HFN Technology & Regulation Client Update

March 2017

Dear Clients and Friends,

We are pleased to introduce you to our March edition of the Technology & Regulation Client Update. The past month has been marked by a variety of regulatory and compliance developments in technology compliance, digital advertising, big data, content, privacy and information security regulations. In this edition of our Client Update, we have concentrated on updating you regarding some of the key developments in these areas, which apply to a number of important regulatory and technological issues. Among these, you can read about the following updates:

- Google's extended enforcement measures against **unwanted software and malware targeting macOS devices,** as well as its new **safeguards for advertisers**;
- The measures Google and Facebook have taken to ease advertisers' concerns, including **MRC audit**;
- The update to Facebook's and Instagram's policies which now **prohibits developers from using platform data for surveillance tools**;
- FTC's enforcement actions regarding **inadequate disclosures regarding data collection and use**, and **online marketing schemes**;
- The New York Attorney General's settlements with three **mHealth app developers for misleading marketing and irresponsible privacy practices**;
- A new CJEU ruling regarding **the "right to be forgotten" in company registers**;
- The UK ICO's enforcement action concerning **sufficient due diligence when buying and using marketing databases**;
- The UK ICO's new guidance on **consent under the impending EU GDPR regime**;
- The final **cybersecurity regulations for institutions providing financial services in New York State**;
- The abolition of the **FCC's privacy rules for broadband providers**; and
- The new **Israeli data security regulations**.

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.

Google is Expanding Protection for Chrome Users on MacOS

TOPICS: App Industry Compliance, Unwanted Software, Google Safe Browsing, Google Chrome, MacOS

Google has recently expanded the scope of Safe Browsing policy protections to macOS devices, enabling safer browsing experiences by improving defenses against **unwanted software and malware targeting macOS.** As a result, macOS users might begin to see more red warnings pages when they navigate to sites with content or files which are considered as unwanted under Google's policies.

Before the change, Google enforced its unwanted software policy in Chrome for PCs only. The new Safe Browsing initiative aims to reduce macOS-specific malware and unwanted software by focusing on two common abuses of browsing experiences: **unwanted ad injection, and manipulation of Chrome user settings, specifically the start page, home page, and default search engine.**

Additionally, from now onwards, the Settings Overrides API **will be the only approved path for making changes to Chrome settings on Mac OSX**, as currently exists on Windows. Furthermore, Google notes that **only extensions hosted in the Chrome Web Store are allowed to make changes to Chrome settings.**

This change will be effective on 31 March 2017, with Chrome and Safe Browsing warning users about software which attempts to modify settings without using the proper API.

Google Expanded Safeguards for Advertisers in Response to an Ad Boycott

TOPICS: Adtech Industry Compliance, YouTube

Google has recently announced expanded safeguards for advertisers on YouTube and the Google Display Network. Google's announcement apparently was in reaction to a growing ad boycott by major brands and government departments in the UK. The boycott was prompted by ads being embedded within and alongside "hate videos" uploaded to YouTube.

The new safeguards are focused on the company's **ad policies, its enforcement of the policies and new ways for advertisers to exercise control where their ads are placed by Google's automated system.**

Google stated that it was taking **a tougher stance on hateful, offensive and derogatory content**. This includes **removing ads more effectively from content that is attacking or harassing people based on their race, religion, gender or similar categories**. The company also stated that it planned to **tighten safeguards in order to ensure that ads are shown only against legitimate creators in its YouTube Partner Program** - as opposed to those who impersonate other channels or violate its community guidelines. Additionally, Google stated said **it would not stop at taking down ads**. The company clarified that the YouTube team is taking a hard look at the existing community guidelines in order to determine what content is allowed on the platform—and not just what content can be monetized.

Another major change Google announced earlier this month, **gives increased control to advertisers on how and where ads should be placed.** Google stated that it was **changing the default settings for advertisers** in order that they will have broader latitude in describing the kind of content they consider objectionable and wish to exclude from consideration for ad placement. The company also stated that it would **introduce new account-level controls** that will allow advertisers to exclude specific channels and websites from all their campaigns across all Google properties with just one click of a button. Additionally, Google stated that it would introduce new controls to make it easier for brands to **exclude higher risk content and fine-tune where they wish their ads to appear**.

