HFN Technology & Regulation Client Update

December 2017

Dear Clients and Friends,

Towards the end of 2017, we are pleased to introduce you to our December edition of the Technology & Regulation Client Update, which includes a significant number of material regulatory, self-regulatory and industry-compliance developments, in the fields of technology compliance, digital advertising, content, eHelath, data privacy and data security. These include the following updates:

- **Starting of blocking "unwanted ads" in Google Chrome;**
- **Expansion of Google Safe Browsing protections to Android;**
- **The EU's Article 29 Working Party additional new guidelines on Binding Corporate Rules, consent, transparency and adequacy referential under the GDPR;**
- **Google Play Policy updates concerning lockscreen monetization, children data and content rating;**
- **Blocking of third-party software injections in Google Chrome;**
- **Apple's revision of its controversial guidelines on template-based apps;**
- **Facebook's new measures against "engagement bait" posts;**
- **Repealing of the Net Neutrality Rule in the US;**
- **The new NAI Code of Conduct for online advertising; and**
- **New self-regulatory guidelines addressing privacy, security and content in mobile health apps.**

Happy New Year,

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, please let us know.

Google Chrome to Start Blocking Unwanted Ads

TOPICS: Adtech Industry Compliance, Ad Blocking, Better Ads Standards, Google Chrome

As reported back in our June update, Google has announced it would take measures across its services in order to block ads and ad formats that are considered by users as annoying or unwanted, as per the standards of the Coalition for Better Ads, with which Google has joined.

Following this, Google has now announced that its **Chrome browser would be blocking ads on websites, which are not complaint with the Better Ads Standards from 15 February 2018**. Violations of the Better Ads Standards will be reported to websites owners via the Ad Experience Report, and site owners can submit their website for re-review once the violations have been fixed. Chrome will remove **all ads** from sites with a "failing" status in the Ad Experience Report for more than 30 days.

We would be happy to provide further advice and recommendations concerning the new standards and blocking measures by Chrome.

Additional Protections added to Safe Browsing for Android Users

TOPICS: App Industry Compliance, Data Collection, Google Safe Browsing, Android

In our pervious updates, we reported on Google's ongoing efforts to strengthen its security features, such as Google's limitations on changing Chrome settings, Google adding new "Unwanted Software Cleanup" features in Chrome and Google Chrome Will Automatically Prevent Webpages from Redirects.

This month, Google announced that their Safe Browsing team has expended enforcement of Google's Unwanted Software Policy to Android devices. Consequently, Google Safe Browsing tool will warn **mobile users** on **apps and on websites leading to apps that collect a user's personal data without their consent**.

Developers of applications that handle **personal user data**, including email addresses, phone numbers or other device data will need to **prompt a message alerting users about such data collection** and provide their own privacy policy in the app as well. Developers of apps that collect user data for **purposes unrelated to the application's functionality will now have to explain prior to collection and transmission of the data how they plan to use it**. Finally, users will need to provide their **consent before** that type of application can be used. Aforementioned **data collection requirements apply to all functions of the app including those that used during analytics and crash reporting**.

These requirements, under the Unwanted Software Policy, apply to apps distributed through Google Play **as well as through other Android app stores** and may result in warnings shown on user devices via Google Play Protect or on webpages that lead to these apps.

We would be happy to provide web and app developers further advice and recommendations concerning the required steps, to ensure compliance of their Apps with Google's Unwanted Software Policy.

The EU's Article 29 Working Party New Guidelines on GDPR

TOPICS: Adequacy Referential, Binding Corporate Rules, Consent, Transparency, Article 29 Working Party, EU General Data Protection Regulation, European Union

The EU General Data Protection Regulation ("**GDPR**") enters into force in May 2018. As part of the implementation period, the EU's Article 29 Working Party ("**WP29**") has **recently issued additional key guidelines addressing various key aspects** of the GDPR (see our report regarding the previous set of guidelines here).

Although the WP29's opinions and guidelines are not binding, since it is an advisory body made up of a representative from the data protection authority of each EU Member State, and includes the European Data Protection Supervisor and the European Commission, these guidelines can assist in understanding how European data protection authorities will interpret various requirements of the GDPR.

The new guidelines include the following:

- Guidelines on **Binding Corporate Rules** ("**BCRs**") for Controller BCRs and for Processor BCRs (adopted and available for public consultation before their final adaption);

- Guidelines on **Consent** (adopted and available for public consultation before their final adaption);

- Guidelines on **Transparency** (adopted and available for public consultation before their final adaption); and

- Guidelines on **Adequacy Referential** (adopted and available for public consultation before their final adaption).

