HFN Technology & Regulation Client Update

May 2019

Dear Clients and Friends,

We are pleased to present the latest edition of our monthly **Technology & Regulation Client Update**, which includes a variety of notable regulatory and industry compliance developments in the fields of digital advertising and content regulations, personal data protection, cybersecurity, internet platform compliance policies and more. These include the following:

- **The Interactive Advertising Bureau's Updated Transparency and Consent Framework**;
- The German Data Protection Authorities' guidelines on the applicability of GDPR to telemedia services, including **requirements on cookies and other tracking technologies**;
- A **$3 million fine for HIPAA violations** imposed on a diagnostic medical imaging services company due to the **lack of cybersecurity protocols and mishandle of data breach incident**;
- A Fine of **$100,000 imposed on a company's CEO** for **violation of Canada's Anti-Spam Law**;
- **China's new guidelines for the protection of online personal information**, with new requirements on cybersecurity and the processing of personal information;
- An FTC warning which led to the removal of **dating apps from various app stores over potential COPPA violations**;
- **Facebook's updated policy on Blockchain and Cryptocurrency** advertising, exempting contents from pre-approval process;
- **Google's ban on a Chinese apps developer** and tightening evaluation procedures following the investigation of **abuse of permissions and ad fraud**; and
- **San Francisco's ban on city use of facial recognition technologies**.

Kind regards,

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

IAB Releases Updated Version of its Transparency and Consent Framework

TOPICS: Cookies, Digital Advertising, Transparency and Consent Framework, Interactive Advertising Bureau, GDPR

The Interactive Advertising Bureau (**"IAB"**), in partnership with IAB Tech Lab, has introduced for consultation, new technical specifications for its second iteration of the Transparency and Consent Framework (**"TCF v2.0"**), which is designed to facilitate General Data Protection Regulation (**"GDPR"**) and ePrivacy Directive compliance for ad-tech vendors.

The first version of the IAB Consent Framework, released a year ago in tandem with the entry into force of the GDPR, was designed to standardize requests for consent across the digital ad supply chain, in order to support consent collection, and the transmission and handling of standard and audit trails, including through third party vendors (such as ad servers, DSPs, DMPs and header tags). **The TCF is the largest collaborative effort with organizations and professionals in the digital advertising and publishing industries areas, in order to provide solutions to key GDPR and ePrivacy Directive compliance challenges.**

After the release of the first version, stakeholder feedback has been sought to improve the standards, with Google taking a very active and contributory role in this process, following its 50 million euro penalty for not being sufficiently transparent as to the use of personal information and not obtaining specific consent for ad-targeting purposes under the GDPR. **Google is set to officially integrate the framework as a recognized TCF vendor after the new release.**

In this new version, publishers will gain greater control and flexibility as to how they integrate and collaborate with their technology partners. New "publisher restrictions" will enable them to restrict the purposes for which personal data is processed on a publisher's site by vendors on a per-vendor basis, which will allow publishers to exercise a more "granular" control.

Some of the main changes in the updated framework include:

- The expansion of the original five purposes for processing personal data to a more "granular" 12, with more accommodation being given to the principle of legitimate interests;
- Allowing users to express directly through a TCF Consent Management Platform, their "right to object" to the vendor processing of their personal data, based upon the legitimate interests principle; and
- More controls over whether and how vendors may use certain features of data processing, including the use of precise geolocation data.

TCF also includes technical measures and a set of user interface requirements.

Following the expiration of the public comment period, detailed implementation manuals will be issued for vendors, publishers and CMPs.

We have previously released a Practical Consent Handbook for Websites, Apps and Advertisers, which included analysis and considerations regarding the first version of the TCF.

German Regulators Release Guidelines addressing Cookies and other Tracking Technologies under the GDPR

TOPICS: Data Protection, Cookies, German Telemedia Act, German Data Protection Authorities (DSK), GDPR

The Conference of the German Data Protection Authorities (**"DSK"**) has released Guidelines confirming its view on the applicability of the General Data Protection Regulation (**"GDPR"**) over the German Telemedia Act ("**TMG**"). Under these guidelines, the **DSK reviews possible legal bases under the GDPR for tracking technologies and cookies, explicitly stating that consent is not always required for the use of cookies.**

According to the new DSK's Guidelines, in the interplay between the TMG and GDPR, **the GDPR takes precedence with respect to processing personal information in the provision of telemedia services and, as such, the processing of personal data in connection with cookies and tracking functionalities is only lawful if there is a legal basis under the GDPR**.

