo.

Once the verification and consent process is completed, the identification information submitted by the parent will be deleted within five minutes.

“Do Not Track” will not be enforced by the FCC

The FCC has **rejected** the privacy advocacy group Consumer Watchdog's petition to compel Internet companies like Google, Facebook and ad providers not to ignore the "Do Not Track" setting in many browsers, which if ignored will be illegal.

"Do Not Track" was created as a standard signal which browsers can send along with other data when visiting a website. When detected, it is intended to inform the visited websites that users do not want their Internet activity to be tracked and shared with third parties, such as advertisers and other online tracking companies.

While the FCC enacted, earlier this year, strict rules providing user privacy protection, it explained that enforcing "Do Not Track" falls outside its jurisdiction. The endorsement of the "Do Not Track" setting by the FCC could have been a powerful regulatory tool that improves users’ privacy. However, for now, the response to a user’s “Do Not Track” setting by websites and third parties, remains voluntary.