



HERZOG FOX & NEEMAN  
LAW OFFICE



---

## HFN AdTech & Technology Compliance Client Update

---

January 2016

Dear Clients and Friends,

The Adtech and Technology Compliance Team is back with our first Client Update of 2016. As in our previous updates, the update highlights key industry, compliance and regulatory developments in the fields of digital advertising, content, media, technology compliance and information privacy regulations. In this update we discuss, among other updates:

- Microsoft's new policy banning **ad-injection methods by out-of-browser technology**;
- New developments in the **ongoing legal battle surrounding ad-blocking**;
- The increasing enforcement and regulatory attention around **apps and advertisements using children's information**;
- The new FTC **Native Ads enforcement policy and guidelines**; and
- Recent regulatory reports concerning **Big Data** and **Internet of Things**.

Kind regards,

Ariel Yosefi, Partner

[Head of AdTech and Technology Compliance](#)

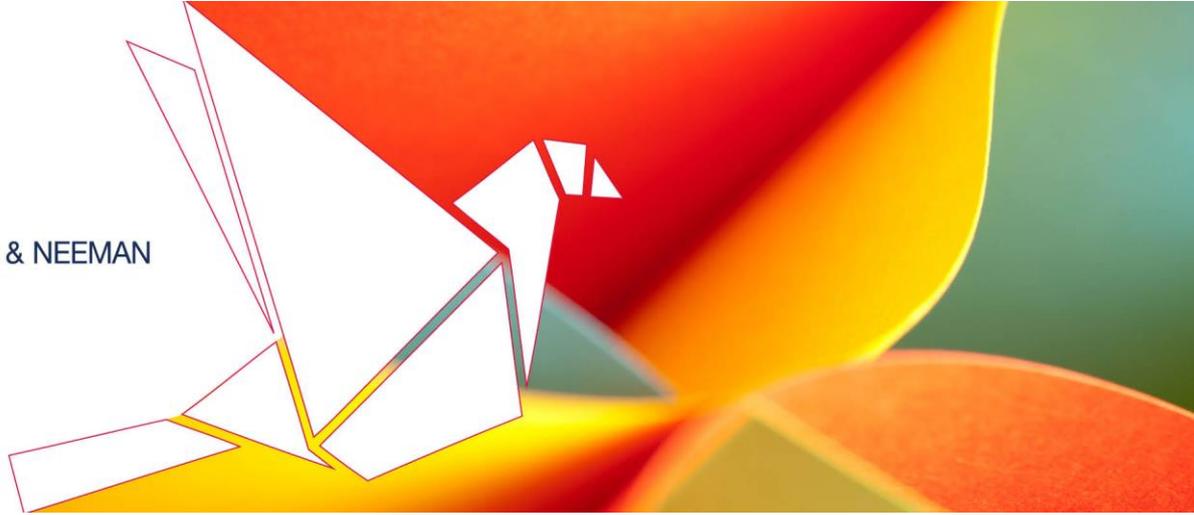
Herzog Fox & Neeman

### Quick Navigation

[Industry Compliance Developments](#) | [Notable Legal and Regulatory Actions](#)  
[Regulatory and Legislative Developments](#)



HERZOG FOX & NEEMAN  
LAW OFFICE



## Industry Compliance Developments

### Microsoft to block "Man in the Middle" advertising software

Microsoft has [announced](#) that starting on 31 March 2016 it will begin blocking **ad-injection methods** which use a variety of "Man in The Middle" techniques, such as **injections through proxy, changing DNS settings and network layer manipulation**. The update follows Microsoft's [former announcements](#) on this matter in addition to the **policy and enforcement measures which it had taken**, addressing unwanted behaviors exhibited by advertising programs which take away both choice and control from users.

According to Microsoft, it is the company's aim to keep the users' control of the browsing experience and to **disable advertising operated by any software located outside the browser**. The Objective Criteria will require that: "*programs that create advertisements in browsers must only use the browsers' supported extensibility model for installation, execution, disabling, and removal*".

The abovementioned requirement aligns with Google's similar policy reflected in its [Malware and Unwanted Software Guidelines](#) which, as previously reported by us in various updates, require that any and all changes to the browsing experience and functionality be done by an extension approved by the Chrome Store and solely via an in-line installation process.

