HFN Technology & Regulation Client Update

September 2018

Dear Clients and Friends,

We are pleased to introduce you to our new edition of the monthly Technology & Regulation Client Update, which includes a variety of notable regulatory and industry compliance developments in the fields of personal data protection, digital advertising, content, data security and app compliance. These include the following:

- **Data protection legislative trend in the US**: the State of California amends the California Consumer Privacy Act and enacts the first IoT Security Bill in the US;
- Google Ads announces a crackdown on **technical support fraud schemes**;
- Apple updates its **App Store** policy to require all apps to post **privacy policies**;
- **Fighting "Fake News"**: Adtech industry giants agree on a voluntary Code on Disinformation;
- **Russia imposes VAT obligations on foreign service providers supplying online services** to recipients based in that country;
- **NIST launches a collaborative Privacy Framework Initiative**;
- **White Hat Hackers may be immune from prosecution** subject to several conditions as set out in the new Israeli State Attorney's guidelines on computer offences;
- **Equifax is fined £500,000** by the ICO concerning a 2017 data breach; and
- Fake reviewer on TripAdvisor is imprisoned in Italy.

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, please let us know

California Legislature Amends the California Consumer Privacy Act

TOPICS: Personal Information, California Consumer Privacy Act, California, United States

In June of this year, the State of California enacted the California Consumer Privacy Act of 2018 ("**CCPA**") giving specific, new rights to California residents relating to their online privacy (see our related update here). Earlier this month, **California's Governor signed law SB-1121** (the "**Bill**"), **amending certain provisions of the CCPA**. Whilst the Bill is designed to address drafting errors, ambiguities, and inconsistencies in the CCPA, it also adds new substantive provisions to the CCPA.

The Bill's key amendments to the CCPA are as follows:

- **Clarification as to the "personal information" definition**: the Bill clarifies that information is considered personal but only if it "*identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household*;"

- **Entities exempted from the CCPA**: some companies are subject to other privacy legislation, such as the Federal Gramm-Leach-Bliley Act, the Federal Health Insurance Portability and Accountability Act ("HIPAA"), or the California Financial Information Privacy Act. In order to avoid a conflict arising for those companies, the Bill clarifies that the relevant entities that are subject to certain specific privacy laws, are not subject to the CCPA. The Bill also clarifies that some clinical trials and healthcare providers covered by the California Confidentiality of Medical Information Act, which supplements the HIPAA privacy requirements, are exempted from the CCPA;

- **Extension in enforcement**: in addressing the privacy requirements of the CCPA, the Bill grants a six-month grace period from the date on which the California Attorney General issues applicable regulations under the CCPA, before enforcement actions can be brought. The Bill also extends the date on which the Attorney General is required to publish implementing regulations, as required under the CCPA, from 1 January 2020 to 1 July 2020;

- **Private right of action**: the Bill clarifies that a private right of action permitted under the CCPA, is granted only for violations of unauthorised access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information. It also requires the consumer to be provided with a written notice of 30 business days and an opportunity to cure any violation, unless the action is being brought solely to claim

pecuniary damages. In addition, the requirement that a consumer bringing a private right of action should notify the Attorney General, is omitted; and

- **Limitation of civil penalty**: the Bill limits the civil penalty of any business that fails to cure any alleged violation within 30 days of being notified of an alleged non-compliance, to $2,500 per violation, or $7,500 for each intentional violation.

We would be happy to advise our clients and clarify the implications arising from this new bill.

Google Ads Plans Crackdown on Technical Support Ads

TOPICS: Digital Advertising, Adtech Industry Compliance, Technical Support, Google

Google has announced that due to the increase in misleading third-party support providers' advertisements, it will implement a verification program in order to validate legitimate providers. This restriction follows the misleading regulatory scrutiny concerning the technical support of products (see our related update here and here), as well as similar restrictions imposed by other companies in the industry. In its announcement, Google noted that last year, it removed more than 3.2 billion ads that violated its advertising policies.

Google's announcement follows an investigation into these scams, which revealed that many fraudsters were exploiting Google's advertising system by impersonating legitimate technical support providers.

Google will begin to implement the restriction on these ads immediately. However, it will take several weeks until fully effected in all languages and jurisdictions. Meanwhile, Google notes that it will continue to take the required means in order to ensure the online advertising ecosystem is a safe place for all users.