According to the DSK, consent is not the only possible legal basis for tracking technologies, since **legitimate interests,** determined by the controller (Article 6 (1) lit. f) GDPR) can also be considered as an adequate legal basis. Examples of where a legitimate interest is a sufficient base for processing, include cases of analytics tools with the sole purpose of analyzing website usage or measuring the range of usage (including, the number of visitor, devices used and language preferences), and for **tools that do not exchange data with third parties**, or **at least do not allow the third party to use the collected information for its own purposes**.

When relying on legitimate interests, a substantial documented balancing test will be necessary, by which the legitimate interest has to be specified and confronted with the interests and freedom of the users. Reasonable expectations of data subjects, opt-out possibilities beyond legal requirements, linking of data, the involved stakeholders and the duration of the tracking, shall also be taken into account as part of such balancing test.

With this context, cookie-banners should only be used for collecting consent if actually required. This is due to the fact that data processing as such, cannot be based on another legal basis, such legitimate interests or – in limited cases – performance of a contract.

Consent, will be required for more invasive tracking tools, such as tracing user behavior in detail, processing of unique identifiers (IP or MAC addresses), relying on hidden pixels or device fingerprinting or which have consequences for content provided to users on other websites, and thereby affecting their right to information. **Moreover, tracking on websites which are health related or may reveal sexual orientation, such as dating platforms, requires consent, as this may involve the processing of special categories of data.**

When consent is needed, the user must be informed in advance of all of the processing activities and recipients of the data, and must be given the opportunity to provide a specific consent to the various forms of data processing. **Users shall be provided with a real choice, based on "granular" consent, and consequently, a general "OK" option will not be sufficient.**

Before users give their consent, all cookies, tools and scripts that collect user data must be deactivated. Tracking may only commence after the user has actively given his/her consent. In order to demonstrate consent under the accountability principle, the storing of information on the user's device without a user-id, will be sufficient.

Finally, according to the DSK, **it must be possible to view a website without consenting to non-essential cookies, which appears to be a partial prohibition on the use of cookie walls**.

The topic of cookies has been widely debated amongst European regulators. In our previous newsletter, we reported on decisions by the Dutch Data Protection Authority, which clarified that cookie walls are not compliant with the GDPR, similar to the UK's Information Commissioner's Office ("ICO") approach in a case involving the Washington Post website. In adopting a different direction, the Austrian Privacy Regulator decided that, in a case where an online publisher offered different options to readers, including the option to refuse cookies and receive full access to the site via an online subscription model that was reasonably priced, having a cookie wall for free access, this would be considered an acceptable practice.

Our previous newsletter also dealt with the topic of the Interplay between the ePrivacy Directive and GDPR, including with regard to cookies, in accordance with the European Data Protection Board guidance.

$3 million Fine to a Diagnostic Medical Imaging Services Company over Cybersecurity Breach

TOPICS: Health Data Protection, Cybersecurity, US Department of Health and Human Services, HIPAA

The US Department of Health and Human Services ("**HHS**") settled a case against Touchstone Medical Imaging ("**Touchstone**"), a Tennessee based company that provides diagnostic medical imaging services in several US States. **The company has agreed to pay a $3 million fine and to implement a robust corrective cybersecurity action plan.**

The investigation was triggered after HHS had received an email alleging that the social security numbers of Touchstone's patients were exposed online via an insecure file transfer protocol (FTP) web server. Following a further investigation, jointly with the FBI, **HHS confirmed that personal health information for Touchstone patients, including some social security numbers, were visible via a Google search**. Uncontrolled access to data permitted search engines to index the personal health information of Touchstone's patients, which remained visible on the Internet even after the server, was taken offline. As a result, **the personal information of more than 300,000 patients was exposed including names, birth dates, social security numbers, and addresses.**

According to the settlement, even after being notified of the breach by the FBI, Touchstone failed to accurately identify and respond to the incident, or to notify the affected individuals. According to the findings of the HHS, **Touchstone also failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities** as to the confidentiality, integrity, and availability of all of its electronic individual data, and in addition, failed to have business associate agreements put in place with its vendors, including their IT support vendor and a third-party data center provider, as required by the Health Insurance Portability and Accountability Act ("**HIPAA**").

