HFN Technology & Regulation Client Update

October 2016

Dear Clients and Friends,

We are pleased to introduce you to our October edition of the Technology & Regulation Client Update, which includes a variety of industry and regulatory developments in the fields of technology compliance, digital advertising, content, cybersecurity and information privacy regulations. Among these, you can read about:

- The recent updates to **Google Play's developer policies**;
- Enforcement action in the UK against **a telecom company which failed to preclude a cyber-attack**;
- FTC's continuous enforcement focus on **technical support scammers' advertisements**;
- A new CJEU ruling which determined that **dynamic IP addresses can constitute personal data**;
- New regulatory guidelines for **HIPAA-covered entities that use cloud computing services involving ePHI**;
- New regulatory best practice guidelines for **modern vehicles cybersecurity**;
- A new **data breach response guide for businesses**;
- The expected enforcement of **cross-device data collection and use guidelines**; and
- New **privacy and data security rules in the US for ISPs**.

Kind regards,

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

INDUSTRY COMPLIANCE DEVELOPMENTS

Google Play Policy Updated with Reasons for which Apps are Taken Down

Google has updated its Play Store Developer Policy with evident examples of what developers are not allowed to insert into their app listing in the Play Store. These include **sexually explicit material, excessive graphic violence, or use of drugs, plus some "Metadata" app listing items** such as **user testimonials, excessive details, misleading references to other apps or products, and repetitive, excessive or irrelevant keywords.**

Some examples of inappropriate text, images, or videos within developers' listing, are as follows:

- **Imagery or videos with sexually suggestive content**. Developers should avoid suggestive imagery containing breasts, buttocks, genitalia, or other fetishized anatomy or content, whether illustrated or real;
- **Language inappropriate for a general audience**. Developers should avoid profane and vulgar language in their app listing. If it is a critical element of their app, they must censor its presentation within the Play store listing;
- **Graphic violence prominently depicted in app icons, promotional images, or videos**; and
- **Depictions of the illicit usage of drugs**. Even EDSA (Educational, Documentary, Scientific, or Artistic) content must be suitable for all audiences within the Play store listing.

The update demonstrates the company's ongoing enforcement policy against incompliant apps, and calls upon developers to review their app listings and ensure that they do not violate any of the new policies. We would be happy to provide further advice and recommendations concerning the required steps in order to ensure compliance with the applicable obligations and their scope.

NOTABLE LEGAL AND REGULATORY ACTIONS

TalkTalk Fined £400,000 for Failing to Prevent a Cyber-Attack

The UK Information Commissioner's Office (**"ICO"**) issued a record monetary **penalty of £400,000** against the telecoms group TalkTalk, for security failings that allowed a cyber-attacker to access customer personal data of nearly 157,000 customers "with ease".

The ICO issued this penalty against the company for breaching the Seventh Data Protection Principle under the Data Protection Act 1998 (DPA), which provides that: ***"Appropriate technical and organizational measures shall be taken against an authorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"***. The ICO did not find that these conditions had been met since the **minimal level of protection in place and the outdated**

software holding the data, allowed the database to be compromised through a low level cyber-attack. Additionally, **a patch specifically designed to fix this vulnerability had been openly available for over three years and was well-known**. The ICO also criticized the company for **not taking proactive monitoring actions to identify such vulnerabilities**. Such proactive actions could have discovered that the database which was compromised can be accessed via internet-accessible webpages.

Several key points from the ICO's Monetary Penalty Notice that companies should implement, are as follows:

- **Understand your Information technology (IT) infrastructure and data and the risks that relate to that data;**
- **Ensure your security and patching is up-to-date, and be aware of attacks that are happening to other companies;**
- **Identify, respond appropriately to, and learn from actual and attempted cyber breaches**; and
- **Consider your contractual indemnities and limitations on liability relating to data**.

This decision sends a strong message to personal data controllers highlighting the necessity of compliance with data protection principles. As we previously reported, from May 2018, **maximum fines under the General Data Protection Regulation (GDPR) for this kind of breach will be 4% of the group's total worldwide turnover or €20 million, whichever is the greater.**

FTC Charged Tech Support Companies with Using Deceptive Pop-Up Ads

The Federal Trade Commission (**"FTC"**) has recently charged the operators of a multinational tech support company with using deceptive pop-up internet advertisements for the purpose of frightening consumers into purchasing unneeded technical support services for hundreds of dollars. A Federal Court has issued an order temporarily freezing the defendants' practices and assets.

According to the complaint filed by the FTC, **the defendants violated the FTC Act by using affiliate marketers to place internet pop-up advertisements on consumers' computers, deceiving them into believing that the ads originated from Apple, Microsoft, or other legitimate technology companies. These ads allegedly warned consumers about viruses or malware on their computers and prompted them to call a toll-free number for assistance**. Once connected to the number, telemarketers in a call center in India attempted to persuade them to spend anywhere from $200 to $400 for repair services that were effectively useless.