California Passes the First IOT Security Bill in the US

TOPICS: Security Standards, Internet of Things, California, United States

The State of California legislature has passed SB-327 Information privacy: Connected devices (the "**Bill**"), **which introduces security requirements for connected devices sold in California. The Bill will come into effect on 1 January 2020**.

"Connected devices" are defined under the Bill as **any device that connects directly or indirectly to the internet and has an IP or Bluetooth address**. This Bill is narrower in scope than the CCPA enacted in June (see our related update above in this Client Update and here).

The Bill requires all manufacturers of connected devices to equip their device with a reasonable security feature, or with features that are:

- Appropriate to the **nature and function** of the device;
- Appropriate to the **information it may collect, contain, or transmit**; and
- **Designed to protect the device and any information contained therein from unauthorised access, destruction, use, modification, or disclosure.**

In addition, if a person is able to log into the device outside a local area network (LAN), the Bill requires this device to have either preprogrammed passwords unique to each device, or technology that generates new authentication credentials before accessing it for the first time, in order to be deemed a reasonable security feature.

We would be happy to provide further advice and recommendations concerning the new security Bill and its implementation.

Apple Requires all App Store Apps to Post a Privacy Policy

TOPICS: Personal Information, Privacy, App Industry Compliance, Apple

In an announcement posted to developers through the App Store Connect portal, **Apple states that it is requiring all new apps and app updates to include a link to their developer's privacy policy in the app metadata, before they can be submitted for distribution on the App Store or through TestFlight external testing**.

The new requirement comes into effect on 3 October 2018. Apple notes that apps will not be automatically removed if they do not include a privacy policy after that date, **as this policy only applies to updates and new app releases. However, any developer that makes changes to an app must ensure it has such a policy.**

Apple has also published a guide for best practice regarding privacy policies, which includes the following recommendations for the apps developers:

- Review **guidelines from governmental or industry sources**, including the Federal Trade Commission's report on mobile privacy, the EU Data Protection Commissioners' opinion

on data protection for mobile apps and the California State Attorney General's recommendations for mobile privacy;

- **Request access to sensitive user or device data** and **explain the reason** why the app needs that data;
- Be **transparent** with users as to how their data will be used;
- Provide settings that allow users to **disable access to certain types of sensitive data**;
- Request and use the **minimum amount of user and device data** for a certain purpose; and
- Take reasonable steps to **protect user and device data**, including storing the data in an encrypted format.

We would be happy to provide further advice and practical recommendations concerning the new policy changes and its implementation.

Fighting "Fake News": Industry Agrees on a Voluntary Code on Disinformation

TOPICS: Digital Advertising, Disinformation, Adtech Industry Compliance, EDiMA Trade Association, European Commission, European Union

In light of the European Commission communication "Tackling online disinformation: a European approach", the advertising and online platform sectors have presented the Code of Practice on Disinformation, which is the first time industry has agreed on a global and voluntary basis, to self-regulatory standards in order to combat disinformation.

According to the European Commission, Facebook, Google, Twitter, Mozilla and some additional members of the EDIMA trade association, are among those that have signed the self-regulatory Code, **which will come into effect within the next month**.

The Code specifies the obligations each signatory should undertake in order to address the challenges related to disinformation. These obligations concentrate on five main areas of action:

- **Disrupting advertising and monetisation incentives for certain accounts and websites that spread disinformation** by, for example, restricting advertising services or limiting paid placements;

- **Political advertising and issue based advertising, being more transparent**, by, inter alia, ensuring that all advertisements are clearly distinguishable from editorial content, including news, and enabling public disclosure of political advertising, which could include identifying actual sponsors and the amounts spent;

- **Addressing the issue of fake accounts and online bots** by putting in place policies regarding identity and the misuse of automated bots on their services and policies, on what constitutes the impermissible use of automated systems, and for this policy to be made publicly available on the platform and accessible to EU users;

- **Empowering consumers to report disinformation and access different news sources, while improving the visibility and findability of authoritative content,** for example, by investing in products, technologies and programs in order to assist individuals in making informed decisions when they encounter online news which might be false and investing in technological means to prioritise relevant, authentic and authoritative information in automatically ranked distribution channels; and

- **Empowering the research community to monitor online disinformation through privacy-compliant access to the platforms' data**, by committing to support independent efforts to track disinformation and to encourage research into disinformation and political advertising.