Following these findings, Touchstone agreed to a settlement with HHS, under which, in addition to paying the significant fine, the company will undertake **a robust corrective action plan that includes the adoption of business associate agreements, completion of an enterprise-wide risk analysis, and comprehensive policies and procedures to comply with the HIPAA Rules**. This includes steps such as: (i) completion of an inventory of all electronic equipment, data systems, off-site data storage facilities, and applications that contain or store ePHI, which will then be incorporated in its risk analysis; (ii) conducting on an annual basis,

an accurate and thorough assessment of the potential risks and vulnerabilities; and (iii) documenting the security measures implemented in order to sufficiently reduce the identified risks and vulnerabilities.

Touchstone is also required to provide enhanced training materials for its employees, which must be submitted to HHS for its review and approval. Employees must be trained within 14 days of commencing their employment and in all cases, before being provided with access to patient's information.

Finally, Touchstone is required to submit a report on a periodic basis, with respect to the status of, and findings, regarding its compliance, and to maintain records relating to compliance for 6 years, which must be provided to HHS upon request**.**

We would be happy to provide guidance in regard to HIPAA compliance and the necessary breach prevention and governance measures.

CEO Receives a Fine of $100,000 for Company Violation of Canada's Anti-Spam Law

TOPICS: Spam, CASL, Canadian Radio Television and Telecommunications Commission

The Canadian Radio Television and Telecommunications Commission (**"CRTC"**) recently issued penalties of $100,000 against the CEO of a group of businesses known as the "nCrowd" companies. This case represents the **first decision in which an individual has been held liable under the Canadian Anti-Spam Law** (**"CASL"**) for violations committed by a corporation.

The CASL, which **applies if a computer system located in Canada is used to send or access the electronic message**, requires that **commercial electronic messages** must: (i) be sent with consent (express or implied); (ii) clearly identify the sender; and (iii) include an unsubscribe mechanism in the prescribed form. The CASL also provides that individuals can be found vicariously liable for the non-compliance by an organization if such individuals directed, authorized, assented to, acquiesced in or participated in the commission of a CASL violation.

Following over 246 complaints filed to the anti-spam reporting center in 2015, the CRTC began an investigation in relation to email messages that appeared to have been sent by nCrowd companies. All of the messages promoted products or services offered by various merchants via the online sale of corresponding vouchers through nCrowd's platform.

The investigation found that nCrowd's listing contained over 1,928,015 email addresses, most of which were purchased from a third company, Couch Commerce. The list also contained several general email addresses, typically reserved for the technical support and website management of major companies, which, according to CRTC, makes it unlikely that the authorized users of those email addresses would have expressly consented to receiving CEMs from a "daily deals" company.

In this context, **the CRTC determined that nCrowd failed to demonstrate what steps it took, if any, to ensure that it had obtained the express or implied consent to send commercial messages** to the email addresses on its list. nCrowd also failed to provide any document showing the policies and procedures relating to its unsubscribe mechanism.

The CRTC identified that any enforcement actions directed towards such companies would have no deterrent effect, and, as a result, pursued the corporate directors through vicarious liability in order to

encourage future compliance. Given that email distribution lists were central to nCrowd's business, that the CEO was familiar with both their importance and with nCrowd's platform for managing them, and that the CEO was personally involved in acquiring them, the CRTC determined that he must have either known about the problems with nCrowd's lists, or knowingly turned a "blind eye" to them, and was therefore to be held personally liable.

We will be happy to provide further advice on lawful means to send commercial electronic messages, including on how to obtain consent and document proper procedures.

China Issues Guideline for the Protection of Personal Information Online

TOPICS: Data Protection, Guidelines for Protection of Personal Information, China's Cybersecurity Law, Ministry of Public Security

China's Network Security Bureau of the Ministry of Public Security (**"MPS"**), together with the Beijing Network Industry Association and the Third Research Institution of the Ministry of Public Security, have jointly released a Guideline for Protection of Personal Information Online.

Although not a legally enforceable regulation, the Guideline is part of MPS' efforts to implement China's Cybersecurity Law, and **presents new requirements that might be the object of enforcement**. It is still unclear how the Guideline will interact with other existing regulations and national standards, such as China's national standard on personal information protection.

The Guideline applies to both information controllers and processors, and is relevant to internet service providers and organizations, as well as individuals controlling or processing personal information, through either a private network or an offline environment. The Guideline includes an expansive definition of the term **"use of personal information", as referring to any operation of personal information.**

The Guideline requires personal information holders to implement a wide range of internal policies and processes in order to protect personal information, including organizational controls, personnel security measures in terms of hiring, screening and training employees, technical measures for the protection of network infrastructure, such as network segregation, identification and authentication controls, security audits, systems and communication security, and computing environmental controls.

