HFN AdTech & Technology Compliance Client Update

April 2016

Dear Clients and Friends,

The April edition of our AdTech & Technology Compliance Client Update is full with new policy and industry updates, together with 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 new **user data policy** for Google Chrome Web Store;
- The beginning of **the "chatvertising" era** as introduced by **Facebook's new "chat bots"**;
- **Microsoft's extended malware protection policy** affecting **programs that change user browsing experience** without using a permitted browser extension;
- The blocking of websites embedding "social engineering" content and ads by Google's Safe Browsing tools;
- Facebook's new policy allowing **Native Ads on News Feeds**;
- New developments in the continuing **ad-blocking legal battle**; and
- New regulatory guidelines and review of **health apps** and **smart TVs**.

We wish our clients and friends a happy Passover and a joyful spring holiday season.

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 | **Regulatory and Legislative Developments**

INDUSTRY COMPLIANCE DEVELOPMENTS

New User Data Policy for Google Chrome Web Store

Google has published an important update to its User Data Policy for the Chrome Web Store. The new policy adds the following **transparency requirements and data usage restrictions** to the existing rules and policies:

- **Posting a Privacy Policy & Secure Transmission** - If an extension/app ("**Product**") handles personal or sensitive user data (including personally identifiable information, financial and payment information, health information, authentication information, website content and resources, form data, and web browsing activity), then the Product must:
  - Post a privacy policy, and
  - Handle the user data securely, including transmitting it via modern cryptography.

- **Privacy Policy Requirements** - The privacy policy must, together with any in-Product disclosures, comprehensively disclose how the Product collects, uses and shares user data, including the types of parties with whom it is shared. The Product must make the policy accessible by providing a link:
  - In the designated field in the Chrome Web Store Developer Dashboard; and
  - In the Product's inline installation page (if applicable).

- **Prominent Disclosure Requirement** - If the Product handles personal or sensitive user data that is not closely related to functionality which is prominently described in the Product's Chrome Web Store page and user interface, then prior to the collection, it must:
  - Prominently disclose how the user data will be used; and
  - Obtain the user's affirmative consent for such use.

- **Other Requirements** - The new policy also adds various requirements and restrictions concerning specific types of personal or sensitive user data, including a new restriction, according to which, the collection and use of web browsing activity is prohibited except to the extent required for a user-facing feature described prominently in the Product's Chrome Web Store page and in the Product's user interface.

More information regarding the new policy is available on the following FAQ page.

Developers will have until **14 July 2016** to **make any changes needed for compliance**. After that date, Products that violate the policy **will be removed from the Web Store** and will need to become compliant in order to be reinstated.

We encourage our clients and friends to review their products, if applicable, and to take the appropriate measures to ensure compliance with the new policy. We will be glad to provide further advice and recommendations in this regard.

Facebook has Launched Chat Bots for its Messenger Platform

Facebook's dramatic announcement concerning the new tools for developers to build bots inside Facebook Messenger, brings a range of new functions to the popular communication app. The released tools include an **API that permits developers to build chat bots for Messenger and chat widgets for the web**.

In a developer blog post Facebook outlined the three main capabilities, as well as directing developers and businesses to the Messenger Platform page to obtain further information:

- **Send/Receive API**: This new capability includes the ability to send and receive basic text, images and interactive rich bubbles containing multiple calls-to-action ("**CTA**");
- **Generic message templates**: include structured messages with calls-to-action, horizontal scroll, URLs and postbacks; and
- **Welcome screen + null state CTAs**: giving the developers the real estate and the tools to customize user's experience.

Nonetheless, according to the new policy, at this stage in time, the Send/Receive API **must not be used to send marketing or promotional messages**, such as sale or product announcements, brand advertising, branded content, newsletters or the up-selling or cross-selling of products or services.

All developers will be given full access to documentation for building their own bots for Messenger, which can then be submitted for review, and to **ensure that its bots adhere to Facebook's standards and protect the user experience**.

It is expected that Messenger bots will facilitate a whole new range of ways for users to connect with brands, and have the potential to cause a significant and wider shift in eCommerce, **while raising new compliance and regulatory challenges for developers**.

