HFN Technology & Regulation Client Update

Google, Facebook, Microsoft and Twitter Introduce Open-Source Platform Promoting Universal Data Portability

TOPICS: Data Portability Personal Data, General Data Protection Regulation, Google, Facebook, Microsoft, Twitter

Google, Facebook, Microsoft and Twitter recently announced a new initiative: a Data Transfer Project (DTP), which is an open-source data portability platform to which any online service can join using APIs.

The project enables users to transfer their data directly between different services without needing to download and re-upload it.

The project was announced in the wake of the General Data Protection Regulation ("**GDPR**") entering into force, which included the right of data subjects to request that their personal data be ported between different services, encouraging businesses to develop interoperable formats that enable this type of data portability.

Services joining the project are required to implement robust privacy and security standards in order to safeguard against unauthorised access, diversion of data, or other types of fraud**,** as well as to inform users of the types and scope of data being transferred, how the data will be used, and the privacy and security practices of the destination service.

The existing code for the project is an available open source consisting of adapters able to convert a range of proprietary APIs into an interoperable transfer.

Currently, the project supports data transfer for photos, mail, contacts, calendars and tasks. It is based on publicly-available APIs from Google, Microsoft, Twitter, Flickr, Instagram, Remember the Milk and SmugMug. While data may already be transferred by other means, the platform is designated to become a more robust and flexible alternative to existing conventional APIs.

Recent Developments in US Privacy Legislation

TOPICS: Personal Data, Privacy, Data Security, Data Brokers, California, Colorado, Vermont, US

In tandem with global attention focused upon tightening data protection issues, **several US states have recently adopted new privacy laws that aim to protect consumers' privacy**. These laws reflect a different approach to privacy and security regulations in the US, **with more of an affinity to the European GDPR regime.**

California Enacts a New Data Privacy Law

California has passed The California Consumer Privacy Act of 2018 ("CCPA"), granting consumers greater control over the use of their personal information online. The CCPA grants consumers **broad notice, access and deletion rights concerning their personal information**. In addition, the CCPA requires businesses to provide consumers with the same quality of services as those who have opted out of the sale of their personal information. The **CCPA also makes it easier for consumers to sue companies in the case of a data breach**.

The CCPA will take effect on January 1, 2020, and will apply to any organisation conducting business in California that either has annual gross revenues in excess of 25 million dollars, or that annually handles the personal information of 50,000 or more consumers, households, or devices, or that otherwise derives 50 percent or more of its annual revenues from selling consumers' personal information.

The key provisions of the CCPA include the following:

- **Expanded definition of personal information**: the new definition includes names, IP addresses, account names, commercial information such as purchasing or consumption histories and records of personal property, internet browser and search history, geo-location data, educational information and professional information.

- **Disclosure of personal information collected**: consumers now have the right to request that any business collecting their personal information shall disclose:
  (1) the categories of personal information it has collected about that consumer;
  (2) the categories of sources from which the personal information is collected;
  (3) the business or commercial purpose for collecting or selling this information;
  (4) the categories of third parties with whom the business shares it;
  (5) the specific items of personal information the business has collected about that consumer.

- **Deletion of personal information**: consumers now have the right to request that a business that has collected personal information from them will delete it, subject to several exceptions.

- **The right to opt out**: businesses may not sell personal information without giving notice and the opportunity for affected consumers to "opt out" by placing a link on their website homepage titled "Do Not Sell My Personal Information". That link should redirect to a webpage that enables a consumer to "opt out" of the sale of its personal information. The consumers shall have the right to "opt out" at any time.

- **Violation**: The California Attorney General may enforce the CCPA's provisions. Violations of the CCPA carry penalties of up to USD 2,500 per violation and up to USD 7,500 for intentional violations. In addition, the CCPA creates a private right of action by California residents in connection with data breaches resulting in the exfiltration, theft or disclosure of a consumer's non-encrypted or non-redacted personal information and providing for statutory damages of between USD 100 to USD 750 per incident.