Finally, Google stated that it would offer advertisers and agencies **more transparency and visibility on where their ads are running**, and in the coming months it would **expand availability of video-level reporting** to all advertisers. Moreover, the company said it would also **hire a significant number** of individuals and **develop new tools** for boosting its ability to review questionable content for advertising.

Facebook and Instagram Banned Developers from Using Their Data for Surveillance

TOPICS: App Industry Compliance, Facebook, Instagram

Facebook, which owns Instagram, has recently announced that it had updated Facebook and Instagram platform policies to state that **developers cannot use data obtained from the platform to provide tools that are used for surveillance**.

The social network company also stated that over the past several **months, it has taken enforcement action against developers who created and marketed tools intended for surveillance, in violation of its existing policies**.

These recent changes in the companies' policies, follow an investigation by the American Civil Liberties Union of California (ACLU) which discovered how developer Geofeedia used Facebook, Twitter and Instagram data to assist U.S. law enforcement agencies in the surveillance of individuals during protests.

Google and Facebook Agreed to an MRC Audit to Ease Advertisers' Concerns

TOPICS: Adtech Industry Compliance, Media Rating Council Audit, Google, Facebook, Snapchat

Google announced last month that it agreed to a series of audits for its video website YouTube by the media industry's independent measurements watchdog, the Media Rating Council (**"MRC"**).

Since 2015, Google has completed integrations with several independent metrics companies to enable third-party viewability reporting on YouTube. These integrations offer advertisers additional choice for

measuring viewability on YouTube, alongside Active View. Last month, Google stated that each of these integrations would undergo a **stringent, independent audit for MRC accreditation**. The audit would validate **data collection, aggregation and reporting for served video impressions, viewable impressions, related viewability statistics and General Invalid Traffic (GIVT) across desktop and mobile,** for each integration adhering to MRC and Interactive Advertising Bureau (IAB) standards.

Additionally, Google stated that it planned to have the **MRC audit data for ads on non-Google sites purchased via two key Google ad buying tech platforms—DoubleClick Bid Manager and AdWords**.

Less than two weeks before Google's announcement, Facebook disclosed a number of new accountability developments in a blog post, the most significant of which is **a commitment to an audit by the MRC to verify the accuracy of the information it delivers to marketing partners**.

According to a recent report on The Wall Street Journal, **Snapchat is under pressure from ad buyers to follow suit and have its ad metrics audited by the MRC**.

For your convenience and ease of reference, here are the links to MRC's guidelines regarding Mobile Viewable Ad Impression Measurement, as well as Viewable Ad Impression Measurement.

The NY Attorney General Settled with Mobile Health App Developers for Misleading Marketing and Privacy Practices

TOPICS: Privacy Regulatory Enforcement, e-Health, Misleading Marketing, New York, United States, Food and Drug Administration

The New York Attorney General has recently announced settlements with three **popular health-related applications** (Matis Ltd., Runtastic GmbH, and Cardiio, Inc.) sold in Google Play and Apple's App Store **concerning misleading claims and irresponsible privacy practices**.

The Attorney General's investigation disclosed that two app developers argued that their apps accurately measured heart rate after vigorous exercise, using only a smartphone camera and sensors. A third developer contended that its app transformed a smartphone into a fetal heart monitor and thus could be used to play an unborn baby's heart rate, even though the app was not approved by the US Food and Drug Administration ("**FDA**") as a fetal heart monitor. **The three developers initially marketed these apps without possessing sufficient information to support their marketing assertions**, but have since cooperated with the Office of the Attorney General to alter their advertising, consumer warnings, as well as privacy practices.

Under the settlements, **the developers agreed to provide additional information regarding the testing of the apps, to change their ads in order to make them non-misleading, and to pay $30,000 in combined penalties to the Office of the Attorney General**. In Addition, **the developers now post clear and prominent disclaimers informing consumers that the apps are not medical devices and are not**

approved by the FDA.

Moreover, the developers have also made modifications in order to **protect consumers' privacy**. The developers now **require affirmative consent to their privacy policies for these apps and to disclose that they gather and share information that may be identifying individuals**. This includes **users' GPS location, unique device identifier, and "deidentified" data which third-parties may be able to use to re-identify specific users**.

The FTC is Combatting Online Marketing Schemes

TOPICS: Adtech Regulatory Enforcement, Online Marketing, Federal Trade Commission, United States

The US Federal Trade Commission ("**FTC**") has recently charged a group of online marketers with deceptively luring consumers with "free" and "risk-free" trials for cooking gadgets, golf equipment, and access to related online subscription services. As alleged by the FTC, **the defendants asked people for their credit card information to cover shipping and handling, and then charged them for products and services without their consent**.

