HFN AdTech & Technology Compliance Client Update

March 2016

Dear Clients and Friends,

We are pleased to introduce you to the March edition of our AdTech & Technology Compliance Client Update. The Update includes various important 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:

- The recent revamp to **Google Play's Policy Center**;
- Regulatory and industry developments and actions in relation to **native advertising and sponsored online influence**;
- Enforcement cases concerning **Silverpush** code and **Supercookies**;
- **Anti ad blocking** tools and tactics suggested by the IAB; and
- Regulatory guidance for **health app developers**;

And a few other important updates and reports.

Kind regards,

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

Quick Navigation

INDUSTRY COMPLIANCE DEVELOPMENTS

Google Play has updated its Developer Program Policy Center

On 1 March 2016, Google Play has added a significant update to its Developer Program Policy Center.

The new Policy Center includes **important updated rules and guidelines for apps published on Google Play**, as well as visual examples for the most common violations. The new Policy Center also includes expanded information on **policy enforcement** in order to help resolve violations.

Some of the key changes and clarifications in the new policy include the following:

Quality and network abuse

- Apps that result in a **low quality** experience may not be eligible for promotion on Google Play.
- Apps must comply with the default Android system optimization requirements as documented in the Core App Quality guidelines for Google Play.
- Apps may not attempt to bypass system power management which are not eligible for whitelisting.

Privacy and user data

- Apps **must post a privacy policy** which, together with any **in-app disclosures**, comprehensively discloses the collection, use and sharing of any user data handled by your app, how it is used, and the types of parties with whom it is shared.
- Apps must **handle the user data securely**, including transmitting it by using modern cryptography (for example, over HTTPS).
- Apps that **monitor or track a user's behavior** on a device must present users with a **persistent notification and unique icon** that clearly identifies the app.
- If the app collects **personal user data unrelated to functionality** which is prominently described in the app's listing on Google Play or on the app interface, then prior to the collection, it must **prominently highlight how the user data will be used** and ensure that the user provides affirmative consent for such use (for example, an app that collects or transmits the user's inventory of installed apps should be subject to adequate disclosure and obtain the user's consent).

Ads and monetization

- Apps should not display **inappropriate ads**, given the intended audience of the app (even if the content by itself is otherwise compliant with Google Play policies).
- Ads associated with the app **should not**:
  - Be **triggered by the home button** or other features explicitly designed for **exiting the app**.

- **Interfere** with other apps, ads, or the operation of the device, including system or device buttons and ports (and which include overlays, companion functionality, or widgetized ad units).

Content restriction

- Apps with **user generated content** (UGC) should employ sufficient **safeguards against threats, harassment, or bullying**, particularly toward minors.
- With respect to **gambling**, the new policy clarifies that apps should not redirect users to a gambling or betting website where users can earn real money (**including ad SDKs that redirect users to gambling websites** which facilitate real gambling).

It is apparent that the new Policy Center improves the degree of transparency and clarity by which Google Play policies are communicated, and is expected to have a considerable impact on the developers' community. We invite our clients and friends to approach us with any questions concerning Google Play policies.

Google's Best Practices for Bloggers Reviewing Free Products

Google has published **best practices for bloggers who receive free products from companies**. Adhering to these guidelines is required under Google's Webmaster Guidelines, and non-compliance may lead to a site being removed from the Google index or otherwise being affected by an algorithmic or manual spam action.

The best practice guidelines include a requirement of using the **"nofollow" tag** where appropriate (specifically in the case of links that pass PageRank in exchange for goods or services); a requirement to **disclose** the sponsored relationship; and guidelines regarding **content quality**.

These guidelines demonstrate the increasing regulatory scrutiny concerning native advertising and sponsored online endorsement/influence. As reported in detail below, this issue has been declared as a regulatory priority by regulators, such as the FTC, and we expect to see increased enforcement and industry guidance in this field.

NOTABLE LEGAL AND REGULATORY ACTIONS

Enforcement Actions in Native Advertising and Online Influence

The Federal Trade Commission ("**FTC**") has settled two **important enforcement cases concerning native advertising and using online influencers**. These cases follow the FTC's Enforcement Policy which was published at the end of 2015 and outlined the FTC's intention to **focus enforcement measures in the area of native advertising** (as was reported in our Client Update).

The Lord & Taylor case concerning undisclosed native advertising

The national retailer, Lord & Taylor has settled with the FTC, the charges alleging that it had deceived consumers by paying for **native advertisements**, including an allegedly **objective article** in an online fashion publication and an Instagram post, without disclosing that the posts were in fact paid promotions for the company's 2015 Design Lab collection.