The new Code also includes an annex identifying best practices that should be applied by the signatories in order to implement the industry's new commitments, including advertising policies, service integrity policies, policies and actions to empower consumers and to empower the research community.

Russia Imposes VAT Obligations on Foreign Service Providers Supplying Online Services to Recipients Based in that Country

TOPICS: Online Service Providers, VAT, Russia

Following recent changes in Russian law, **as of 2019, foreign companies engaged in the provision of B2B online services (including SaaS, PaaS, online advertisement etc.) to Russian customers, may be obligated to register with the Russian Tax Authorities and pay Russian VAT directly to the Russian state budget**.

Russian VAT is often applicable to fees payable by a Russian consumer to a foreign (non-Russian) service provider, regardless of the service provider's foreign residence. However, the liability to pay Russian VAT in these instances usually falls on the Russian customer. The Federal Law of 27 November 2017 No. 335-FZ is about to change this model by **directly imposing Russian VAT duty on the foreign service providers** with respect to the online services provided to Russian customers, where the service fee is payable directly by the

Russian customer to the foreign service provider. The VAT rate for this purpose is 15.25% of the gross amount actually payable by the customer under the contract for the online service.

As of 2018, this duty has been already imposed on foreign service providers offering online services to Russian nationals who are not registered as "individual entrepreneurs" with the Russian tax authorities. As of 2019, this duty shall be extended to **all online services provided to Russian consumers**, including Russian nationals (whether or not registered as "individual entrepreneurs") as well as corporate entities.

The new law includes a broad definition of the term "online services", including various SaaS, PaaS, online advertisement, web hosting, online data processing and storage and other services. The online sale of offline goods or services, the sale of software and databases supplied on a tangible data medium, provision of services via email and internet access services are, on the other hand, excluded from this definition. Additionally, at this stage, software-licensing transactions remain exempt from Russian VAT; however, caution should be exercised in this regard, since the definition of "licensing" under Russian law is significantly narrower than the conventional, Western definition.

The foreign service provider, which does not operate a Russian branch or representative office, is **not** entitled to deduct VAT payable by it, even if it has its own Russian output VAT. The Russian **customer** is entitled to deduct such VAT from its own output VAT, subject to the customer having demonstrated that the service provider has complied with its duty to pay the applicable VAT. Needless to say, this provision is expected to exert pressure on the foreign service providers to comply with their VAT registration and payment duties.

Under the new law, the foreign service provider, which charges the Russian customers directly (i.e. not via intermediaries or agents) for the services being provided, is required to register with the Russian Tax Authorities and subsequently, file an online tax declaration and pay VAT to the Russian state budget. The service providers providing online services to Russian corporate entities or Russian "individual entrepreneurs" **must submit their registrations with the Russian tax authorities by no later than 15 February 2019**. VAT must be declared and paid by **no later than the 25th day of the month following the respective quarter** to the Russian Federal Tax Service.

We would be happy to provide further advice and recommendations concerning these important changes in Russian law and their implementation.

NIST Launches Collaborative Privacy Framework Initiative

TOPICS: Personal Information, Data Protection, Internet of Things, The US Department of Commerce's National Institute of Standards and Technology, United States

The US Department of Commerce's National Institute of Standards and Technology ("NIST") has announced that the launch of a collaborative project to develop a voluntary privacy framework.

The new framework, accompanied by a fact sheet, aims to help organisations identify, assess, manage, and communicate privacy risks, which stem from cutting-edge technologies such as the IoT, given that these technologies expose data privacy to greater risks. The new framework will offer these organisations privacy protection strategies, enabling them to retain their flexibility, while effective solutions for managing risks will remain in place as technologies continue to develop. The framework is also intended to support the organisations' ability to operate under applicable domestic and international regulations.

NIST will also work with industry, civil service groups, academic institutions, federal agencies, governments, standard-setting organisations, and others, conducting extensive outreach through a series of workshops and requests for public comment.

This new framework comes as the National Telecommunications and Information Administration is developing a "domestic legal and policy approach for consumer privacy", in coordination with the International Trade Administration, in order to ensure consistency with international policy objectives.

