HFN AdTech & Technology Compliance Client Update

June 2016

Dear Clients and Friends,

We are pleased to introduce you to our June 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:

- The extension of Google's Advertising Policies to **apps that are promoted by ads**;
- A new and widely acceptable code of conduct regarding **the review and removal of online hate speech content**;
- **FTC serious enforcement case against mobile ad network – which involved a $950,000 fine and a 20 year compliance monitoring plan that was imposed by the FTC on InMobi**;
- New Court rulings concerning the **responsibility and liability of UGC platforms**;
- Enforcement measures against **non-compliant personal data transfers outside the EU**;
- **The ongoing adblocking legal battle - the new ruling in favor of publishers in Germany and a formal complaint against adblockers to the FTC in the US**;
- New guidelines and best practices for **direct marketing** and **facial recognition**; and
- New regulatory scrutiny affecting **FinTech** and **marketplace lenders**.

Kind regards,

Ariel Yosefi, Partner
Co-Head - Technology & Regulation Department
Herzog Fox & Neeman

INDUSTRY COMPLIANCE DEVELOPMENTS

Google to Require Advertised Apps to be Compliant with its Policies

Google has published an update to its AdWords Policy concerning enforcement for mobile apps.

According to the updated policy, mobile applications that use ad formats such as app promotion ads or app engagement ads, will need to comply with Google's advertising policies. Pursuant to the updated policy, not only the ads, but **also the apps that are promoted or deep linked to** from ads which are subject to Google's advertising policies, will need to be compliant. This includes **the app installation page, splash screens, disclaimers, home screen, and deep linked pages from ads**.

The updated policy will come into effect during the next few months.

Technology Companies Agree to the EU Code of Conduct on Online Hate Speech

Facebook, Twitter, YouTube, Microsoft as well as the European Commission have released a new code of conduct demonstrating these companies commitment to remove hate speech content in less than 24 hours across these social media platforms.

The code of conduct is not legally binding for the Internet companies, even though many of its policies are already covered by other EU legislation such as the e-commerce directive. Instead, it establishes **"public commitments"** for the companies, **including the requirement to review the "majority of valid notifications for removal of illegal hate speech" in less than 24 hours** and to make it easier for the law enforcement authorities to notify the companies directly. The companies have also stated that they would continue to collaborate with the EU in order to identify and discredit extremist speech by promoting so-called "counter-narratives" and supporting educational programs which stimulate critical thinking.

The code of conduct signals the first major attempt to codify how technology companies should respond to hate speech content online, while trying to find the appropriate balance between freedom of expression and hateful content.

NOTABLE LEGAL AND REGULATORY ACTIONS

Ad Network InMobi to Pay $950,000 for Deceptively Tracking Consumers' Locations

The Singapore-based mobile ad company InMobi will pay **$950,000 in civil penalties** and implement a **comprehensive privacy program** to settle Federal Trade Commission (**"FTC"**) charges, according to which it deceptively tracked the locations of hundreds of millions of consumers, including children, without their knowledge or consent in order to serve them geo-targeted ads.

The FTC alleged that InMobi undermined phone users' **ability to make informed decisions regarding the collection of their location information**. Although the company claimed that its software collected geographical locations only when end-users provided opt-in consent, **the software actually used nearby Wi-Fi signals to identify locations when permission was not given**. InMobi then archived the location information and used it to send **targeted advertisements** to individual phone users.

In its complaint, the FTC also alleged that InMobi violated the Children's Online Privacy Protection Act (**"COPPA"**) by **knowingly collecting personal information from thousands of child-directed apps in order to track children's locations and serve them with interest-based advertising**. According to the complaint, this tracking occurred notwithstanding the company's promise not to do so without sending the parents notification or receiving their consent.

Under terms of the settlement, **InMobi is subject to a $4 million civil penalty, which is suspended to $950,000 based on the company's current financial situation**. In addition, the company will be required to delete all information it collected from children, and will be prohibited from other violations of COPPA. Additionally, the company will be prohibited from collecting consumers' location information without their affirmative express consent for it to be collected, and will be required to respect consumers' location privacy settings. The company will also be required to delete the location information of consumers it gathered without their consent and will be prohibited from further distorting its privacy practices. In addition, the settlement requires InMobi **to establish a comprehensive privacy program** that will be independently audited every two years for the **next 20 years**.

This case emphasizes the wide regulatory reach of the FTC's enforcement measures to non-US companies. It also demonstrates the expansion of FTC's enforcement policy - which has been focused so far on user facing software and services - to cover intermediary players such as ad networks.

Germany's Axel Springer Wins a Partial Court Victory against Adblock Plus

As we reported in some of our previous client updates, the legal questions surrounding ad-blocking, continues to make headlines. Recently, a German court has granted the publisher Axel Springer a significant success in its ongoing legal battle against ad-blockers, which users can install on computers

or mobile devices to prevent advertising from being shown. This is the first decision of a court of appeals in this regard in favor of the publisher.