Colorado's New Data Privacy Law

Colorado has passed a new breach notification law, titled Protections for Consumer Data Privacy ("HB 18-1128").

The new law imposes **stricter requirements on businesses that collect, process and store electronic or paper copies of personal identifying information ("PII") of Colorado residents.**

The HB 18-1128 will come into effect September 1, 2018. It requires businesses to maintain a policy for the disposal of documents containing consumer data and notification of Colorado residents of any security breaches involving their data within 30 days of its occurrence.

The key provisions of HB 18-1128 include the following:

- **Expanded definition of PII**: Colorado's previous legislation defined "PII" as a combination of a Colorado resident's first name or first initial and last name with their social security number, driving licence number. The amended definition of "PII" now also includes the following elements: student, military, or passport identification number; medical information; health insurance identification number; and biometric data. The new PII definition extends to include a Colorado resident's username or email address, in combination with a password or security questions/answers permitting access to an online account.

- **Breach notification requirements**: a business must notify in the event of a likely security breach.

Unless the investigation concludes that misuse of personal information is unlikely to occur, the notification must be made no later than 30 days of discovery, and if more than 500 Colorado residents are affected, the state's Attorney General must also be notified.

The notification must include certain minimum information, including the date of the security breach, the types of PII that may have been affected and any appropriate steps an affected individual may or should take to protect the information. In addition, in cases where more than 1,000 Colorado residents have been affected, the business is also required to notify all consumer-reporting agencies that compile and maintain files on consumers nationwide.

- **Documentation and retention requirements**: the HB 18-1128 includes a specific requirement for businesses to have a written policy which requires them to destroy or arrange for the destruction of such documents when they are no longer needed.

- **Protection of PII**: businesses must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the PII and the nature and size of the business and its operations. In addition, businesses must also require any third-party service provider with access to PII to take measures to protect such information.

Vermont Passes First U.S. Law to Regulate Data Brokers

Vermont has passed a new law, titled H.764, an act relating to data brokers and consumer protection ("the Law"), becoming the first state in the US that has enacted legislation regulating data brokers.

The Law, which will come into effect on January 1, 2019, requires data brokers to develop and implement a comprehensive security programme that shall include administrative and technical safeguards to protect personal information.

The Law defines "data brokers" as businesses that collect and sell or licence data about consumers with whom the business does not have a direct relationship. The Law excludes from that definition businesses that collect information from their own customers, employees, users or donors, and businesses that provide services for consumer-facing businesses and maintain a direct relationship with those consumers.

The Law includes the following key obligations for data brokers:

- **Annual Registration**: the Law requires data brokers to register annually with the state of Vermont and provide information about their data collection activities, "opt-out" policies, purchaser credentialing practices, and security breaches.

- **Freedom from Monetary Deterrents:** credit-reporting agencies are required to offer consumer credit security freezes and unfreezes, free of charge. In addition, a consumer requesting a freeze should receive a PIN, a password, or other authentication method for dealing with the credit-reporting agency regarding the freeze.

- **Duties to Protect Personally Identifiable Information:** the Law requires data brokers to develop, maintain, and implement a security programme to protect personally identifiable information, which should include administrative, technical, and physical safeguards. The Law provides a list of minimum requirements, such as management of access to personally identifiable information, adoption of security policies and management of third-party vendors.

We would be glad to advise our clients and clarify the far-reaching implications arising from this new US privacy legislation.

Facebook has Reversed its Blanket Ban on Cryptocurrency Ads

TOPICS: Adtech Industry Compliance, Cryptocurrency, Binary Options, Initial Coin Offerings, Facebook.

Facebook has reversed its ban on cryptocurrency advertising, only six months after the company updated its policy to ban all cryptocurrency ads (see our related report from January 2018). The blanket ban on crypto-related ads appeared necessary to Facebook at the time in order to make it harder for scammers to profit from a presence on Facebook and to protect its users from illegitimate promoters.