The FTC's complaint also stated that the company gave its product (a dress) to 50 online fashion "**influencers**" and paid them to post Instagram photos of themselves wearing the dress but **without disclosing the payment, or that they had given each "influencer" the dress in exchange for their endorsement**.

Under the terms of the settlement, Lord & Taylor is prohibited from presenting advertising which it pays for as deriving from an independent or objective source. It also prohibits the company from misrepresenting the independence of endorsers, and requires the company to **clearly and conspicuously disclose material connection between itself and any influencer or endorse**r.

The Machinima case concerning undisclosed payments to online influencers

The FTC has confirmed a final consent order with Machinima, Inc., requiring the company to disclose **when it has compensated "influencers" to post YouTube videos or other online product endorsements as part of "influencer campaigns."**

According to the FTC's complaint, Machinima and its influencers were part of an Xbox One marketing campaign conducted by Microsoft's advertising agency, Starcom MediaVest Group. The FTC argued that **the influencers had failed to adequately disclose that they were being paid for allegedly objective opinions**.

The final order settling the charges brought against Machinima by the FTC, prohibits Machinima from misrepresenting in any influencer campaign that the endorser is an independent user of the product or service being promoted. Among other things, it also requires Machinima to ensure that all of its influencers are aware of their responsibility to make **required disclosures** and for the company to **clearly disclose any material connection between the endorser and the advertiser**, and prohibits Machinima from compensating any influencer who has not made the required disclosures.

The FTC's Endorsement Guides, which were published in May 2015, addresses this issue in detail and provides further regulatory guidance.

These two cases emphasize the various compliance requirements and the increased level of scrutiny in **native advertising and the use of social media to endorse products or services**.

FTC Issued Warning to App Developers Using Silverpush Code

The FTC has issued warning letters to mobile app developers who have installed **software that can monitor a device's microphone to listen for audio signals that are embedded in television advertisements** (Silverpush). The letters were sent to 12 developers whose apps are available for download in the Google Play store and appear to include the Silverpush software.

The Silverpush code allows for the monitoring of consumers' TV habits through unique **audio beacons emitted by TV**, which cannot be heard by the consumer, as long as the mobile phone is in the same surrounding. The letters note that the software would be capable of producing a specified log of the television content viewed while a user's mobile device was turned on for the purpose of targeted advertising and analytics.

The warning letters point out that the apps in question ask users for permission to use the device's microphone, notwithstanding that the apps do not have a requirement for that functionality. However, they **do not inform consumers that the app could monitor television viewing usage**, **even if the app is not in use**. The letters also warn the app developers that if their statements or user interface state or imply that the applications in question are not collecting and transmitting television viewing habits data, when in fact they do so, this could constitute a violation of Section 5 of the Federal Trade Commission Act.

It should be noted that applicable relevant guidance was published by the FTC back in 2013 and included best practices for **privacy disclosures in mobile apps**.

Verizon Paid $1.35m to Settle FCC "Supercookie" Case

As we previously reported, the field of "supercookies" continues to attract the attention of the Federal Communications Commission ("FCC").

Recently, the FCC settled with Verizon Wireless to resolve the investigation against Verizon into whether the company violated the FCC rules by **inserting "supercookies" into consumers' Internet traffic over its wireless network**, as part of the company's **targeted advertising programs**, while failing to reveal this practice to its customers or take appropriate measures to safeguard the information. "Supercookies", like those being used by Verizon and other organizations, make it less difficult for advertisers to reach a consumer with **targeted ads across devices**. It should be emphasized that "supercookies" themselves are not what the FCC is taking issue with, but rather the issues of disclosure and consent.

According to the settlement, Verizon will pay a **$1.35 million fine**, as well as take other actions to refrain from taking similar missteps in the future. Verizon agreed to **notify consumers** about its targeted-advertising programs and obtain the customers' consent **before sharing the supercookie information with third parties or internally**. Moreover, under the settlement, Verizon must only

generate Unique Identifier Headers of a customer through methods that comply with reasonable and accepted **security standards**.

This is the first time that the FCC has fined a company for using "supercookies", which are inserted into mobile web traffic in order to assist companies deliver targeted advertisements. This case should serve as a reminder to all telecommunications and broadband providers to take affirmative action and adopt policies, procedures and practices, in order to ensure compliance with FCC regulation.

STANDARDS AND BEST PRACTICE GUIDANCE

IAB launches Ad Blocking Guide for Publishers

Further to our recent reports concerning the continual legal and industry publicity surrounding ad blocking, ad blocking software and application trends continue to make headlines.

In an effort to prevent the ever growing use of ad blocking programs for web browsers, the Interactive Advertising Bureau ("**IAB**") has revealed a **set of tools and techniques which publishers around the globe can use in response to ad blocking**.