Microsoft's New Restrictions on Programs that "Change User Browsing Experience"

Microsoft has published an updated policy for its Malware Protection Center ("**MMPC**"), extending the scope of the evaluation criteria according to which, it detects and blocks programs considered by it as unwanted or as "malware". According to the new policy:

> "Programs that **change the user browsing experience must only use the browsers' supported extensibility model for installation, execution, disabling and removal.** Browsers without supported extensibility models will be considered as non-extensible".

This supplement addresses software that affects or interacts with the browsing experience in different ways (without doing so through a browser extension), and **not just those that insert ads into the browsing environment**. Accordingly, MMPC has moved the criterion from the Advertising criteria to becoming an expansion of its Browser Modifier criteria.

Microsoft encourages developers who may be affected by this policy, to fix their software in order to become compliant with the new criteria and to **follow the respective browser policies. Enforcement of the new policy will commence on 2 May 2016.**

This change in policy is similar to Google's "Unwanted Software Policy" which extended at the beginning of 2015, the application of the company's malware protection tools to programs that make "any change to a browser's functionality… without doing so through a browser extension" (see our related report).

We will be glad to provide further advice and recommendations in this regard concerning the required steps to achieve compliance with the applicable obligations, including their scope.

Google Safe Browsing now Blocks Websites Embedding "Social Engineering Content"

Google has expanded its **Safe Browsing** protection policy and begun to block websites that use deceptive embedded content or ads ("**social engineering content**"). Google considers an embedded content as "social engineering content" when it:

- **Pretends to act, or look and feel, like a trusted entity** — such as the user's own device or browser, or the website itself.
- **Tries to trick users into doing something they would only do for a trusted entity** — such as sharing a password or calling tech support.

This development is part of Google's ongoing efforts which focus on deceptive or unwanted software and content.

Facebook Allows Native Ads on News Feed

Until recently, it has been contrary to Facebook's policies for publishers to post paid articles on their pages, which likewise appear in a user's News Feed. Now, after ongoing feedback and requests from publishers, Facebook has officially updated its branded content policy and ads policy, to **allow publishers to post Native Ads in the form of branded content to their pages**. The new policy applies to text, photos, videos, instant articles, links, 360 videos and live videos.

Although this modification gives rise to many new monetization and promotion possibilities, there are also some limitations which apply. Publishers who wish to post Native Ads **must have pages that have**

been approved by Facebook, and will be required to specify ("tag") the brand that paid for the post. A publisher may also not include any pre-roll or mid-stream commercials within their videos.

Moreover, Facebook is offering **a new tool** that allows **publishers and influencers** to **tag** a marketer when a branded content is published. For brands and businesses, **the new tool will introduce more transparency and allow them to better understand how their marketing initiatives are performing across Facebook**.

This development continues the increasing interest of platforms and publishers – as well as regulators – in various forms of Native Advertising and sponsored influence.

NOTABLE LEGAL AND REGULATORY ACTIONS

The Legal Questions Surrounding Ad Blocking Continue to Make Headlines

Adblock Plus won another legal battle with German publishers

Adblock Plus celebrated another substantial legal victory after one of Germany's biggest newspapers, Süddeutsche Zeitung, had its lawsuit against the company's "Acceptable Ads" dismissed. The case targeted the ad-blocking company's Acceptable Ads program, which whitelists select publishers, based on whether their ads meet a set of criteria, and in the case of larger companies, whether they are willing to pay for it.

At the end of March 2016, a German regional court ruled that **using Adblock Plus to block ads on websites is legal**. The regional court also ruled that the Acceptable Ads initiative **is acceptable under German law**. As part of the ruling, the regional court dismissed the newspaper's argument that Adblock Plus was interfering in a contract which readers were entering into with the newspaper that included accepting ads.

The lawsuit, brought by the company which is behind the leading German newspaper Süddeutsche Zeitung, marks the **fifth successive legal victory for Adblock Plus's parent company Eyeo in Germany**. Nevertheless, the ruling is unlikely to indicate the end of legal challenges to Eyeo, and the decision could be appealed. It remains to be seen how this ruling will affect the ad blocking software industry.

US newspaper groups stand together amid ad blocker's challenge

A group of the biggest US newspaper publishers threatened the maker of the new Brave browser with legal action if Brave Software goes ahead with plans to **replace websites' ads with its own**.