While Facebook continues to prohibit ads that promote binary options and initial coin offerings (**ICO**s), **its new policy, published in late June 2018, allows advertisers to fill out an application form in order for Facebook to be able to assess their eligibility for promoting crypto products.**

Such advertisers are required to provide information about any licences they have obtained, whether they are traded on a public stock exchange, and other relevant public background on their business.

We will be happy to provide further advice and recommendations concerning the new Facebook policy.

Google Play Updates Developer Programme Policies

TOPICS: App Industry Compliance, Cryptocurrency, Child Protection, Google Play

Google Play introduces several changes to its Developer Policy Center, as part of the company's effort to create a positive experience for its developers and customers.

The main changes, which will apply to any new apps as well as to new versions of existing apps, include the following:

- **Child Endangerment:** apps that include content that sexualises minors will be immediately removed from the store. In addition, in the event that Google Play discovers content with sexual abuse imagery, it will report it to the relevant authorities.

- **Cryptocurrency:** Google Play prohibits apps that mine cryptocurrency on devices unless they remotely manage the mining of cryptocurrency.

- **Sale of Dangerous Products**: this new policy prohibits the sale of explosives, firearms, ammunition, or certain firearms accessories.

- **Spam:** Google Play has updated its spam policy, stating that the company does not allow apps that provide the exact experience as other apps that already exist on Google Play (such as apps that copy content from other apps). In addition, the spam policy now includes a restriction on apps the primary purpose of which is to serve ads, such as apps in which interstitial ads are placed after every user action.

- **Misrepresentation**: this new policy includes a prohibition on apps or developer accounts that impersonate others, misrepresent or conceal their ownership or primary purpose.

We would be happy to advise on any questions that may arise regarding these updated policies.

England and Wales Court of Appeal Ruling in Favor of Data Subject Access Requests for Mixed Personal Data

TOPICS: Court of Appeal, Data Subject Request, Right of Access, General Data Protection Regulation, Data Protection Act, Medical, United Kingdom

The England and Wales Court of Appeal published its recent decision in DB v GMC [2018] EWCA Civ 1497, concerning the handling of a data subject access request ("SAR") under data protection laws, where the request is targeted at information that contains a third party's personal data ("mixed personal data").

The background of the case is as follows: the General Medical Council ("**GMC**") investigated a doctor who allegedly failed to diagnose a patient's cancer in the time and should have done so. The GMC commissioned a medical report in relation to the patient's claim, and the patient submitted a request to disclose the full report.

The request to receive access to the report was treated as a SAR (subject access request) under the UK Data Protection Act 1998. However, the doctor filed for an injunction against the disclosure of the report, claiming that the requested information contained the doctor's personal data and as such, its disclosure would infringe upon his privacy rights. In addition, the doctor argued that the request be rejected since it was being requested for litigation purposes.

The High Court previously determined that in cases of SARs relating to "mixed personal data" (essentially, information that contains personal data of a third party), the absence of the third party's consent to disclosure leads to a presumption against disclosure. In addition, the High Court stated that the fact that the request has been made for litigation purposes, rather than to protect privacy, was a weighty factor against disclosure.

The Court of Appeal overturned the High Court decision, holding that it was an error to state that in cases of "mixed personal data" there is a rebuttable presumption against disclosure; instead, the starting point should be one based on reasonableness.

In addition, **the Court of Appeal held that the High Court had erred in stating that where the sole or dominant purpose of the request is obtaining information for the purpose of litigation, that would be considered a weighty factor in favor of a refusal of the SAR.** The Court held that there is no general principle that the interests of the person requesting information, when balanced against the interests of the objector, should be treated as devalued by reason of a motivation to pursue litigation.

Furthermore, the Court of Appeal stated that in general, **data controllers have added discretion regarding relevant factors to the balancing requirement and the weight to be given to each factor they treat as relevant**.

Although the decision was made in light of the previous data protection legislation, it is also relevant under the GDPR regime.