According to the FTC's complaint, the defendants' websites, TV infomercials and emails deceived consumers by prominently claiming that their products and services were free, **without expressly disclosing that they would begin charging consumers if they did not cancel their "free trial" or return the "free" products**. Additionally, the defendants misrepresented their return, refund and cancellation policies. In particular, the defendants **buried these terms in pages of fine print which the recipients could only reach through a tiny hyperlink.**

Furthermore, during the purchase process, the defendants signed consumers for more "free" trials after **forcing them to click through as many as 14 upsell pages to reach a final confirmation page**. According to the FTC's complaint, a large part of those pages included poorly disclosed, or undisclosed, additional "free trials" which resulted in yet more unauthorized charges.

The FTC Settled with a Membership Reward Service over Inadequate Disclosures

TOPICS: Data Protection Regulatory Enforcement, Disclosures, Federal Trade Commission, United States

A membership reward service named Upromise, which was directed at consumers trying to save for college, **will pay a $500,000 civil penalty** to settle allegations that it violated the terms of an FTC order requiring the company **to make disclosures about its data collection and use and to obtain third-party assessments of its data collection toolbar**.

Following the order from 2012, Upromise encouraged consumers to download a toolbar named RewardU. The FTC's order required Upromise to make clear and prominent disclosures regarding RewardU's data collection and use, and to obtain third-party assessments and certifications of the

toolbar describing specific safeguards and their effectiveness in protecting consumers' personal information. In a civil penalty complaint filed on the FTC's behalf by the Department of Justice, the FTC alleged that Upromise failed to comply with both provisions of the 2012 FTC order.

Under a stipulated order announced earlier this month, Upromise must not violate the order from 2012 and **must pay a $500,000 civil penalty**. Before launching a future toolbar, it **must ensure that a third-party professional specializing in website design and user experience** will certify Upromise's adherence to the **order's disclosure and "express, affirmative" consumer consent requirements**. In addition, Upromise **must obtain advance written approval from the FTC of any required assessment's scope and design**. Moreover, **it must permanently expire RewardU-related cookies from consumers' computers and notify those consumers how to uninstall the toolbar and any associated cookies**.

The UK ICO Fined a Local Company for Buying and Selling Non-Compliant Marketing Databases

TOPICS: Data Marketing Due Diligence, Information Commissioner's Office, United Kingdom

The UK Information Commissioner's Office ("**ICO**") has **fined** **a company £20,000 for not exercising sufficient due diligence when buying and using marketing databases**.

Under the monetary penalty notice which was sent to the company, the ICO held that data controllers purchasing lists **must check how and when consent was obtained, by whom, and what the customer was told. It is not acceptable to rely on the assurances of indirect consent without undertaking proper due diligence**. Such due diligence might, for instance, include checking the following:

- How and when was consent obtained?
- Who obtained it and in what context?
- What method was used – e.g. was it opt-in or opt-out?
- Was the information provided clearly and intelligibly? How was it provided – e.g. behind a link, in a footnote, in a pop-up box, in a clear statement next to the opt-in box?
- Did it specifically mention texts, emails or automated calls?
- Did it list organizations by name, by description, or was the consent for disclosure made to any third-party?
- Is the seller a member of a professional body or accredited in some way?

The ICO also held that companies **cannot sell marketing lists if they do not maintain clear records of individuals' consent to marketing – stressing that both the provider and recipient of data can be held to have breached UK data protection laws**.

In addition, the ICO held that since the data was used for direct electronic marketing, **the company was not entitled to rely on its data sources' generic consent requests, but** rather, in order to be compliant with the UK privacy regulations, marketing consent requests **must specifically name the party which sends the communication.**

The CJEU held that the "Right to Be Forgotten" could not be generally applied to Company Registers

TOPICS: The Court of Justice, European Union, Court Ruling, The Right to Be Forgotten

The Court of Justice of the European Union ("**CJEU**") has recently considered **whether the "right to be forgotten" should be applied to a register of companies**. The CJEU had previously held that the right to be forgotten might apply to the processing of personal data by search engines in a case from 2014 (see our previous related report).

In its recent judgment (*Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), the CJEU ruled that **the "right to be forgotten" could not in general, be applied to a company's register, though it did suggest that there may be some very limited circumstances where limitations might be imposed on access to personal data held on such a register**.

