HFN Technology & Regulation Client Update

October 2018

Dear Clients and Friends,

The past month was notable in terms of the extent of regulatory and industry developments in the fields of data privacy, cyber security, digital advertising, content and app compliance. In this edition of our monthly Technology & Regulation Client Update, you will find the following:

- California's and Twitters' measures concerning **bots and Election Integrity**;
- The first and significant **enforcement action under the GDPR** by the UK's ICO;
- **Expansion by the Securities Authorities in their cyber-security** related supervision;
- Various **regulatory and industry codes and guidelines on blockchain**;
- The relaxation of some of Google's and Facebook's prohibitions on **cryptocurrency advertising**;
- Data and content related updates to **Chrome Web Store and Google Play policies**;
- **Significant settlements concerning a number of data breach incidents**;
- New guidance in Europe on **Geo-Blocking Regulation**;
- The coming into force of the new Canadian **Mandatory Breach Reporting Rules**; and
- The UK's Code of Practice for **consumer IoT security**.

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, let us know

California and Twitter Introduce Measures for Election Integrity

TOPICS: Bots, Election Integrity, Twitter, California, United States

A new Bill, which bans the use of undeclared bots during elections ("the Bill"), has been signed by the Governor of California.

A "bot" is defined under the Bill as an **automated online account** in which all actions or posts, or at least most of them, are not carried out by a person. The Bill makes it **illegal to use a bot to communicate or interact online with another person in California with the intent to mislead that person with respect to its artificial identity in order to: (1) incentivise a purchase or sale of goods or services in a commercial transaction; or (2) influence a vote in an election.**

A person using a bot is excluded from the Bill, if that person discloses that it is a bot. The disclosure must be clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts.

The new Bill is set to take effect on 1 July 2019, and does not impose a duty on service providers of online platforms that have 10,000,000 or more unique, monthly, United States visitors or users for a majority of months during the preceding period of 12 months.

The new Bill follows Twitter's reports regarding Russian-controlled bots that were very active during the 2016 United States Presidential election. **Twitter, on its part, is taking steps to protect election integrity ahead of the Midterm Elections, which will take place this November. The platform has announced an update in its work regarding Twitter's "election integrity" project**, which includes several major changes to its site rules and policies.

The main changes to the Twitter Rules include the following:

- **Fake accounts**: in order to overcome manipulation tactics through an evolving platform, Twitter has expanded the rules concerning fake accounts. Twitter may now remove fake accounts which engage in a variety of emergent, malicious behaviour;

- **Attributed activity**: Twitter has expanded the company's enforcement to include accounts that deliberately mimic or are intended to replace accounts which have already been suspended for violating Twitter's rules; and

- **Distribution of hacked materials**: Twitter has expanded its rule such that its review teams will now ban accounts that claim responsibility for a hack, make hacking threats, or issue incentives to hack specific people and accounts.

First Enforcement Action under the GDPR by the ICO

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

An enforcement notice filed by the Information Commissioner's Office ("ICO") against AggregateIQ Data Services Ltd ("AIQ"), a Canadian data analytics firm, has been revealed by a data protection specialist. **This is the first formal enforcement action under the General Data Protection Regulation ("GDPR")** and the UK Data Protection Act 2018.

Although the enforcement action was not published on the ICO's website, it was mentioned in the ICO's report: "Investigation into the use of data analytics in political campaigns". **In the report, AIQ has been associated with the Facebook-Cambridge Analytica scandal as a provider of software and tools for the management of data**, which were intended for use in voter targeting and processing personal data on behalf of UK political organisations, such as "Vote Leave" and "BeLeave".

According to the enforcement notice, although the entity is not established in the EU, as its processing activities are related to the monitoring of data subjects' behaviour that took place within the EU, AIQ is subject to the GDPR. In this regard, the ICO found that AIQ had violated Article 5(a)-(c), and Article 6 of the GDPR, since it processed personal data unbeknown to the data subjects, for undeclared purposes and without a lawful basis for such processing. In addition, the ICO stated that AIQ had failed to provide the transparency information, as required under Article 14 of the GDPR.

The enforcement notice stated that the Commissioner has considered whether the breach has caused (or is likely to cause) any personal damage or distress to a person, and found that this is likely to occur as a result of data subjects being denied the opportunity to understand which personal data is being processed and for what purpose, and not being effectively in a position to exercise their rights as data subjects.

Accordingly, the Commissioner required AIQ to cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise for the purpose of data analytics, political campaigns or other advertising purposes. If AIQ fail to comply with these terms within 30 days, they will be fined up to €20 million, or 4% of an undertaking's total annual worldwide turnover, whichever is the higher.

Securities Authorities Expand Cyber-Related Supervision

TOPICS: Cyber Security, The US Securities and Exchange Commission, The Israeli Securities Authority

SEC Cautions Public Companies to Consider Cyber Threats When Implementing Internal Accounting Controls

The Securities and Exchange Commission ("SEC") has issued a press release and an investigative report, which **caution public companies to consider cyber threats when implementing internal accounting controls**. The report is based on the SEC's investigation into whether nine public companies who were victims of cyber-related frauds, had violated the Securities Exchange Act of 1934 due to insufficient systems with respect to their internal accounting controls.

