HERZOG FOX & NEEMAN
LAW OFFICE

HFN AdTech & Technology Compliance Client Update

February 2016

Dear Clients and Friends,

We are pleased to introduce you to our February edition of our AdTech & Technology Compliance Client Update. As in our previous updates, this update highlights key industry, compliance and regulatory developments in the fields of digital advertising, content, media, technology compliance and information privacy regulations. Among these, you can read about:

- Google's updated **Safe Browsing Policy which will block deceptive embedded content**;
- The **mobile Ad Fraud scheme** which affected nearly **250 Android Apps**;
- New developments in the hot **ad-blocking compliance battles;**
- The announced **banning of Flash-based advertising** in Google's network by the end of 2016;
- FTC enforcement measures against deceptive **browser extension update tactics**;
- **New** guidance on users' **location data monetization**.

Kind regards,

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

Quick Navigation
Industry Compliance Developments | Notable Legal and Regulatory Actions
Standards and Best Practice Guidance

Industry Compliance Developments

Safe Browsing will now block deceptive embedded content

Google has expanded its Safe Browsing protection to block deceptive or social engineering embedded content. The update is provided subsequent to Google's former announcement on this matter in addition to its policy of **escalating the enforcement against "unwanted software" and social engineering**.

The Policy applies to any embedded content which pretends to **act, look and feel, like a trusted source** (such as the user's own browser or the website itself); or **tries to trick the user into doing something he would not have done** if he had known the actual source behind the content (such as downloading phony "updates" embedded in ads, or sharing his user names and passwords).

Google's Safe Browsing systems will warn users, through the standard "Red Warning" page, from navigating to sites that were flagged as hosting deceptive or social engineering embedded content.

Ad Fraud scheme hits Twitter's advertising platform

Security researchers at Sentrant Security have discovered and disrupted an **ongoing mobile in-app advertising fraud scheme** operated through MoPub, Twitter's mobile advertising platform. Based on the findings of the researchers, there have been nearly **250 apps which were widely available via Google Play Store and affected by the ad fraud**. After being notified by Sentrant Security of the scheme, Google removed all rogue apps from Play Store.

This scheme is considered by experts as one of the most sophisticated ad fraud schemes. It had targeted mobile apps in hundreds of thousands of devices running code that runs non-viewable ads in the background. The findings suggest that **this fraud cost more than $250,000 in revenue per day**, involved over 20 shell companies and affected over **500,000 installs** on consumer's Android devices.

This report should not come as a surprise as the **Digital Marketing Community is plagued by a surge of ad fraud activity used to exploit the ecosystem and generate revenues for fake or non-human traffic**. While new standards are expected to standardize the industry and increase the accountability and transparency in the ad supply chain, this case demonstrates how ad fraud is ever-evolving in its complexity and sophistication.

Ad-blocking apps on the hot seat

Following our recent reports (including the previous one) regarding the **ongoing legal and industry attention surrounding ad-blocking**, the ad-blocking software and application trend continues to draw heat.

Earlier this month, **Google has removed the Samsung browser-supported ad-blocker Adblock Fast**, just days after it reached the top of the Play Store. One week following the removal, Google has reversed its decision, accepting the app developers' appeal, and decided to re-instate the app. As the app allowed blocking of ads displayed on another browser app - based on Samsung's update enabling ad-blocking plugins - the reason behind the removal was Google's Developer Distribution Agreement, which disallows apps or plugins offered through the Play Store from "interfering" or "disrupting" services of third parties.

AdBlock Fast was not the only ad-blocking app removed by Google Play. In addition to other cases from the past years, the Crystal ad-block app update was recently rejected based on similar reasons.

It remains to be seen if the growing ad-blocking software industry, which has been facing with legal challenges brought by publishers, will be now see a new compliance challenge posed by the app marketplaces and platforms.

Google to ban Flash-based advertising

Following our previous reports regarding Google's stiffened approach towards flash-based advertisements, Google has recently decided to **exclude flash-based ads from its Display Network**. Consequently, Google Display Network and DoubleClick Digital Marketing **will go 100% HTML5-based**. According to Google's announcement, the chance aims to enhance the browsing experience of more people on more devices, as HTML5 more easily renders multimedia content and is capable of running on any computer and mobile device.

The policy change will go into effect gradually, as follows:

- **Starting 30 June 2016**, display ads built in Flash **can no longer be uploaded** into AdWords and DoubleClick Digital Marketing;
- **Starting 2 January 2017**, display ads in the Flash format **can no longer run** on the Google Display Network or through DoubleClick.