This CJEU's judgment derived from a court case initiated by an Italian person. A company of which he was a director had been unable to sell properties in a tourist complex. **In his view, this was due to his local company register which disclosed that he had been the administrator of another company that went bankrupt in 1992 and was wound up in 2005**. He challenged, before his local courts**, the availability of his personal data**, which referred to the CJEU the question of whether he was entitled to seek limitations upon access to his data.

The UK ICO Published New Guidance on Consent under the EU GDPR

TOPICS: General Data Protection Regulation, European Union, Information Commissioner's Office, United Kingdom

The UK ICO has recently released draft guidance for UK organizations on **how the notion of consent will be interpreted and applied when the GDPR comes into force in May 2018**, and called for comments on the guidance (for further details and recommendations on the GDPR, see our related special client update, which we have recently published). The public consultation expired on 31 March 2017. **The ICO is expected to issue a final version of the guidance in May 2017**.

The ICO guidance, among other things, highlights the following modifications to the consent requirements (as the ICO interprets them):

- The GDPR sets a high standard for consent, and the ICO expects a **significant change to the companies' consent mechanisms**;
- The GDPR is clear that an **indication of consent must be unambiguous and involve a clear affirmative action**;
- The GDPR requires consent to be **separated from other terms and conditions**. It should not generally be a precondition of signing up for a service;

- The GDPR specifically **bans pre-ticked opt-in boxes**;
- The GDPR requires **granular consent for distinct processing operations**;
- The GDPR requires organizations **to maintain clear records to demonstrate consent**;
- The GDPR provides a **specific right to withdraw consent**, **and requires organizations to notify individuals of their right to withdraw consent** and **to offer easy ways to withdraw consent at any time**;
- Public authorities, employers, and other organizations having a position of power over individuals whose consent they are seeking, are **likely to find it more difficult to obtain a valid consent**; and
- Organizations need **to review existing consents and their consent mechanisms** in order to check whether they meet the GDPR standard. If they do, there is no need to obtain any new consent.

This is the ICO's first topic-specific guidance on the GDPR, with **guidance on contracts and liability expected later this year**. **More guidance is also expected from the Article 29 Working Party**, which intends to publish guidance on such topics as **transparency, certification, breach notification and data transfers**, which will supplement their previous guidance on Data Portability, Data Protection Officers and the One Stop Shop (see our previous related report).

The GDPR will require organizations to reevaluate their approach to obtaining consent and using consent as a basis for data processing. 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. On 25 May 2017, we will be hosting at HFN a **special workshop** - just one year before the GDPR enters into force - **in which we will discuss the practical aspects of GDPR compliance, including with respect to the new consent requirements**.

The NYDFS Released Final Cybersecurity Regulation

TOPICS: Cybersecurity Regulation, Department of Financial Services, New York, United States

The New York Department of Financial Services ("**NYDFS**") has recently announced the release of its finalized cybersecurity regulation, which has **become effective since 1 March 2017**. The final version contains a few material revisions from the proposed regulation issued by the NYDFS in late December 2016, which superseded the original proposed regulation published by the NYDFS in September 2016 (see our previous related report).

The final regulation requires **banks, insurance companies, and other financial services institutions** regulated by the NYDFS to **establish and maintain a cybersecurity program** designed to **protect consumers' private data** and ensure the safety and stability of New York's financial services industry.

The final risk-based regulation includes **certain regulatory minimum standards**, while encouraging companies to keep pace with technological advances. The final regulation also provides **significant protections to prevent and avoid cyber breaches**, including the following:

- Controls relating to the governance framework for **a robust cybersecurity program,** including requirements for a program that is adequately funded and staffed, overseen by qualified

management, and reported on periodically to the most senior governing body of the organization;
- Risk-based minimum standards for **technology systems including access controls, data protection including encryption, and penetration testing**;
- Required minimum standards to help address any **cyber breaches including an incident response plan, preservation of data to respond to such breaches, and notice to NYDFS of material events**; and
- **Accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to NYDFS**.

This cybersecurity regulation is likely to have substantial implications far beyond New York State and the regulated entities that are directly subject to the NYDFS's enforcement authority. Given that there are many financial institutions which will be required to comply with these new requirements, **other regulators, clients, customers and counterparties might begin to view them as a baseline standard for cybersecurity in the financial industry**.

