HFN Technology & Regulation Client Update

August 2017

Dear Clients and Friends,

We are pleased to introduce you to our August edition of the Technology & Regulation Client Update. Although the pace of regulatory developments is relatively low during the summer period, the past month has seen a few important updates in the fields of technology compliance, digital advertising, content and information privacy regulations. These include the following:

- **Google Play's updated policies which are beginning to allow gambling apps, placing new requirements on content rating and adding clarifications on user data collection;**
- **A US District Court's ruling which required LinkdIn to unblock a startup company from scrapping public profile data;**
- **Uber's settlement with the FTC over allegations concerning lack of appropriate privacy and data security measures;**
- **The Online Interest-Based Advertising Accountability Program's enforcement of transparency and opt-out principles in targeted ads; and**
- **Russia's new law that will prohibit using VPNs and other anonymization tools**.

Kind regards,

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

If you have an important regulatory or industry compliance update you would like to share with the industry, let us know.

Google Play Policies Update

TOPICS: App Industry Compliance, Gambling Apps, Content Rating, User Data, Google Play

Google has recently introduced a number of significant updates to its Google Play policies. A summary of the key updates is as follows:

- **Gambling apps**

In the past, Google Play policies prohibited the distribution of gambling apps (as opposed to ads promoting gambling, which were permitted about a year ago, subject to certain requirements; see our related update). **Google Play has now officially permitted the distribution and promotion of gambling apps**, subject to the following requirements:

a. The gambling app may only be distributed at this stage in **UK, Ireland, and France**;
b. The developer must submit an application form here (the developer will be required to submit its gambling license details including the regulatory authority, etc.);
c. The developer must be in possession of a **valid gambling license** for each country in which the app is distributed. The app must prevent use from countries which are not covered by the developer-provided gambling license;
d. The app must prevent under-age users from gambling in the app (through an "age-gate") and warn potential end-users that under-age gambling may be illegal;
e. The app must be free to download and install from the store;
f. The app **may NOT use Google payments services** (e.g. Google Play In-app Billing);
g. The **app and its listing must clearly display information as to responsible gambling** (e.g. making available self-tests to allow individuals to determine whether they are at risk of gambling addiction, providing information regarding treatment options for compulsive gambling, and indicating the location of treatment centers for gambling addiction);
h. The app **must be rated AO** (Adult Only) or IARC equivalent; and
i. The app must comply with all applicable laws and industry standards for any country in which it is distributed.

- **Content rating**

Google Play now requires that every app is rated **according to the IARC rating**, which is designed to assist developers communicate locally relevant content ratings to users, and inform consumers, especially parents, of potentially objectionable content that exists within an app.

To receive the IARC content rating, the developer must complete this questionnaire. The app will be assigned a content rating from multiple rating authorities based on the questionnaire responses.

As this process is now mandatory, **Apps without a content rating may be removed from the Play Store.**

- **Collection of user data**

In accordance with existing Google Play policies, if an app collects and transmits personal or sensitive user data unrelated to functionality of the app (e.g. Installed apps), then prior to the collection and transmission, it must **prominently highlight how the user data will be used** and the user will be required to provide **affirmative consent** for such use through an "in-app disclosure".

Google Play policies now clarify that **the "in-app disclosure" must**:

a. Be within the app itself and not only in the Play listing or a website;
b. Be displayed in the normal usage of the app and not require the user to navigate into a menu or settings;
c. Describe the type of data being collected;
d. Explain how the data will be used;
e. Not be placed only within a privacy policy/terms of service, or with other disclosures unrelated to personal or sensitive data collection;
f. Present the consent dialog in a clear and unambiguous way;
g. Require affirmative user action (e.g. tap to accept, tick a check-box, etc.) in order to accept (the app cannot consider navigate away from the disclosure (including tapping away or pressing the back or home button) as consent;
h. Not begin personal or sensitive data collection prior to obtaining affirmative consent; and
i. Not utilize auto-dismissing or expiring messages.

- **Android Instant Apps**

Google Play policies have now included specific and additional requirements relating to the distribution of Android Instant Apps (e.g. payments, technical specifications, app visibility, etc.).

We would be happy to provide further advice and recommendations concerning the updated compliance requirements and their scope.