The IAB does not make any particular recommendation with respect to the best tactic to be used, but rather outlines and explains the tactics which are currently available: Access Denial, Tiered Experience, Payment from Visitors, Ad Reinsertion, Payment to Ad Blocker Companies and Payment to Visitors, or Revenue Sharing. In addition, the IAB suggests that the most effective course of action is to follow the following steps:

- **Detect** ad blocking in order to initiate a conversation;
- **Explain** to visitors the value exchange which advertising enables;
- **Ask** for changed behavior in order to maintain an equitable exchange; and
- **Lift** restrictions or limit access in response to consumer choices.

It remains to be seen how these tools and tactics will affect the ad blocking software industry.

REGULATORY AND LEGISLATIVE DEVELOPMENTS

FCC Proposed New Privacy Rules for Internet Providers (ISPs)

On 10 March 2016, the FCC proposed a set of privacy rules ("**the Rules**") for Internet service providers (ISPs). The Rules would significantly limit the ability of broadband and wireless companies to share **data regarding their consumers' online activities with third parties**.

The proposed Rules will be based on three core principles: **transparency**, **choice** and **security**. Under the proposed Rules, broadband and wireless service providers will need to be transparent with regard to their data collection practices, including **expressly disclosing** how private customer data is being collected, how such data is being shared with third parties, and how it is being used by those third parties. The proposed Rules would also require that consumers will be provided with tools in order to encourage **customers' choice over their data**, such as creating a mechanism which will require customers to actively select their participation in the "sharing personal data" program ("opt-in" consent), rather than to be automatically enrolled in it. In addition, companies will be required to strengthen **security practices** which are aimed at safeguarding customer information.

The FCC has published the proposed Rules for public comments and after concluding that stage, there will be various additional regulatory stages before the final Rules enter into force.

Meanwhile, we will be glad to provide further advice in relation to the practical implications of the new Rules and assist in filing comments on behalf of interested parties.

ICO Releases New Encryption Guidance

The UK's Information Commissioner's Office ("**ICO**") has released updated guidance on encryption, amidst concerns that there was a general lack of understanding of when and how to use encryption software **to protect the security of personal data**. The guidance aims to provide advice to companies on protecting personal data through the use of encryption. It is emphasized by the ICO that encryption should be considered alongside other technical and organizational security measures

The ICO recommends that companies conduct a Privacy Impact Assessment to determine the most suitable security measures to implement in any given scenario, and gives examples of various scenarios indicating when data controllers will be required to deliberate on encrypting data.

The ICO has identified the encryption of data when it is being stored (**data storage**) and when it is being transferred (**data transfer**), as providing effective protection against unauthorized or unlawful processing:

- **Data storage**: Companies that use encryption for data stored by them, should put in place **encryption policies** in order that employees understand when encryption should be used, and also how to ensure that encrypted devices remain protected.
- **Data transfer**: The ICO recommends using an encrypted **communication protocol** as the best way to guarantee the safety of data during transfer.

As with many other regulatory authorities, the ICO takes the view that **regulatory action may follow in cases where a lack of encryption has led to a loss of data**. The guidance highlights the fact that many of the recent penalties that the ICO has issued against organizations, where data loss has occurred, may have been avoided if the data in question had been encrypted. This recent concentration on encryption by the ICO, stressing its application to many forms of data storage and many methods of

data transfer, is designated to serve as an important reminder to companies to keep personal data secure, failing which regulatory action will follow.

New HIPAA Guidance for Health App Developers

The U.S. Department of Health and Human Services' Office of Civil Rights ("**OCR**") recently published guidance for developers working on **healthcare applications** with physicians who may need to follow and comply with the Health Insurance Portability and Accountability Act ("**HIPAA**").

The new guidance, which addresses mobile health (mHealth) apps, primarily concentrates on two main questions: First, how does HIPAA apply to **health information** that a patient creates, manages or organizes through the use of a health app? Second, **when might an app developer need to comply with the HIPAA rules**?

OCR emphasizes that the answers for these questions are **fact and circumstance specific**. Rather than a list of rules, the health app guidance sets out several scenarios for health apps and analyzes whether the app developer would be subject to HIPAA in each scenario.

The OCR guidance emphasizes that regardless of whether HIPAA applies, mobile app developers should consider consumer privacy and security in designing an app. The guidance refers to FTC resources on app security and marketing as a place to start in this regard.

OCR has also published a Crosswalk that charts the National Institute of Standards and Technology (NIST) framework for improving critical infrastructure cybersecurity framework to the HIPAA security rule.

The health app guidance and crosswalk provide a meaningful starting point for mobile app developers in determining whether they are subject to HIPAA regulations. We will be glad to provide further advice and recommendations in this regard concerning the required steps in order to achieve compliance with the applicable obligations.