This decision is in line with the current trend of the migration of digital ads from using Adobe Flash to HTML5 format. As we previously reported, the Interactive Advertising Bureau (IBA) published guidelines for HTML5 Digital Advertising for brand marketers and ads developers, concerning how to produce ads in HTML5 format.

Notable Legal and Regulatory Actions

FTC charges developers for installing apps without users' permission

The enforcement against non-compliant browser extensions has reached a new regulatory stage. While in the past most enforcement measures against such extensions were mainly taken under the respective browsers' policies, it has now become an interest of the Federal Trade Commission (”**FTC**”) as well.

The technology company Vulcun has agreed to settle FTC charges that claimed it had unfairly replaced a web browser game with a **program that installed applications on consumers' mobile devices without their prior consent**. Vulcun, which purchased Running Fred, a Google Chrome browser extension game, allegedly **replaced it with its own extension** named Weekly Android Apps, which purported to offer users unbiased recommendations of popular Android applications. In practice, the extension installed certain apps directly on the consumers' Android devices while bypassing the permissions process in the Android operating system.

The FTC's complaint charged that Vulcun's actions unfairly put consumers' privacy at risk and misled consumers by saying that their extensions provided independent and impartial selections of advertised apps, as well as misrepresented third-party endorsements received by the extensions.

Under the terms of the settlement, the company will be required to disclose to consumers details about the types of information a product will access and how it will be used, display any built-in permissions notice associated with installing the product, and **get users' explicit consent prior to the installation or material change of the product**.

This case outlines yet again that the FTC vigorously pursues cases involving **false and deceptive statements made to online consumers** and its **enforcement measures to improve consumers' choice and control with regard to their personal information**.

Facebook accused of violating the French Data Protection Act

CNIL, the French Data Protection Authority, sent a formal notice to Facebook providing it with three months to **stop tracking non-users' web activity without their consent** and to **stop the transfer of personal data collected from French users to the United States**.

CNIL detailed **five alleged violations** by Facebook of the local Data Protection Act, including the collection of **sensitive data**, such as sexual orientation and political and religious views, without users' explicit consent, the **setting of cookies without notice or consent of its users** and the **lack of opt-out tools for users who choose not to be profiled for advertising purposes**.

In addition, Facebook is also accused of continuing to rely on the void Safe Harbor data transfer mechanism in order to transfer users' personal data to the United States. In this regard, the French privacy order is the **first significant action to be taken against a company transferring personal data from the EU to the United States** following the EU Court of Justice ruling from last October (see our report regarding this ruling and its consequences).

It should be noted that although the European Commission and the United States have recently agreed on a new framework for transatlantic data flows, namely the EU-US Privacy Shield, this framework is yet to come into force.

We will be happy to advise our clients on the updated regulatory aspects of transferring personal data from the EU to the United States and to advise on the applicable solutions which will enable such a transfer.

German Court ruled in favor of YouTube regarding User Generated Content liability

YouTube has been facing several court proceedings in recent years brought against it by German music rights group GEMA . In the most recent case, the Higher Regional Court of Munich ruled that **YouTube is not liable for content uploaded by its users, even when it profits from videos that are clearly copyright infringing**.

In this case, GEMA argued that YouTube is liable for the content its users upload. The music group demanded that YouTube pay €0.375 per view for a selection of copyrighted music videos – totaling to a damages claim of around €1.6 million.

The ruling, which confirmed a ruling from a lower court last summer, resulted in a clear win for Google. This decision is **in line with the "safe harbor" principle which, under the appropriate**

circumstances, holds that User Generated Content services are not responsible for the copyright infringement made by its users if they are unaware of the infringing content and have an effective "notice and take down" procedure in relation to such content. A similar verdict was given in favor of YouTube in the United States three years ago, when Viacom International's arguments stating that YouTube is liable for infringing content uploaded by its users, were denied by the District Court.

Standards and Best Practice Guidance

IAB guidance on location data monetization

The IAB, along with its Mobile Marketing Center of Excellence, released the IAB Mobile Location Data Guide for Publishers. This guide is written for data managers in publishing companies who consider leveraging mobile location data to enhance their advertising inventory and who look for solutions to collect and monetize it.

While the core of the guide is professional, it also provides guidance on questions publishers should ask themselves when evaluating location data vendors and the associated privacy and data security concerns. In this regard, **the guide elaborates on different ways to obtain users' permissions and on the risk of data leakage, including measures and controls that can be implemented by publishers to mitigate this risk.**

In addition, the IAB goes into detail about the **growing opportunity for publishers to license their location data to third parties to increase their revenues**.

We will be glad to provide further advice and recommendations in this regard, given the substantial upside potential of users' location data monetization, as well as the **significant risk attributed to legal exposure**.