Guidelines on BCRs

BCRs consist of internal rules that allow companies, under the GDPR, to transfer personal data to group entities located outside of the EU. The **Controller BCRs Guidelines** and the **Processor BCRs Guidelines** apply to the transfers of personal data from controllers or processors (respectively), established in the EU to other entities of the same group established outside the EU. These guidelines elaborate on the following key principles that should be covered by the BCRs in order to be approved:

- Binding nature;
- Effectiveness;
- Cooperation duty;
- Description of processing and data flows;
- Mechanism for reporting and recording changes; and
- Data protection safeguards.

Guidelines on Consent

The **Consent Guidelines** specify the key requirements for obtaining data subject's consent and demonstrating it under the GDPR in attempt to assist companies understand and anticipate the authorities' expectations. According to the guidelines, controllers must ensure that the following key elements of valid consent exist when collecting personal information based on consent of the data subjects:

- **Freely given** - individuals must have a real choice; consent is not free where individuals feel compelled to consent, where they will endure negative consequences if they do not consent, or where consent is bundled up as a non-negotiable part of terms and conditions. Moreover, the guidelines analyze some challenges of collecting consent in cases of **imbalance between the entity processing the personal data and the individual, conditionality of consent, granularity, and detriment**;
- **Specific** - consent is specific where the purpose of the processing is explained, the granularity principle is implemented and information related to obtaining consent for data processing activities from information about other matters is clearly separated;
- **Informed** - relevant information must be provided by the companies in clear and plain language and be distinguishable from other matters. The information may be presented in various ways, but it should always be easily understandable for the average person;
- **Unambiguous** - for consent to be unambiguous, it should be given through an active motion or declaration. Therefore, pre-ticked boxes do not constitute unambiguous consent. However, active motions such as swiping on a screen, waiving in front of a smart camera provide a valid consent as it is clear that such motions signify agreement to a specific request;
- **"Explicit" consent** - consent as a legal basis of processing **sensitive data**, consent for an **automated individual decision-making** process or consent for **transferring personal data outside of the EU** must also be "explicit";
- **Demonstrating consent** - controllers should be able to demonstrate that they have obtained a data subject's consent, and they are free to develop their own mechanisms for addressing this requirement;
- **Withdrawal of consent** - individuals should be able to withdraw their consent at any given time, and it should be as easy to withdraw it as to give it.

In addition, the guidelines provide additional notes **on digital consent of children**, according to which controllers must obtain **parental authorization and make reasonable efforts** to verify that the person providing that consent is a holder of parental responsibility. Reasonable efforts may depend on the risks inherent in the processing as well as available technology. In low risk cases, verification of parental responsibility via email may suffice, while in high-risk cases, it may be appropriate to ask for more proof.

Guidelines on Transparency

The **Transparency Guidelines** are aimed to assist controllers in understanding the obligation of transparency concerning the processing of personal data under the GDPR. Transparency applies to how controllers **inform** individuals about their processing activities, how they **communicate** with them about their rights, and how they **facilitate the exercise of these rights**. The key elements of transparency, as analyzed in the guidelines are:

- **Concise, transparent, intelligible and easily accessible** - the information must be presented efficiently and succinctly in order to avoid "information fatigue" and it also should be understandable by an average member of the intended audience. Individuals should not have to seek out the information and it should be immediately apparent to them where this information can be accessed;
- **Clear and plain language** - the information should be concrete and definitive. It is recommended that language qualifiers such as "may", "might", "some", "often" and "possible" should be avoided;
- **In writing or by other means** - the information should be in writing form or included by other means such as pop-ups, 3D touch, privacy dashboards, etc. Electronic means which may be provided "in addition" to a layered privacy notice might include videos and smartphone or IoT voice alerts;
- **The information may be provided orally** - automated oral information may be provided in addition to written means, such as in the context of persons who are visually impaired when interacting with information society service providers;
- **Free of charge** - individuals cannot be charged for obtaining information, and the provision thereof may never be conditional upon goods or services; and
- **Changes in privacy notices** - changes must be actually noticed by individuals by using an appropriate modality specifically devoted to such changes. Additionally, controllers should remind individuals of the applicable privacy notice at appropriate intervals in case of ongoing data processing activities to ensure individuals remain well informed.

Guidelines on Adequacy Referential

According to the GDPR, personal information may not be processed to third countries outside the EU, unless one of the exceptions applies. These include an explicit consent for such processing, processing under binding contractual obligations or as per BCRs, and processing to third countries which were declared by the European Commission as countries with adequate level of data protection laws.

The **Adequacy Referential Guidelines** provide updated guidance to the European Commission for the assessment of the level of data protection in **third countries** and international organizations by establishing the **core data protection principles that have to be present in a third country legal framework** or an international organization, in order to ensure essential equivalence with the EU framework. In addition, the guidelines may assist third countries and international organizations interested in obtaining adequacy.