The appeals court in Cologne decided that the ad-blocking provider Eyeo, the parent company of Adblock Plus, **may not charge the publisher for a fee to appear on its "Acceptable Ads" whitelist**. The whitelist enables companies that submit advertising to Eyeo, which is not deemed to be intrusive or annoying, to have their ads served to Adblock Plus' users, while other ads are blocked by the service. **The German court also stated that it did not have objections to ad-blockers as such, confirming earlier rulings** (see our report about the previous decisions).

Adblock Plus has announced that it is planning to appeal the latest ruling to Germany's Supreme Court. Although this case is focused on German law and its implications on adblocking services**, the result and implications arising from this case are likely to have a significant effect on the entire adblocking industry**.

We will continue to monitor these developments in the ongoing legal battle between the ad-blocking industry and publishers, as well as any further updates in this case.

New Rulings Surrounding the Responsibility of UGC Platforms

The issue of the responsibility and liability of online service providers, such as internet platforms that are based on user generated content, continues to be a hotly debated subject in US court rulings.

Although under US law, section 230 of the Communication Decency Act sets out the key "Safe Harbor" principle **that provides online services with immunity from liability concerning the actions of their users** (with certain exceptions, such as infringement of intellectual property), **more and more courts are giving a narrow interpretation to this principle, thereby broadening the potential liability of online service providers**.

At the beginning of the month, a US court of appeals ruled that section 230 does not protect a website from being sued over **failing to warn users of potential harm that could come from other users on the site**. In another ruling from this month, a US court declined to dismiss claims that Facebook should be held **responsible for violating a person's publicity rights**, under the theory that publicity rights are covered under intellectual property (and therefore are exempted from the Safe Harbor principle) . In another ruling, a California appeals court determined that Yelp is **responsible for removing reviews from its site that the court found defamatory**.

As illustrated in these recent rulings, **courts are demonstrating a reluctance to uphold the Safe Harbor principle** in various circumstances, **thereby requiring the service provider to adopt a more "proactive" approach with respect to user behavior and content**. In practice, these rulings reflect that online service providers should apply an increased level of scrutiny and monitor user activity on a more "proactive" basis, as reasonably required, in order to mitigate the associated risks.

German DPA Fined Three Companies for Transferring Data from the EU to the US

In a recent press release, the Data Protection Authority of Hamburg (**"Hamburg DPA"**) announced three final decisions regarding fines imposed on companies which unlawfully transferredpersonal information outside of the EU. The Hamburg DPA determined that after the invalidation of the former "U.S.-EU Safe Harbor Framework" by the European Court of Justice in October 2015, **the companies had failed to otherwise adequately ensure the protection of employee and customer data transferred from Europe to the US.**

The Hamburg DPA's investigation discovered that although the majority of companies had implemented standard contractual clauses (**"SCCs"**) on a timely basis in order to cover their data transfers to the U.S., some were transferring customer and employee personal data in violation of EU law. The three companies that were fined had been found to have unlawfully transferred data from Germany to the U.S. However, since they had transitioned to SCCs during the course of their respective proceedings, the fines were reduced significantly from the potential maximum of €300,000 to €8,000, €9,000 and €11,000, respectively**.**

The Hamburg DPA enforcement actions are the first enforcement actions made public against companies that did not adjust their EU-US data transfer compliance practice, and will probably not be the last. **Companies should also anticipate enforcement actions for non-compliance from other European DPAs.** We will continue to closely monitor and provide updates on future developments.

Twitch Filed Suit over Artificial Viewer Inflation Bots

Twitch Interactive, Amazon.com's subsidiary that operates a platform which allows users to watch others play video games, has filed a lawsuit in a California Federal Court against **seven bot makers for selling bots that are allegedly used to inflate the view-count, follower the count, and engage in chat activity on Twitch channels**.

The popular live streaming video platform, argued that the bots harm Twitch and its user community by **misleading them regarding the broadcasters' true popularity and making it difficult for users to discover legitimate broadcasters**. Twitch also brought claims of federal trademark infringement, cybersquatting, computer fraud and abuse, tortious interference, unfair competition, fraud, breach of contract, and violation of the California Comprehensive Computer Data Access and Fraud Act.

View-count inflation is a significant issue for streamers and video producer as it causes users to be misled regarding a broadcasters' true popularity. By filing this lawsuit, Twitch is sending a clear message concerning its plan to enforce the quality of social interactions on its service.

STANDARDS AND BEST PRACTICE GUIDANCE

ICO Released updated Direct Marketing Guidance

The UK Information Commissioner's Office (**"ICO"**) has introduced some new changes to its Direct Marketing Guidance, presenting more direction on what constitutes a **valid consent** under the applicable regulations in the context of carrying out direct marketing via calls, texts and other electronic means. Key changes include these new guidelines:

- **Indirect or third party consent and using bought-in marketing lists:** indirect consent is very unlikely to be valid for marketing through emails, texts or calls. It will also be very difficult to use bought-in lists for text, email, or automatic call campaigns, as specific consent is required.