US Federal Court Required LinkedIn to Unblock Startup from Scraping Public Profiles

TOPICS: Public Data Scraping, LinkdIn, US District Court, United States

Earlier this month, the US District Court for the Northern District of California granted a preliminary injunction ordering LinkedIn to allow hiQ Labs **free access to LinkedIn's website and to remove, within 24 hours, any technology preventing hiQ from accessing public profiles**.

The decision was given following a lawsuit brought by hiQ in June, after LinkedIn had issued a "cease and desist" letter demanding that the company will cease scraping LinkedIn's website as it violates LinkedIn's terms of use. The letter indicated that LinkedIn had implemented technological measures to prevent hiQ from continuing to scrape its data and that further attempts to circumvent such protections would be a violation of the Computer Fraud and Abuse Act ("**CFAA**"). After the parties were unable to agree on a resolution, hiQ filed a complaint arguing that hiQ's right to have access to public LinkedIn profiles, has been infringed. In addition, hiQ filed a request for a preliminary injunction

to be granted against LinkedIn.

In its decision, the Court **declined to accept LinkedIn's motion that the CFAA can be raised in order to prevent access to publicly available data** and held that a broad interpretation of the CFAA "could profoundly impact open access to the Internet, a result that Congress could not have intended when it enacted the CFAA over three decades ago". This decision diminishes a previous ruling from July 2016 of the US Federal Court of Appeals for the 9th Circuit (Facebook v. Power Ventures) which expanded the interpretation of the CFAA's prohibition to access computer material, without authorization, to a case of circumventing technological barriers (such as IP blocking) to otherwise publically available websites (see our related reported here).

In its decision, the Court held that the hiQ's continued access to LinkedIn's **public profiles**, even after LinkedIn has explicitly revoked permission to do so, should not be considered as an "access" to computer "without authorization" within the meaning of the CFAA. Moreover, the Court stated that **circumvention of a technological barrier does not automatically gives rise to a CFAA violation** and consequently, the circumvention of LinkedIn's blocking techniques, which prevent use of bots or implements IP address' blocks, does not violate the CFAA, **since hiQ accessed only public information which was not protected by an authentication gateway**.

An additional important outcome is that LinkedIn's decision to block access to "open data" may be considered as giving rise to "unfair" competition under California's Unfair Competition Law. In this regard, the Court specified that there is a basis to conclude that LinkedIn unfairly leveraged its position in the professional networking market for an anticompetitive purpose and that such activity could possibly constitute a violation of anti-trust laws.

LinkedIn announced it would challenge the decision, as the case could dictate the extent to which companies have control over publicly available information which is hosted on their services.

Given the above, companies that rely on accessing publicly available information, should monitor the developments in this case and carefully consider how they are accessing such information. We will be happy to advise our clients and clarify the overreaching implications of this decision.

Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims

TOPICS: Privacy and Data Security, Data Breach, Federal Trade Commission, United States

Uber Technologies has agreed to implement a **comprehensive privacy program** and obtain regular, independent audits to settle the Federal Trade Commission's ("**FTC**") charges that the company deceived consumers by **failing to: (i) monitor employee access to consumer personal information**; and (ii) **reasonably secure sensitive consumer data stored in the cloud**.

According to the FTC's complaint against Uber, the company failed to fulfill its claims that it closely monitored employee access to consumer and driver data and that it deployed reasonable measures to

secure personal information stored by it on a third-party cloud provider's servers.

Following news reports alleging Uber employees were improperly accessing consumer data, the company issued a statement in November 2014 that it had a "strict policy prohibiting" employees from accessing rider and driver data – except for a limited set of legitimate business purposes – and that employee access would be closely monitored on an ongoing basis. Although the company developed an automated system for monitoring employee access to consumer personal information, the company ceased to use it less than a year after it was put in place. The FTC's complaint alleges that Uber, for more than nine months afterwards, **rarely monitored internal access to personal information regarding users and drivers**.