We would be happy to provide further advice and recommendations concerning the various WP29's GDPR guidelines and their scope. For further details and recommendations published by us on the GDPR, see our update on How to prepare to the new EU General Data Protection Regulation, as well as our recent GDPR Compliance Playbook.

Updates to Google Play Policies on Lockscreen Monetization, Children Data and Content Rating

TOPICS: App Industry Compliance, Monetization, Children's Online Privacy, Privacy, Security, Google Play

Following various updates which were introduced in the recent months, as reported in our previous client updates, Google continues with introducing additional important updates to its Google Play developer policies:

- **Guidance for apps that seek to monetize the lockscreen** - according to the updated policy, **apps that are not developed exclusively for lockscreen purposes may not introduce ads or features that monetize the locked display of a device**;

- **Clarification for program requirements for Designed for Families** - apps that target child audiences are prohibited from using Google API Service that accesses data associated with a Google Account. This new restriction includes Google Play Games Services as well as any other Google API Services using the OAuth technology for or authentication and authorization. Additionally, apps that target both children and older audiences (mixed audience), should not require users to sign in to a Google Account, but can offer this option, for example, Google Sign-In or Google Play Games Services as an optional feature. In these cases, **users must be able to access the application in its entirety without signing into a Google Account**.

- **Content rating guidelines for unrated apps** - Since August 2017, Google Play requires that every app will be rated according to the IARC rating by filling out this questionnaire. According to the revised policy, **any changes to the app content or features that affect the responses to the rating**

questionnaire must be followed by submitting a new content rating questionnaire in the Play Console.

We would be happy to advice on any questions that may arise regarding the updated policies.

Google Chrome Will Stop Third-party Software Injections

TOPICS: App Industry Compliance, Code Injection, Google Chrome

In the past we reported on Google's research regarding ad injections and various steps the company has taken in order to limit the possibility of extensions and other software to inject content to webpages. This month, Google announced that Chrome for Windows will start **blocking third-party software that injects code to Chrome processes**.

Third party software spans from anti-virus scanners and video driver utilities that often inject libraries into running processes to do things like inspect network traffic, to malicious software that can also do the same to spy on users, steal passwords etc. According to Google, Chrome extensions and Native Messaging APIs are modern and safer alternatives to running code inside Chrome processes, and developers are encouraged to use them instead of injecting code from a third party software.

The change will be gradual and start from Chrome 66, due in April 2018, which will begin showing affected users a **warning** after a crash, alerting them that other software is injecting code into Chrome and guiding them to update or remove that software. The next stage will be introduced in Chrome 68, due in July 2018, which will begin **blocking third-party software from injecting** into Chrome processes, but if this blocking prevents Chrome from starting, Chrome will **restart and allow** the injection, together with the warning message. The final stage will come with Chrome 72, due in January 2019, which will block code injection entirely.

The blocking will not apply to accessibility software (such as screen readers), Input Method Editors (used to compose complex scripts, and essential for many Asian languages), and any code that has been signed by Microsoft will continue to be allowed.

Apple Revises its Controversial Guidelines on Template-based Apps

TOPICS: App Industry Compliance, App Store, App Template, Apple

Apple has revised its App Store **guidelines to allow apps built using templates and other app-generation services**. The decision on its previous policy that banned such apps was meant to reduce the number of low-quality apps and spam. However, after many companies had been given a deadline of 1 January 2018 to be compliant with the guidelines or otherwise been removed, an industry concern induced that banning template-based apps as a whole would be an overreach. Such decision would

affect a much wider market — including small businesses, restaurants, nonprofits, organizations, clubs and others who do not have the expertise or funds to build custom apps from scratch.

Apple's new guidance is meant to offer better clarification on what sort of apps will and will not be accepted in the App Store. While according to the revised policy, developers are allowed to use an app template, they have to be the ones to publish the app in the App Store, rather than the app building service. This means that despite the lack of internal expertise, publishers of the app will have to review the App Store documentation and licensing agreement themselves, and more actively participate in the app publishing process.

We would be happy to advice on any questions that may arise regarding the revised guidelines.

Facebook Fights "Engagement Bait" Posts

TOPICS: App Industry Compliance, Engagement Bait, Content, Facebook

The tactic known as "engagement bait" seeks to take advantage of Facebook users' News Feed algorithm by boosting engagement in order to get greater reach. It does so by posting spammy posts that provoke people into interacting with likes, shares, comments etc.

This month, Facebook has announced that it will **begin demoting individual posts from people and Pages that use engagement bait**, and is implementing stricter demotions for Pages that systematically and repeatedly use engagement bait to artificially gain reach in News Feed. Facebook will, however, make some exceptions, and posts that ask people for help, advice, or recommendations such as circulating a missing child report, raising money for a cause, or asking for travel tips will not be demoted.