This action by the FTC continues the ongoing enforcement focus on scammers who scare consumers into paying for expansive and unnecessary technical support services and computer repairs (see our previous report on this regulatory trend). **Looking forward, it seems that tech-support scammers will be subject to ever increasing scrutiny from states and federal agencies**.

CJEU Affirmed Dynamic IP Addresses to be Personal Data

The Court of Justice of European Union (**"CJEU"**) issued its judgment in *Patrick Breyer v. Federal Republic of Germany*. In its landmark decision in this case, the CJEU held that **a dynamic IP address constitutes personal data** under Directive 95/46/EC (Data Protection Directive). The CJEU substantially followed the opinion of the EU Advocate General from May of this year (see also our previous Client Update which reported the opinion of the Director of the FTC's Bureau of Consumer Protection in this regard).

The CJEU further held that **dynamic IP addresses qualify as personal data, even if the website operator in question cannot identify the user behind the IP address**, since the users' internet service or access providers (ISPs) are in possession of data which, in combination with the IP address, can identify the users in question.

Following this decision of the CJEU, it is strongly recommended that all relevant operators should review the collection, processing and use of IP addresses in connection with their online operation.

STANDARDS AND BEST PRACTICE GUIDANCE

HHS Published Guidance on HIPAA and Cloud Computing

The US Department of Health and Human Services ("**HHS**") has released guidance for Health Insurance Portability and Accountability Act ("**HIPPA**") covering entities that use cloud computing services involving Electronic Protected Health Information (**"ePHI"**). This guidance assists such entities, including Cloud Services Providers (**"CSPs"**), in understanding their HIPAA obligations.

The guidance makes it clear that **CSPs that store ePHI are business associates according to HIPPA, even if they store only encrypted ePHI and lack an encryption key for the data**. In essence, the same HIPAA analysis applies even if the CSP cannot actually view the ePHI stored on its servers. HHS's guidance also clarifies that **CSPs do not fall within the conduit exception to the HIPAA rules**, since this exception is limited to transmission-only services for PHI, including any temporary storage of PHI which is incidental to such transmission.

Additionally, the guidance explains that the entities and business associates which are covered under this guidance, **may use cloud services to store or process ePHI, provided that the covered entity or business associate enters into a HIPAA-compliant Business Associate Agreement ("BAA") with the CSP**. The BAA **must establish the permitted and required uses and disclosures of ePHI**, and **require the BAA to appropriately safeguard ePHI**, including by implementing the requirements of the HIPAA

Security Rule. The BAA **must also require the CSP to report to the applicable entity or business associate whose ePHI it maintains, as to any security incidents of which it becomes aware**. In addition to a BAA, a Service Level Agreement can be used to address specific expectations, including issues related to HIPAA compliance.

In addition, the guidance **permits health care providers to use mobile devices to access cloud-stored ePHI**, provided that appropriate physical, administrative and technical safeguards, as well as appropriate BAAs, are in place to protect the ePHI's confidentiality, integrity and availability. The guidance also **allows the applicable entities and business associates to use CSPs that store ePHI on servers outside of the U.S.**, while emphasizing that entities using CSPs to maintain ePHI outside the US **should consider the risks associated with the country where the cloud server is located**. Moreover, the guidance notes that, pursuant to the HIPAA Security Rule, **CSPs are directly liable for failing to safeguard ePHI, as well as for any impermissible use or disclosure of ePHI**.

HHS's guidance includes several other common questions and answers relating to cloud computing and how it may affect the applicable entities or business associates as to how they handle and maintain ePHI security.

NHTSA Published Best Practice Guidelines for Modern Vehicles Cybersecurity

The US Department of Transportation's National Highway Traffic Safety Administration (**"NHTSA"**) released new guidance as to **how automakers should approach cybersecurity** amid growing scrutiny prompted by high-profile vehicle hacks and the spread of **car connectivity technologies**. The guidance focuses on layered solutions to ensure that vehicle systems shall take appropriate and safe actions, even when a cyber-attack is successful.

The cybersecurity guidance recommends, inter alia, **risk-based prioritized identification and protection of critical vehicle controls and consumers' personal data**. Furthermore, it recommends that **companies should take into consideration the full life-cycle of their vehicles and facilitate rapid response and recovery from cybersecurity events**.

NHTSA's guidance also recommends **the industry self-audit and consider vulnerabilities and exploits that may influence their entire supply-chain of operations**. Moreover, it also recommends **employee training to educate the entire automotive workforce regarding new cybersecurity practices and to share lessons learned with others**.