The US Congress Voted to Revoke FCC's Privacy Rules for Broadband Providers

TOPICS: Broadband Providers, Privacy Regulations, Federal Communication Commission, United States

The US Senate has recently voted to revoke the new broadband provider privacy regulations, which were approved by the Federal Communication Commission ("**FCC**") in October last year (see our previous related report). The vote passed 50 to 48 along party lines, with Republicans in favor of the repeal and Democrats against.

The most notable part of the rules, which has not yet become effective, **required broadband providers to obtain explicit consent before sharing consumers' web-browsing data and other personal information with advertisers**.

The House of Representatives has supported the Senate's resolution, which aims to roll back FCC's privacy rules for broadband service providers, and voted 215-205 to overturn a yet-to-take-effect regulation. President Donald Trump is expected to sign the Bill into law, according to a White House statement.

New Disclosure Requirements for Native Advertising in Australia

TOPICS: Advertising Regulations, Native Advertising, Marketing Communications, Australia

The Australian Association of National Advertisers ("**AANA**") has announced that a new provision, which requires **advertising and marketing communications to be clearly distinguishable to the relevant audience**, will be inserted into the AANA's Code of Ethics, with **effect from 1 March 2017**.

The AANA has also published a Best Practice Guideline for Clearly Distinguishable Advertising to assist

advertisers in understanding their new disclosure obligations. The new Guideline indicates that the Code will only apply to advertising and marketing communication where the following two key criteria are met: the marketer has **a reasonable degree of control over the material**; and the material **draws the attention of the public in a manner which is calculated to promote a product or service**.

The Guideline also provide that **contextually targeted branded content, integrated content and native advertising** might be included within the definition of "advertising and marketing communication" under the Code.

Advertisers will have flexibility as to how to ensure that material is distinguishable as advertising or marketing communication. **They might use logos or brand names combined with other visual or audio cues where appropriate, such as background shading, outlines, borders, graphics, video or audio messages depending on the medium**.

In addition, a consumer will be able **to lodge a complaint** to the Advertising Standards Board (**"ASB"**) if they consider that advertising or marketing material is not clearly distinguishable to the relevant audience.

The AANA states in its Guideline that in determining the relevant audience of an advertising or marketing communication, the ASB might consider: **the content** of the advertising or marketing material; material that might be provided by the advertiser to the ASB in response to a consumer complaint, including **classification material, audience measurement data, and the media placement plan**; **data from audience measurement suppliers**; and in the case of social media, **the opt-in nature of the medium and the age-gating** which might apply to some social media sites.

Although it will be necessary to assess content on a case-by-case basis, the key to ensuring compliance with the new disclosure requirements is **to adopt a policy of disclosure** where any content is commercial in nature.

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

New Landmark Data Security Regulations Promulgated in Israel

TOPICS: Data Security Regulations, Data Breach Notifications, Israel

The Israeli Parliament (The Knesset) has recently promulgated **extensive data security regulations**, titled Protection of Privacy Regulations (Data Security), after more than seven years since a first draft of the regulations was released under the Israeli Law, Information, and Technology Authority (ILITA) for public comments. **The Regulations will come into effect in late March 2018**.

The new regulations include a comprehensive **set of detailed requirements for anyone who owns, manages or maintains a database containing personal data in Israel (including both data controllers**

and data processors in Israel's public and private sectors), which is based on four separate levels of **information security governance**: databases **maintained by individuals**, databases subject to the **basic level** of data security requirements, databases subject to the **intermediate level** of data security requirements, and databases subject to the **high level** of data security requirements.

The regulations set out data security requirements concerning, inter alia, the following: **a database specification document; a data security officer; data security protocols; database's computer systems mapping; risk assessments; physical and environmental security; personnel training; access permissions; authentication; access monitoring; documentation of information security incidents; portable devices; segregation of systems; systems updates; communication security; outsourcing; periodic audits; retention of security records; backup and recovery; encryption; data breach notifications; and penetration tests.**

The new data security regulations will undoubtedly require a significant degree of compliance for companies operating within Israel, as well as having an effect on regional and multinational companies which gather data on Israeli citizens.

Asia House, 4 Weizmann St., Tel-Aviv 6423904, Israel | Tel: (972)-3-692-2020 | Fax: (972)-3-696-6464
Twitter: @hfnlaw | Blog: unfolding.co.il | hfn@hfn.co.il | www.hfn.co.il