In particular, the Guideline requires encryption protection for the migration process of cloud computing virtual machines, as well as data collection and transmission via "Internet of Things" devices. In addition, the Guideline states that personal information generated and collected by personal information holders in China, must be stored within China and adhere to specific rules if the cross-border transfer of data is necessary. **In the case of a security incident, such as data breach, the Guideline requires that personal data holders shall promptly report the incident to the Ministry of Public Security.**

In terms of business procedures, **the Guideline prohibits the large-scale collection or processing of Chinese citizens' sensitive personal information**, such as race, nationality, political view and religious belief, and specifies that covered entities may only collect and use the summary information of personal biometric information, rather than collecting the original information. Publicly disclosing physiological information (such as biometric information and information concerning genes and diseases) and the analysis of sensitive information (for example, a Chinese citizen's race, nationality, political view or religious belief), is prohibited without exception.

Finally, **the Guideline also creates distinct standards of consent for particular uses of automatically processed user-profiling technology**. As a rule, the users' opt-in is not required but users are entitled to reject or object to such use of their information. However, in cases where the same technology is used for credit rating services, administrative judicial decisions or other value-added applications that may result in legal consequences, the individuals must provide their prior consent.

This is yet another move by China's authorities to implement the Chinese Cybersecurity Law. In our previous newsletter, we also reported on the creation of a national, voluntary security certification scheme for mobile applications.

We would be happy to provide further advice on China´s privacy laws framework and compliance procedures.

Following FTC warning, App Stores Remove Dating Apps over Potential COPPA Violations

TOPICS: Children Data Protection, App Stores, COPPA, US Federal Trade Commission

The Federal Trade Commission ("**FTC**") issued a letter warning to Ukraine-based Wildec LLC, which operates the apps Meet24, FastMeet, and Meet4U, stating that the **three dating apps appeared to be in violation of the Children's Online Privacy Protection Act ("COPPA") and possibly the FTC Act's prohibition against unfair practices.** The apps have been removed from the app stores until they address the alleged violations outlined by the FTC.

Despite a statement in each app's privacy policy that users under 13 years of age are not allowed to use the apps, users who indicate they are under 13 are not prevented from accessing and using the apps or being visible to other users. **Accordingly, in practice, these apps allowed children as young as 12 to access them, even while being aware of the fact that children were using the service**.

In addition, the apps **allowed children to be contacted by other users**, which, according to the FTC, poses a serious health and safety risk. In the letter, it was also stated that several individuals have reportedly faced criminal charges for allegedly contacting or attempting to contact minors using Wildec's apps.

The COPPA requires app providers to give notice and obtain consent from parents before collecting or sharing any personal information concerning children under the age of 13. **Given that Wildec appeared to be aware that children under 13 were using all three of the apps, it was obligated to comply with COPPA's requirements.**

The letter urged the company to immediately remove personal information from children on the three apps, to seek parental consent before allowing minors to access the apps, and to ensure that all versions of the apps comply with COPPA.

The FTC also issued a parent advisory letter urging parents to remove these apps if they are on children's devices, as well as to set children's devices in order that they must obtain parental approval before purchasing any new apps.

This case is part of the FTC's focused enforcement on the protection of children online. In our previous newsletter, we reported that the operators of the video social networking app Musical.ly, have agreed to pay $5.7 million in order to settle a COPPA case, in what is the largest civil penalty ever applied by the FTC in a children's privacy case.

We would be happy to advise our clients in understanding the applicability of, and implications arising from, COPPA, as well as the relevant compliance mechanisms.

Facebook Updates Policy on Blockchain and Cryptocurrency Advertising

TOPICS: Cryptocurrency, Blockchain, Advertising, Social Media, Facebook

Facebook has announced an update to its Prohibited Financial Products and Services Policy, according to which**, ads pertaining to blockchain technology, industry news, as well as events and educational materials for cryptocurrencies, can now be displayed on Facebook without obtaining prior approval.** The company also announced that it will no longer allow ads promoting contracts for difference (CFDs), due to their complexity and the fact that they are often associated with predatory behavior.

This marks a change from last year, when Facebook implemented a policy that required crypto and blockchain advertisers to obtain prior consent before they could run any type of advertisements.