The FTC's complaint also alleges that despite Uber's claim that data was "securely stored within our databases," Uber's **security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases which Uber stored with a third-party cloud provider**. As a result, a hacker accessed personal information concerning Uber drivers in May 2014, including more than 100,000 names and driver's license numbers that Uber stored in Amazon's cloud service. The FTC alleges that Uber did not take reasonable, low-cost measures that could have helped the company prevent the breach. For example:

- Uber did not require programmers to **use distinct access keys** to access personal information stored in the cloud. Instead, Uber allowed them to use a single key that gave them full administrative access to all the data, and did not require multi-factor authentication for accessing the data; and
- In addition, Uber stored **sensitive consumer information**, including geolocation information, in **plain readable text** in database back-ups stored in the cloud.

Under its agreement with the FTC, Uber is required, inter alia, to implement a comprehensive privacy program that addresses privacy risks relating to new and existing products and services and protects the privacy and confidentiality of personal information collected by the company; and to obtain within 180 days, **and every two years after that time, and for the next 20 years**, independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order.

This settlement is an important reminder for companies holding employees and consumers' personal data, not only to put in place appropriate privacy and data security policies, but also to maintain appropriate monitoring tools in order to ensure that the required policies are being adequately implemented within the organization.

Enforcement of Transparency and Opt-out Principles in Targeted Ads

TOPICS: Adtech Industry Compliance, Behavioral Advertising, Targeted Ads, Online Interest-Based Advertising Accountability Program

As we previously reported, the Online Interest-Based Advertising Accountability Program ("**the OIBAAP**") is actively enforcing the Digital Advertising Alliance self-regulatory privacy and disclosure principles ("**the Principles**") with respect to online behavioral advertising.

Recently, two digital advertising companies, Adbrain and Exponential Interactive, were subject to enforcement action by the OIBAAP for non-compliance with the Principles. The enforcement actions highlight two primary principles:

- **Enhanced Notice – both publishers** (such as website and mobile app) and companies involved in digital advertising (such as ad networks, agencies and servers) **share the responsibility for providing an "Enhanced Notice"**, which is a clear and prominent link placed in or around the advertisements, which takes end users to a disclosure that explains the adherence to the Principles and links to an "opt-out" mechanism. In its Exponential decision, the OIBAAP found that Exponential, while not having direct access to the website from which it collected data, was nonetheless responsible for ensuring that the Enhanced Notice was being provided.

- **Opt out** – In its Adbrain decision, the OIBAAP found that Adbrain did not provide an "easy-to-use" tool for end users to opt out of behavioral advertising. Interestingly, although Adbrain had an opt-out mechanism that was operative, the OIBAPP **found it was so difficult to use that it resulted in a violation of the Principles**, stating that "Adbrain's opt-out solution was easy for the company, not for the consumer."

The key takeaways from these enforcement actions are:

- Digital ad networks, agencies and servers should review the publishers' properties (such as websites and mobile apps) to ensure that the Enhanced Notice is being provided to end users.
- An opt-out mechanism should be easy to use. By way of example, requiring the user to enter into a text box the "device ID" of the mobile device they wished to opt out, is not compliant with the Principles.

These decisions demonstrate the importance of complying with the industry's privacy and disclosure codes with respect to delivering online behavioral advertising. We encourage our clients and friends to consider the implementation of these requirements and to contact us with any questions concerning this issue.

Russia Joins China in Prohibiting Browsing Anonymization Tools

TOPICS: Internet, VPNs, China

Recently, Russia has passed a law **prohibiting software that allows users, on an anonymous basis, to view internet sites which are barred in the country**.

The new law, which will take effect on 1 November 2017, prohibits services that allow people to use the internet anonymously, such as **virtual private networks** (VPNs) and proxies, and requires internet providers to block websites that host these services.

According to Russia's Chairman of a parliamentary committee on information policy and communications, it is stated that the new law "only included the restriction of access to information that is already forbidden by law or a court decision." In this regard, the Russian internet regulator Roskomnadzor maintains a blacklist of thousands of websites, which was introduced in 2012 and was originally meant to apply to sites that had content on illegal drugs, child pornography, and suicide. However, a 2013 amendment expanded the blacklist to any content "suspected of extremism," and allows for "flexible interpretation" by the government.

Russia is not the only first country to ban VPNs. China announced a few months ago that it would place restrictions on unauthorized VPNs, and following this development, all VPN apps were removed from China's version of Apple's App Store.