- **General categories of organizations**: Consent must be "specific" and a general category of organization will not be sufficient to obtain specific consent for such marketing purposes.

- **Obtaining freely given consent**: "freely given" consent must be demonstrated where any marketing consent is a condition of receiving products or services.

- **Marketing by not-for-profit organizations:** In the not-for-profit sector (including charities) as well as any other sector, any messages that have a marketing element will still be caught by the definition of direct marketing even if the primary purpose for the communication is not a marketing one**.**

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

Facial Recognition Technology Best Practices

The National Telecommunications and Information Administration finalized its privacy guidelines for the commercial use of facial recognition ("**the Guidelines**"), which introduce a set of **voluntary best practices** for the commercial use of facial recognition technology.

The Guidelines generally apply to any person, including corporate affiliates (collectively, "**Covered Entities**") which **collect, store or process facial template data**, namely, a unique facial measurement generated by automatic measurements of an individual's facial characteristics, which are used by a Covered Entity to uniquely identify an individual's identity or authenticate an individual. The Guidelines do not apply to the use of facial recognition for the purpose of aggregate or non-identifying analysis.

The Guidelines cover different issues of transparency, privacy, security and other essential topics

which relate to facial recognition use. In particular, the Guidelines include the following requirements:

- **Transparency**: Covered Entities should **disclose to users their data practices regarding the collection, storage and use of facial template data** (e.g. by referring them to a suitable privacy policy). Such disclosure should elaborate on the purposes of the data collection, the data retention periods, the use of any de-identification practices, and more.

- **Privacy by design**: When developing their **facial template data management practices**, the Guidelines suggest that Covered Entities should consider certain issues, such as: the way by which facial template data will be stored and used; the collection and processing of any non-facial recognition sensitive data; the risks and harms this process may impose on users; and the reasonable expectations of users with respect to the use of their facial template data.

- **Data sharing**: Covered Entities should offer their users the opportunity to **control the sharing of facial template data with third parties**.

- **Security**: Covered Entities should implement **reasonable security measures to safeguard users' data**, consistent with the nature and scope of the activities of the Covered Entities and the sensitive nature of the data.

- **Users' privacy rights**: Covered Entities should take reasonable steps to maintain the **integrity of the facial template data** collected by them and to offer users a procedure to contact the Covered Entity with regard to its use of facial template data.

These Guidelines reflect privacy and security risks surrounding the use of facial recognition technology and demonstrate the focus of the industry as well as other regulators, aiming to address the various privacy and security concerns stemming from these technologies.

REGULATORY AND LEGISLATIVE DEVELOPMENTS

NAA Asked FTC to Investigate Unlawful Ad-Blocking Practices

The legal and regulatory examination of adblocking services is expanding to the US. Recently, the Newspaper Association of America filed a formal Complaint and Request for Investigation with the FTC alleging that certain adblocking technologies and related services violate FTC rules designed to protect consumers from **unfair and deceptive** trade practices.

The complaint requested the FTC to investigate **ad-blockers that offer "paid whitelisting" - a service which charges advertisers to bypass ad-blocking software - along with services that substitute adblockers' own advertising for blocked ads or to avoid publishers' subscription pages** (see our

related report regarding Brave Software).

This complaint demonstrates an increasing correctness by publishers to legally challenge adblockers and their business model, which affects publisher's ad-revenue opportunities.

FinTech and Marketplace Lenders under Scrutiny

Recent regulatory developments point to the potential for **increased regulatory scrutiny of marketplace lending and their service providers**.

Among these developments is the FTC's new FinTech forum which addresses **marketplace lending**. The forum was promoted by the FTC as the first in a series **it plans to hold in order to explore emerging financial technology and its implications for consumers**. The discussion in the forum covered a wide range of themes relevant to marketplace lending, including the **implications of the Fair Credit Reporting Act ("FCRA")** on marketplace lenders' usage of information about consumers in making credit decisions; the appropriate tools and context of disclosing **loan terms during an online application process**; and issues concerning the regulatory limitations on **sharing consumer data by marketplace lenders and related third parties, including lead generators**.

The FTC's regulatory review regarding this issue was also followed by the announcement of the Consumer Financial Protection Bureau concerning the **acceptance of complaints on consumer loans from online marketplace lenders**, as well by the announcement of the U.S. Treasury Department with regard to the **publication of a White Paper concerning its review of the online marketplace lending industry**.

We will continue to closely monitor and provide updates on future regulatory developments in this field.

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel | Tel: (972)-3-692-2020 | Fax: (972)-3-696-6464
Twitter: @hfnlaw | Blog: unfolding.co.il | hfn@hfn.co.il | www.hfn.co.il