We will be happy to provide further advice and recommendations concerning the far reaching implications of this court decision in light of the GDPR.

Google Announces a "Measurement Partners" Programme to Provide Advertisement Measurement Solutions

TOPICS: Digital Advertising, Adtech, Better Ads Standards, Google

Google is launching a new "Measurement Partners" programme, as part of its focus on improving transparency in advertisement data tracking.

In its announcement, Google stated that as the customers' "journey" becomes more complex, the measurement has become increasingly challenging. For this reason, **the Google Measurement Partners is aimed at assisting marketers obtain accurate and trustworthy measurements. It gathers a group of verified partners across certain specialisations in order to help advertisers ensure that their ads are delivered in brand-safe environments, including in terms of visibility, reach, brand safety, brand lift, sales lift, app attribution, and marketing-mix modeling**.

The Measurement Partners programme currently gathers more than 20 verified companies that have worked closely with Google, to meet precise standards in order to provide measurement solutions. Some of the partners include ComScore, Ekimetrics, Tune, Adjust, Oracle Data Cloud, Nielsen, Innovd and Sizmek. **Google has also mentioned that it works closely with those partners in order to ensure their solutions respect users' privacy**.

FTC Settles with California Company over False Privacy Shield Claims

TOPICS: Federal Trade Commission, EU-U.S. Privacy Shield framework, General Data Protection Regulation, Federal Trade Commission Act, US.

The Federal Trade Commission ("**FTC**") has reached a settlement with ReadyTech Corporation, an online training services company (the "**Company**") for falsely publishing that it was in the

process of being certified for complying with the EU-U.S. Privacy Shield framework (Privacy Shield).

According to the FTC's complaint, the Company set out privacy policies and statements regarding its practices on its website, **including statements that argue that the Company is in the process of certifying its compliance with the Privacy Shield.**

While the Company did indeed initiate an application to the U.S. Department of Commerce for Privacy Shield certification, **it did not, however, complete the necessary steps for obtaining this certification**. By doing so, the FTC found that **the Company had violated Section 5(a) of the Federal Trade Commission Act, which prohibits deceptive acts or practices.**

The settlement agreement provides, in part, that the **Company is prohibited from further misrepresentation of its participation in any privacy or security programme, which is sponsored by the government or any self-regulatory or standard-setting organisation,** including the Privacy Shield.

The FTC announced that this is the fourth case it has brought enforcing the Privacy Shield, demonstrating its commitment to its enforcement, as **the FTC believes Privacy Shield is a critical tool for ensuring the protection of international data transfer and privacy**.

CRTC Fines Two Companies for Aiding in the Installation of Malicious Online Advertising

TOPICS: Canadian Radio-television and Telecommunications Commission, Canadian Anti-Spam Law, Malicious Computer Programmes, Canada

The Canadian Radio-television and Telecommunications Commission ("CRTC") announced that it has taken enforcement actions against two companies for the installation of malicious computer programmes through the distribution of online ads, without obtaining the consumers' express consent, in breach of Canada's anti-spam law (the "Act").

The CRTC sent notices of violation to each of the companies, Datablocks Inc. ("**Datablocks**") and Sunlight Media Network Inc. ("**Sunlight Media**").

The CRTC found that both companies had provided technical means for the installation of malicious computer programmes through the distribution of online ads. In addition, Sunlight Media actively promoted services for the installation of malicious computer programmes, formed business relationships with clients that are known for facilitating such practices, and

adopted various practices which permitted and encouraged a high degree of anonymity (such as using cryptocurrency payment methods).

In addition, while the companies were alerted by the Canadian Cyber-Incident Response Center, they did not put appropriate safeguards in place to prevent the prohibited acts: by way of example, the companies did not have written contracts with their clients which requiring them to comply with the Act, and did not put any monitoring measures or compliance policy in place to ensure compliance with the Act.

As a result of these violations, **the CRTC imposed administrative monetary penalties of $100,000 against Datablocks and $150,000 against Sunlight Media**.