This change, however, will not apply to advertisements that seek to promote a particular cryptocurrency, and consequently, ads for initial coin offerings (ICOs) and binary options remain forbidden. Companies that wish to promote cryptocurrency and closely related products, such as cryptocurrency exchanges and mining software and hardware, will still be required to undergo a review process, involving their pre-approval.

This announcement comes in the wake of Facebook's own plans to launch a cryptocurrency for digital payments system, in approximately a dozen countries, by the first quarter of 2020 (Project Libra). The company has also recently expanded its blockchain division.

Google Bans Chinese Apps Developer and Tightens Evaluation Procedure Following an Investigation on the Abuse of Permissions and Ad Fraud

TOPICS: App Stores, Ad Fraud, Baidu, Google, China

Following a BuzzFeed News report on how a prominent Chinese Android app developer with over 600 million installs was abusing user permissions to engage in ad fraud, **Google has blacklisted 6 apps from the developer and published a blog post outlining a new approach to user permissions** and measures in order to prevent "bad-faith developers".

The findings are part of a wide BuzzFeed News investigation, which analyzed the top Android apps that requested a significant number of permissions, including those assigned as "dangerous" based upon Android's classifications. Last year, BuzzFeed had already reported that two other prominent Chinese Android app developers, Cheetah Mobile and Kika Tech, were abusing user permissions to engage in ad fraud. In this new investigation, BuzzFeed found that at least six of DO Global's apps, which together have more than 90 million downloads from the Google Play store, **have been fraudulently clicking on ads to generate revenue, and at least 2 of them contain a code that could be used to engage in a different form of ad fraud.**

DO Global is a Chinese app developer, spun off from Baidu, one of China's largest tech companies, that claims to have more than 800 million monthly active users on its platforms. BuzzFeed found that 6 of its

apps had taken steps in order to conceal their connections to the developer and **had failed to clearly disclose they were collecting and sending data to China and whether such data was being shared with third parties, such as the Chinese Government.** In addition, some of the apps, such as a selfie app, contained a code that causes it to fraudulently click on ads without the user's knowledge, **including for ads served by AdMob and MoPub**.

According to BuzzFeed, the findings demonstrate *"how Google's Play store, the largest app store in the world, has been exploited by developers who easily conceal their identity from users, offer apps with invasive permissions, and use these permissions to commit ad fraud*". In response, Google has banned the developer's apps from the Play Store and released a blog post stating that the company is working to provide users with more transparency and control, while reviewing the Play Developer policies in order to further enhance user privacy. Google will also be hiring more people to evaluate apps and respond more efficiently to developers' appeals.

These findings follow concerns on IT and Privacy threats coming from China, which led to several discussions regarding cybersecurity and the adoption of a resolution by the EU Agency for Cybersecurity, as reported in our previous newsletter.

San Francisco Bans City Use of Facial Recognition Technologies

TOPICS: Data Protection, Facial Recognition, San Francisco, US

San Francisco is the first city in the US to ban local government agencies' use of facial recognition, following the approval of its Stop Secret Surveillance Ordinance, which was passed by the San Francisco Board of Supervisors in an 8-to-1 vote.

The Ordinance implements a ban on San Francisco city agencies' use of facial surveillance, which tech companies currently sell to various US government agencies**.** According to the Ordinance, "*The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits (…) and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring*".

The Ordinance does not prevent the technology's use at airports and ports, which are federally regulated, and does not imposes any bans or restrictions on the use of such technologies by the private sector. It also allows for private businesses and citizens to share security camera footage, including from tools that use facial recognition tech in conjunction with the police in order to assist in investigations, following certain procedures.

In addition, the Ordinance **requires city agencies to obtain the city's approval before purchasing other kinds of surveillance technologies**, such as automatic license plate readers and camera-enabled drones, **and disclose to the public any such technologies currently in use.**

The ban follows a recent study published by the MIT Media Lab that found the existence of gender and racial bias in facial recognition technologies, and several articles published on the New York Times regarding China's use of facial recognition, as a means for state surveillance and widespread social control.

Although this Ordinance applies to the public sector only, several discussions and rulings regarding the use of recognition technologies in the private sector have been trending. In our previous newsletter, we reported on an Illinois Supreme Court's ruling that an individual does not need to allege or prove actual injury or adverse effect, beyond mere violation of his or her rights, in order to qualify as an "aggrieved" person and be entitled to seek damages pursuant to the Illinois Biometric Information Privacy Act ("BIPA"), which applies to facial recognition technologies.