NIST will be gathering information from stakeholders in order to develop a framework that fits the needs of many different organisations. To collect this information, NIST is holding a series of public workshops, starting on 16 October 2018.

Israeli State Attorney has Published New Guidelines for Dealing with Computer Offences; "White Hat Hackers" Immune in Some Cases

TOPICS: Computer Law, Israeli State Attorney, Israel

Following the proliferation of cybercrimes in recent years, **the Israeli State Attorney has published new guidelines regarding the offence of "unlawful breach of computer material" under the Israeli Computers Law.** The guidelines specify the manner by which prosecutors are required to evaluate the evidence for the offence, the considerations for prosecution, the relationship between this offence and other offences, as well as the considerations for punishment in the case of conviction of this offence.

The guidelines establish a hierarchical severity of acts that constitute a breach of computer material. They explain that **the punishment should be proportionate to the harm caused by the act**, taking into account the potential harm caused by computer offences and the public's dependence on computers. **In this regard, the guidelines state that the offence of "unlawful breach of computer material" can exist even where the attacker does not need to overcome a technological barrier** (such as a password or other means of security), which adopts the Supreme Court judgment in Nir Ezra case.

The guidelines differentiate between three categories of appropriate punishment in terms of sentencing policy considerations.

In addition, the guidelines state that in some circumstances, breach of computer material for a legitimate purpose, may lead to the conclusion that the offender(s) should not be prosecuted. **This extension is relevant particularly for cybersecurity experts who act for the benefit of their organisation, as well for "white hat" hackers. It will apply if the breach was for a legitimate reason, such as for information security testing, where the breach was made in good faith, without any other motive, and without any real examination of the content of the computerised information**.

We would be happy to provide further advice and recommendations concerning the new Israeli guidelines and their implications.

Equifax Fined by ICO Over 2017 Data Breach

TOPICS: Personal Information, Data Protection Act 1998, Information Commissioner's Office, United Kingdom, European Union

The Information Commissioner's Office ("ICO") announced it has issued a £500,000 fine to the credit rating agency Equifax Ltd, for failing to protect the personal information of 15 million UK individuals during a cyber-attack in 2017. **The investigation was carried out under the Data Protection Act 1998**, as the failings occurred before the General Data Protection Regulation came into force.

The ICO found that the UK arm of Equifax failed to take adequate steps to ensure that its US parent company was protecting this data. The ICO stated that Equifax contravened five out of eight data protection principles of the Data Protection Act 1998, including failure to secure personal data, poor retention practices and lack of a legal basis for the international transfers of UK citizens' data.

The ICO stated that the contravention was especially serious for several reasons, including:

- The number of data protection principles that were contravened by Equifax, including significant problems with data retention, IT system patching, and audit procedures;

- The contravention included several systemic inadequacies in Equifax's technical and organisational measures for safeguarding the personal information;

- The organisational inadequacies were significantly problematic in light of the nature of the company, the volume of personal information being processed and the number of data subjects involved;

- Several inadequacies have been in place for a long period without being discovered or addressed by the company; and

- The data breach was not reported to the ICO immediately following detection, but two months after the event.

As a result, Equifax Ltd has received the highest fine possible under the Data Protection Act 1998, flagging the fact that although **the US Department of Homeland Security had already warned the parent company regarding a critical vulnerability during March 2017, insufficient steps were taken to address the vulnerability**.

Italian Jailed over Fake TripAdvisor Reviews

TOPICS: Consumer Protection, User Generated Content, Digital Advertising, Italy

TripAdvisor announced that an Italian court has sentenced a user, who turned out to be a fake reviewer, to nine months in prison, as well as an €8,000 fine, one of the first cases of a fraud review leading to criminal conviction.

The reviewer, the owner of *Promo Salento*, offered the publication of fake reviews to members of the hospitality industry across Italy, in order to raise their profile on the website. When business-owners forwarded the letter they received from him, TripAdvisor blocked more than 1,000 attempts by him to post reviews and filed a report to the police, which found sufficient evidence of criminal conduct to prosecute.

TripAdvisor added that the company now employs a team of in-house investigators searching for paid-review companies, and uses "advanced tracking technology" to analyse information and detect unusual patterns that might indicate that a review is fake. The company strongly

encourages its consumers to report in any case where they are approached or contacted by companies or individuals offering fake reviews.