This announcement is a move to make the content users see in News Feed as more authentic. According to Facebook, publishers and other businesses that use engagement bait tactics in their posts should expect their reach on these posts to decrease. Meanwhile, pages that frequently share engagement bait posts will see significant drops in reach.

FCC Repeals Net Neutrality Rule

TOPICS: Net Neutrality, Internet Service Providers, The Federal Communications Commission, United States

Following heated controversy and protests, the Republican majority of the Federal Communications Commission (the "**FCC**") voted this month to repeal the so-called Net Neutrality Rule, which **restricted the power of internet service providers to influence loading speeds for specific websites or apps**.

The Net Neutrality Rule banned cable and telecom companies from blocking or slowing down any websites or apps and prohibited broadband providers from striking special deals that would give some websites or apps "priority" over others. The repeal reflects the believes of the Trump administration and the new FCC chairman, Ajit Pai, that unregulated business will eventually yield innovation and help the economy.

The repeal was criticized publicly and there have been numerous protests across the US, while several public interest groups promised to file a suit. The Internet Association, the trade group that represents big tech firms such as Google and Facebook, said it also was considering legal action. Critics of the changes state that consumers will have more difficulty accessing content online and that start-ups will have to pay to reach consumers.

It is unclear how much will eventually change for internet users. Major telecom companies like AT&T and Comcast, as well as two of the industry's major trade groups, have promised consumers that their experiences online would not change.

The Network Advertising Initiative Updated Code of Conduct

TOPICS: Adtech Compliance, Online Behavioral Advertising, The Network Advertising Initiative

The Network Advertising Initiative ("**NAI**") released its 2018 NAI Code of Conduct (the "**Code**"). The Code basically merges the 2015 Update to the NAI Code of Conduct with the 2015 Update to the NAI Mobile Application Code, which previously existed as two separate documents, and also includes references to NAI Guidance documents published over the past 3 years, including Cross-Device Linking.

The NAI Code is one of the leading industry self-regulatory codes of conduct governing **online behavioral advertising** and is comprised of Adtech companies that agree to adhere to the initiative's code of conduct, which outlines a series of self-regulatory principles related to **privacy, data governance, data collection and notice and choice**. Some of the notable elements in the Code are:

- The Code imposes **notice, choice, accountability, data security** and **use limitation requirements** on NAI member companies.

- The Code clarifies some existing **terminology**, such as:
  - Personally-Identifiable Information ("**PII**") - refers to the data that is used, or intended to be used, to directly or indirectly identify a particular individual;
  - Device-Identifiable Information ("**DII**") - non-personally identifiable information, that is linked or intended to be linked, to a browser or device or group of devices, but is not used or intended to be used to identify a particular individual;
  - De-Identified Data - refers to data that is not linked to either an individual, browser or device;

  - Sensitive Data - includes specific types of PII that are sensitive in nature, as well as DII related to sensitive medical conditions and sexual orientation.

- The Code collectively refers to "Interest-Based Advertising," "Cross-App Advertising," and "Retargeting" as **"Personalized Advertising**," though it considers each a distinct practice.

- **Transfer Data Restrictions -**
  - **Unaffiliated parties to which members of NAI provide PII for Personalized Advertising** or ad delivery and reporting purposes should adhere to the Code's provisions concerning PII;
  - **All parties to which members of NAI provide DII should be required contractually to not attempt to merge DII with PII to re-identify** the individual for Personalized Advertising purposes without obtaining the individual's opt-in consent.

- **Data Retention** - the Code requires member companies to keep DII or PII used for Personalized Advertising or ad delivery and reporting purposes only, as long as it is necessary to serve their business needs.

We would be happy to advice on any questions that may arise from the updated Code.

New Guidance on Privacy, Security and Content for Mobile Health Apps

TOPICS: EHealth Industry Compliance, Privacy, Security, American Medical Association, Healthcare Information and Management Systems Society, American Heart Association, DHX Group

Xcertia, a group founded a year ago by the American Medical Association, Healthcare Information and Management Systems Society, the American Heart Association and the nonprofit DHX Group, released this month preliminary guidance documents that aim to provide more clarity and self-assessment tools around **operability, privacy, security and content of mobile health apps**.

The set of guidelines include the following:

- **App Operability** - for assessing whether a mobile health app installs, loads, and runs in a manner that provides a reasonable user experience;

- **App Privacy** - for assessing whether a mobile health app protects the user's information, including Protected Health Information (PHI) in full compliance with all applicable laws, rules and regulations;

- **App Security** - for assessing if the application is protected from external threats; and

- **App Content** - for assessing whether the information provided in the mobile health app is current and accurate.

Xcertia will solicit public comments on the guideline content through the end of January 2018. Comments can be submitted through the website.

We would be happy to advice on any questions that may arise regarding the new guidance documents and their scope.