It should be noted that the Best Practice guidelines are non-binding and follow earlier guidance for automakers concerning self-driving vehicles, which was recently reported in our last Client Update. Despite this, NHTSA's guidance stresses the importance of making cybersecurity a top leadership priority for the automotive industry.

The FTC Released a Guide for Businesses on Handling Data Breaches

The FTC has issued a guide for businesses on **how to handle and respond to data breaches**. This guide outlines the **steps businesses should take once they become aware of a potential data breach**.

Among the key steps in the new guide are **securing physical areas, cleaning up businesses' websites, and providing breach notification**. It also emphasizes the need for **cyber-specific insurance** towards offsetting potentially significant response costs.

If companies' service providers were involved in the data breach, then companies need to ensure that the **service providers have rectified all vulnerabilities** and consider **whether they need to change their access privileges**. Additionally, **companies should check their network segmentation** such that a breach by one server or site does not lead to a breach in another.

The guide also underscores the significance of a **notification of a breach** and emphasizes that **notification should be made to individuals, other affected businesses, regulators and law enforcement, taking into account all applicable state data breach notification laws and federal regulations**. Moreover, the FTC's guide highlights the need for expedient notification which will enable affected parties to take steps in order to secure their information as soon as possible, and **provides a sample data breach notification letter in this regard**.

We will be happy to provide further advice and recommendations concerning the required steps a company should take in order to be properly prepared for a data breach event.

REGULATORY AND LEGISLATIVE DEVELOPMENTS

The DAA to Begin Enforcing Cross-Device Data Guidelines Next Year

The Digital Advertising Alliance (**"DAA"**) has recently announced that **it will begin enforcement of its cross-device guidance**, titled Application of the DAA Principles of Transparency and Control to Data Used Across Devices on 1 February 2017 (see our previous related report).

The cross-device guidance outlines how the existing **Transparency and Consumer Control principles** contained in the DAA's Self-Regulatory Principles for Online Behavioral Advertising and Multi-Site Data and Guidance on the Application of Self-Regulatory Principles to the Mobile Environment, **apply to the collection and use of information from the same user across multiple browsers or devices**. Under the DAA's Guidance, a user's choice to opt-out of online behavioral advertising on a particular browser or device prevents: data collected from that browser or device from being used on other linked devices for online behavioral advertising (and vice versa); and the transfer of data collected from the opted-

out browser or device for online behavioral advertising.

In practical terms, this requires both of the first-parties (e.g., websites and mobile apps) and third-parties (e.g., advertising technology companies) to reveal cross-device tracking practices in their privacy policies, as well as providing "enhanced notice" of such practices through clear, meaningful, and noticeable links outside of the privacy policy. The DAA's cross-device guidance also requires that the opt-out choices made available to consumers for interest-based advertising must also stop cross-device targeting on the device from which the consumer has opted-out.

Accordingly, companies that engage in cross-device tracking and targeting should make sure that they are compliant with the DAA's cross-device guidance. **Failure to comply with the guidance could result in an Accountability Program enforcement action**.

We will be happy to provide further advice and recommendations concerning the required steps to ensure compliance with the applicable obligations and their scope.

The FCC Approved Broad new Privacy and Data Security Rules for ISPs

The Federal Communications Commission (**"FCC"**) has adopted new privacy and data security rules related to Internet Service Providers (ISPs). We previously reported as to the FCC's initial proposal in this regard, which was widely criticized by internet providers and other firms from the industry as being inconsistent with data privacy standards applicable to the rest of internet service providers.

The adopted rules include, inter alia, the following requirements for:

- **Clear notification regarding the collection, use and sharing of consumer information**, including providing a persistent notice in an online privacy policy;
- **Opt-in consent for any use or sharing of "sensitive information**", which the proposal defines as including **geo-location, children's information, health information, financial information, social security numbers, web browsing history, app usage history and content of communications**;
- An **opt-out for the use and sharing of non-sensitive information**;
- **Strong protections for the use and sharing of de-identified information**;
- **Prohibition of "take-it-or-leave-it" offers requiring consent to data sharing and use** that are unnecessary to provide the service, as a condition of obtaining the service;
- **Heightened notice requirements for discounts and other incentives** in exchange for consumers' express affirmative consent to the use and sharing of their personal information to the extent that is unnecessary to operate the service, and **restrictions on pricing services for those who do not consent**; and
- The new rules also refer to the inclusion of **data security requirements** based on FTC and National Institute of Standards and Technology (NIST) cybersecurity frameworks and a **harm-based data breach notification rule**.

Several marketing industry groups have expressed concern over the potential impact of the updated rules, given that customers' web browsing and app use history has traditionally been subject to an opt-out consent requirement only. Nevertheless, by a 3-to-2 vote, the FCC has approved the new privacy and data security rule and **broadband providers will have approximately 12 months to make the changes required by the new rules**.