The investigations focused on **business email compromises** ("email phishing"), which involved fake emails from persons purporting to be company executives or vendors, prompting their personnel to transfer large sums to bank accounts controlled by the perpetrators.

Although the SEC decided not to pursue enforcement actions against those public companies, the report emphasises the risks and threats under which the capital market and companies operate, and to which all industries are subject, due to cyber-attacks. **The report states that public companies should pay more attention to the obligations under the Act, which require them to maintain internal accounting controls that reasonably safeguard the company from cyber-related frauds**. According to the SEC, having sufficient internal accounting controls is an important role in a company's risk-management approach to external cyber-related threats, and, ultimately, in order to protect investors.

The Israeli Securities Authority Requires Companies to Include Cyber Threats in Filings

The Israeli Securities Authorities ("ISA") has published a new Staff Position concerning cyber-related disclosures. In its Staff Position, the ISA stated that cyber-attacks are a significant threat to the ability of companies to evolve, as well as causing loss of income, potentially leading to significant loss from which the company might be unable to recover.

Accordingly, the ISA now requires relevant companies to include information regarding cyber-attacks and potential cyber threats potentially affecting the company's performance in their fillings to the Stock Exchange, shareholders and their board of directors..

The document does not create new discovery obligations under the Israeli securities regulations but rather, emphasises the requisite attention against cyber-threats and defines conceivable threats or events under the law.

New Regulatory and Industry Guidelines on Blockchain Technologies

TOPICS: Blockchain, Privacy, The United States' National Institute of Standards and Technology, General Data Protection Regulation, French Data Protection Authority, The Interactive Advertising Bureau's Tech Lab

NIST to Publish its Final Report on Blockchain Distributed Ledger Technology

The United States' National Institute of Standards and Technology ("NIST") has issued a final version of its interagency report on blockchain-distributed ledger technology. The Blockchain Technology Overview provides a high-level overview and explanations, inter alia, on how blockchain works, the characteristics of this emerging technology that has enabled the development of several cryptocurrency systems, the blockchain components and consensus models, and its application processes, known as **smart contracts**. As explained by NIST, the report is designed as an introduction to provide the foundation for a **planned series of publications on more specific aspects of blockchain**.

The report highlights some of the limitations and misconceptions of blockchain technology in order to prevent organisations from incorrectly incorporation. These misconceptions include the following:

- **Immutability**: Although the blockchain is usually described as immutable, there are different ways in which **the concept of immutability for blockchain ledgers can be violated**. For instance, for some blockchain implementations, some blocks are subject to being replaced by a longer chain with different "tail" blocks;

- **Cybersecurity**: The use of blockchain does not remove inherent cybersecurity risks, and as a result, a **robust cybersecurity program is still required** in order to provide protection from cyber threats. A common misconception is that blockchain is so secure, that once a transaction is committed to the blockchain it cannot be changed. However, this fact is not necessarily true when it comes to transactions that have not yet been included in a published block within the blockchain; and

- **Users involved in blockchain governance**: According to the report, another misconception is that blockchain networks lack control and ownership. In fact, this claim is not strictly true since, for example, **authorised blockchain networks are generally set-up and run by an owner or consortium**, who governs the blockchain network.

According to the report, blockchain technology solutions can be relevant to activities or systems that require features such as numerous participants; a need for a decentralised naming service; or a need for cryptographically secure system ownership.

CNIL Publishes Initial Guidance on Blockchain and GDPR

The French Data Protection Authority, CNIL, has published an initial assessment regarding the blockchain and the GDPR, becoming the first data protection authority to provide solutions to the challenges that arise from the potential conflict between blockchain technology and data subject rights under the GDPR.

The CNIL states that the GDPR applies to the use of blockchain **in any instance where personal data is handled**. However, the GDPR has excluded distributed ledger technology (DLT) solutions from the scope of the assessment, considered too "rare" to allow CNIL to carry out a generic analysis; and private blockchains, given that they do not raise particular GDPR issues that are relevant to the public blockchains and consortium blockchains.

The CNIL's assessment include several key issues as follows:

- **Controllers and Processors within the meaning of the GDPR**: CNIL distinguishes between: (i) those who have permission to write on the chain ("Participants") and (ii) those who validate transactions and create blocks according to the blockchain rules ("Miners"). A Participant who decides to submit data for validation by Miners, is considered a **data controller** when the Participant is an individual; the processing is linked to a commercial activity; or the Participant is a legal entity and writes personal data on the blockchain. **Data processors** may be "smart contract" developers, which process personal data on behalf of the Participant; or Miners, which validate transactions on behalf of participants.

- **Minimisation of risks to data subjects**: As part of the principle of 'Privacy by Design' under the GDPR, data controllers must consider in advance **whether blockchain technology is appropriate** for the implementation of their data processing activities. **In this regard, the** CNIL recommends the controller adopt a different technological solution where possible.