## Notable Legal and Regulatory Actions

### Concern for Ad-Blocking technologies pursuant to a new Court ruling

A new development was recorded in the ongoing legal battle between the ad-blocking industry and publishers. As we [previously reported](#), ad-blocking software has been faced with legal challenges brought by publishers trying to ban ad-blocking in Germany, albeit with no success for the publishers thus far.

Whilst the previous two cases, in which publishers filed legal claims against an 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, a new [ruling](#) by the German District Court in Frankfurt took an opposite and negative approach.



HERZOG FOX & NEEMAN  
LAW OFFICE



In a lawsuit filed on behalf of the news portal Die Welt, the district court **ruled against Adblock Plus** stating that the ad-blocking software interferes with the legitimate business of Die Welt. The Court upheld that the targeted elimination of external advertising by ad-blocking software is regularly unfair and **issued an injunction against Adblock Plus prohibiting it from blocking ads in the Die**

**Welt website.** However, the impact of the ruling is limited at this point given that the decision has been issued in an interim proceeding and may be dismissed at a later stage.

As we [reported](#) last month, Blockr - one of the new iOS 9 ad-blocking extensions that allows users to block ads in the Safari mobile browser – was brought to court by Axel Springer, who also owns Die Welt. In this instance, the Court ruled in favor of the ad-blocker pointing out that a publisher has other options to fight ad-blocking such as preventing users from using the website when detecting that they have enabled ad-blocking software.

We will keep monitoring these contradicting developments in the ongoing legal battle between the ad-blocking industry and publishers.

### **FTC and worldwide authorities increase enforcement against apps using children's private information**

The Federal Trade Commission ("FTC") recently reached settlements with two app developers ([LAI Systems](#) and [Retro Dreamer](#)) concerning **violation of the Children's Online Privacy Protection Act ("COPPA")**.

These app developers **created several apps directed to children**, and allowed **third-party advertisers to collect end users' persistent identifiers** (i.e., data that can be used to recognize a user over time and across different websites or online services, such as MAC address and IMEI), for the purpose of **delivering targeted ads**. According to the FTC, the app developers did not inform the ad networks that the apps were directed to children and **failed to satisfy COPPA's parental notice and consent requirements** before collecting and using the information. Pursuant to the settlements, the FTC has imposed **civil penalties which accumulated to \$360,000** on the app developers.

These enforcement actions are especially noteworthy given that this is the first enforcement action of the FTC under COPPA with respect to the **sole collection of persistent identifiers** and not other types of children's personal data. Furthermore, both **app developers were held liable for the data collection activities of third parties** even though the app developers, themselves, did not collect the data, but rather the data was collected by the ad networks integrated within the respective apps.



HERZOG FOX & NEEMAN  
LAW OFFICE



This enforcement action reflects the FTC's **rigorous approach with respect to children's data collection and related advertising practices** within sites and mobile apps and underscores the importance of taking steps to **ensure compliance with COPPA when offering ad-supported apps for children.**

In this context, we note that the Global Privacy Enforcement Network, which fosters cross-border cooperation among privacy authorities, has [published](#) its Privacy "Sweep" results, which provided interesting conclusions concerning **children's targeted apps and websites**, among which:

- **41%** of the 1,494 sites and apps that were reviewed worldwide raised **legal concerns**, which include the **amount of personal data collected**, the **manner in which the personal data was shared** and **insufficient or misleading disclosures about the practices of processing personal data.**
- over **70%** of the total sites and apps didn't offer an **accessible means for deleting account information**; and
- **Less than 25%** of the sites and apps requested some form of **parental involvement.**

**In light of the increasing popularity of computers and smart devices with young children, the issue of privacy compliance with regard to apps and websites is likely to be a growing area of interest for regulators worldwide.**

### **App developer faces \$2 million fine due to deceptive marketing**

The FTC charges against the app developer Lumos Labs were [settled](#) in a **\$2 million immediate fine**, due to deceptive marketing of the "brain training" app.

The app was advertised as an application which helps users perform better and reduce or delay cognitive impairment associated with age and other serious health conditions. The company advertised that using its games about 15 minutes 3-4 times a week could help customers achieve their "full potential in every aspect of life". However, the FTC found **such attributes and representations to be unfounded and lacking the science evidence to back them up.**

In addition to the \$2 million immediate fine, the settlement requires that Lumos Labs must notify subscribers about the FTC action and must provide means to cancel their subscription.