The new browser, the launch of which was announced earlier this year, is available on multiple platforms, and has ad-blocking software imbedded in it, **which blocks all ads by default and replaces**

them with its own ads which it argues load quicker and protect data sovereignty and the anonymity of users by blocking tracking pixels and cookies.

In a cease-and-desist letter addressed to Brave's CEO, the 17 newspaper-publishing companies that cosigned the letter, argued that Brave's advertising-replacement plan would constitute copyright infringement, a violation of the publishers' terms of use, unfair competition, unauthorized access to their sites, and a breach of contract, and in this regard, these publishers intend to fully enforce their rights**.**

It may be the case that the Newspaper Association of America intends to litigate away ad blockers. However, that strategy has proven to be "challenging" outside the US, as reported above regarding Adblock Plus's cases in Germany.

Oracle Resolves Java Security Case with the FTC

The Federal Trade Commission ("**FTC**") has affirmed a final order resolving the Commission's complaint against Oracle alleging that the company deceived consumers as to the security provided by updates to its Java Platform Standard Edition software (**Java SE**).

The FTC's complaint specifically alleged that, as Oracle rolled out updates to users, the software merely updated the most recent version persisting on the user's device; the software updates **failed to remove older versions** of the program or update all versions on the device, and consequently, **left older versions potentially vulnerable to hackers**. **According to the complaint, notwithstanding having knowledge of these issues**, Oracle failed to inform consumers that they needed to manually remove older versions of Java SE.

In accordance with the terms of the consent order, Oracle will be required to **notify affected customers that they may have outdated, insecure versions of Java SE on their computers, and to provide instructions on how to uninstall it**. Additionally, the company will be required to provide a widely available notice to consumers through social media and their website regarding the above mentioned.

STANDARDS AND BEST PRACTICE GUIDANCE

New Regulatory Guidance and Tools for Health App Developers

The FTC has created a web-based tool to assist **mobile app developers** in determining which federal privacy laws apply to their mobile health applications.

The guidance tool presents a series of ten targeted questions to developers that include topics such as:

- The **type of information** the app will create, receive, maintain, and transmit;
- The **type of entity** creating the app (or on whose behalf the app is created);
- The **purposes of the app**; and
- The **information the app will provide** to consumers or patients.

Based on the developer's answers to those questions, the guidance points the app developer towards specified information regarding certain laws and regulations that may likely apply to the app. These include the FTC Act, the FTC's Health Breach Notification Rule, the Health Insurance Portability and Accountability Act ("**HIPAA**") and the Federal Food, Drug and Cosmetics Act ("**FDCA**"). The interactive developer tool also directs users to definitions for common regulatory terms, links, tips and guidance regarding compliance, and other federal agency resources.

Alongside the release of the guidance tool, the FTC also issued its own business guidance aimed at helping health app developers comply with the FTC Act, by **building privacy and security into their apps**. This guidance follows the release of Office for Civil Rights' Health App Use Scenarios & HIPAA guidance, as was reported in our last Client Update.

The increased regulatory activity in the **health-technology sphere** in recent months suggests that **health privacy and security, specifically in the mobile environment, will be an area to be scrutinized by regulators in the upcoming year.**

REGULATORY AND LEGISLATIVE DEVELOPMENTS

FTC to Address Privacy Issues Raised by Smart TVs

The FTC has announced its plans to explore **consumer protection issues raised by new technologies, including smart TVs**.

The FTC specified that nowadays, virtually all television delivery systems – smart TVs, streaming devices, game consoles, apps, and even old-fashioned set-top boxes – **track consumers' viewing habits, and sometimes in new and unexpected ways** (see a related report regarding FTC's enforcement measures concerning the silverpush code in our last Client Update).

According to the FTC, television and streaming device manufacturers, software developers, and the advertising industry are collaborating to learn more about what consumers are watching. These collaborations allow advertisers to precisely target and pinpoint consumers and better understand what ads are working, and consumers may even find advertisements based on their television viewing habits appearing on their phones and desktop browsers.

For example, smart TV manufacturer Vizio is currently facing a federal lawsuit for allegedly sharing information concerning people's viewing histories with ad-tech companies and data brokers. This lawsuit was filed shortly after ProPublica reported that Vizio tracks television viewers by default and then shares data with companies that send targeted ads to people's phones, tablets and other devices.

We expect to see a growing regulatory scrutiny in this type of new fast-evolving advertising technology.