This case demonstrates the FTC's ongoing enforcement measures against **misleading advertising, especially in the field of health related applications.**



HERZOG FOX & NEEMAN  
LAW OFFICE



## Regulatory and Legislative Developments

### FTC publishes enforcement policy and guidelines addressing Native Advertisements

The FTC has recently released an [Enforcement Policy Statement](#) ("Policy Statement") that sets out **the legal principles and standards which apply to the delivery of native ads**. Additionally, the FTC has also published the [Native Advertising: Guide for Businesses](#) ("Guide"), which supplements the Policy Statement and lays out **practical guidelines and examples concerning the delivery of native ads (such as in-house, in-stream ads and other sponsored content)**.

The Policy Statement and the Guide set forth the legal framework which applies to the delivery of digital advertising formats which are designed to resemble the publisher's organic content, **considering the potential for consumers to be deceived or misled by the nature or source of the promotional content** (taking into account various factors, including the ad's **overall appearance**, the **similarity of its style to non-advertising content**, the degree to which the ad is **distinguishable from such other content** and the **consumer's customary expectations based on its prior experience with the media**).

The Guide includes **various important guidelines and examples** concerning the delivery of acceptable native ads, amongst such:

- **Clarity** – native ads' labels should be **effective in conveying the commercial nature** of the ads. Accordingly, the terms "**Promoted**" or "**Promoted Stories**" should be avoided, as they could potentially mislead consumers that advertising content is endorsed by the publisher;
- **Prominence** – the native ad's disclosures should be **large and visible enough** for consumers to notice them (taking into account various visual cues, such as screen size, color contrasts and fonts);
- **Proximity** – the disclosure should to be in a **location where the consumer is likely to see it**, in front of or above the headline or directly on the focal point of the ad, and **upon first contact** with the consumer.

The FTC clarified that **the Policy Statement and Guide apply to everyone who participates in creating or presenting native ads**, including advertisers, ad agencies, content recommendation platforms and publishers alike.

The Policy Statement and the Guide demonstrate a **more assertive stance of the FTC** concerning the delivery of sponsored content and native ads, and is expected to be **reflected in future enforcement actions**.



HERZOG FOX & NEEMAN  
LAW OFFICE



## The FTC provides recommendations regarding the growing use of Big Data analysis

The FTC has issued a [report](#) that outlines a number of issues for companies to take under consideration **regarding their use of Big Data analytics**. The report aims to highlight the use of Big Data analytics and outlines the benefits and risks it creates.

The FTC notes that Big Data analytics can benefit low-income populations by helping to target educational, credit, healthcare and employment opportunities. Potential inaccuracies and biases, however, might have detrimental effects on those same people.

The FTC urges companies to **ensure that they have an understanding of consumer protection laws that might apply to their Big Data practices** and proposes **key policy questions that aim to depict the ways in which Big Data can both present and prevent harm**. The policy questions are designed to help companies determine how best to maximize the benefit of their use of Big Data while limiting possible harm.

The FTC stated that it will **continue to monitor areas where Big Data practices could violate existing laws** and will bring enforcement actions where appropriate.

## Cybersecurity awareness within the IoT industry

As we [previously reported](#), the field of Internet of Things ("IoT") continues to attract the attention of multiple regulatory authorities. A recent report [suggests](#) that Federal agencies are increasing efforts to counter cybersecurity threats to devices and wearables connected to the Internet.

The Food and Drug Administration **has intensified its attention on medical device cybersecurity in the field of IoT**. The FDA published [cybersecurity guidelines](#) providing non-binding recommendations to medical device manufacturers, including positioning cybersecurity as an **integral component in the design and development process**.

Last year, the FTC published a [Staff Report](#) on IoT with the headline – "Privacy and Security in a Connected World". In the report, the FTC provided recommendations for companies to **ensure that their products, including medical devices, have built-in security features from the outset**.

It seems that this trend of cybersecurity awareness within the IoT industry is only gathering momentum, where enforcement actions are currently limited but will be destined to become more prominent. **Relevant companies should keep a close eye on future regulatory and compliance developments**.