  In addition, since the blockchain contains the credentials of Participants and Miners, as well as additional data entered to the transaction, and which may relate to another individual, and where such data cannot be minimised, the **retention period** of such data must necessarily correspond with the lifetime of the blockchain. With respect to the additional data, CNIL recommends the use of solutions where personal data is processed outside the blockchain or on the blockchain, if it is cryptographically protected.

- **Data subject's rights**: In its assessment paper, the CNIL raises a concern regarding **the ability to ensure the right of "erasure"**, as it is technically impossible to delete data stored on the blockchain. Accordingly, the CNIL recommends the use of encryption in order to delete the data as far as possible**.**

- **Security requirements**: The CNIL recommends determining a **minimum number of Miners** to avoid collusion attacks, implementing organisational and technical measures in order to limit the impact of a possible failure in transactional security due to an algorithm (as well as to ensure confidentiality), and in addition, **documenting the governance of the evolution of the software used to create a transaction and to mine**.

IAB Tech Lab to Publish a Pilot for Blockchain-Based Protocol that will Simplify Consent Management

The Interactive Advertising Bureau's (IAB) Tech Lab has announced that it has launched a pilot version of PrivacyChain, a blockchain-based protocol developed by LiveRamp. The aim of this protocol is to simplify consent-management across complex supply chains and to assist publishers and advertisers in building more trusting relationships with their customers. The current version is now available for public comment.

The protocol's aim is to assist companies in managing and controlling how they handle and share users' personal data. The use of blockchain, in this case, effectively provides a shared, immutable and distributed ledger, which ensures all of PrivacyChain's participants have a single, consistent and up-to-date view of a consumer's opt-ins or opt-outs. As a result, companies will be able to build more trusting relationships with their customers. **The protocol will also enable them to easily demonstrate compliance with several privacy regulations worldwide, including the GDPR.**

Google to Allow Certain Cryptocurrency Advertising

TOPICS: Adtech Industry Compliance, Cryptocurrency, Google, Facebook, United States

Google has announced it will resume accepting cryptocurrency-related online advertising after banning such ads in March (see our related report here). The new policy was updated in October and **allows regulated cryptocurrency businesses to advertise on Google's platform. This means that the ban on initial coin offering ("ICO") related posts will still be in effect.**

Google's updated policy applies to advertisers all over the world, with the exception that the ads can **run only in the US and Japan**, and interested businesses will have to apply for a **certification** to serve ads in each country on an individual basis, once the new policy comes into effect.

Google's move follows Facebook, which announced that it has reversed its June ban on certain types of crypto-related ads , having introduced it in January (see our related update here). However, Facebook stated that **ads promoting binary options and ICOs remain prohibited**. Facebook's updated policy requires advertisers wishing to run ads for

cryptocurrency products and services, to submit an application in order enabling Facebook to assess their eligibility. Facebook stated that it will "listen to any feedback" and if necessary, revise its policy over time, as it continues to "study" this technology.

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

Updates to Chrome Web Store and Google Play Policies

TOPICS: Browser Extensions, Chrome, Mobile App Industry Compliance, Google

Google Announces Changes to Its Chrome Web Store to Improve Extensions Experience

Google has announced several changes as to how its Chrome browser handles extensions that request numerous permissions, as well as new requirements for developers who wish to publish their extensions in the Chrome Web Store. These changes are part of the company's work in order to make Chrome extensions safer (see our related update regarding Google's previous update of disabling inline installations here).

The upcoming changes include user controls for **host permissions**; **new code readability requirements** (developers of extensions in the Chrome Web Store with obfuscated code are asked to review Google's content policies as well as Google's recommended minification techniques and submit a new compliant version before 1 January 2019); and in addition, **2-Step verification requirements** for developer accounts.

In addition, beginning with the new version of Chrome (v70), **extensions that ask for extensive permissions will be subject to a more comprehensive review process**. Google will also begin monitoring extensions with a remotely-hosted code in order to quickly detect malicious changes. In this regard, Google requests that the extension's permissions (sought by the extension developers), have as narrow a scope as possible.

Google Play Updated Policies

Google Play has updated several policies as follows:

- **Google's Enforcement section has been updated, and offers a better explanation regarding the extent of Google's policy coverage and actions that will be taken against policy violations, in which it is stated that if an app violates any of Google's policies, it will be removed from Google Play**. In cases of repeated or serious violations of Google's policies or the Developer Distribution Agreement, an individual's or related account will be terminated;

- **Malicious Behaviour policy: this policy has been updated to clarify the prohibition on surveillance and commercial spyware apps**. Inter alia, it prohibits all kinds of malicious software, such as viruses and Trojan horses; apps that link to the distribution or installation of malicious software; and apps or SDKs that download executable code from a source other than Google Play. The only exception to this prohibition is policy-compliant apps, which are exclusively designed and marketed for parental monitoring or enterprise management, provided they comply with Google's requirements, and do not present themselves as spyware or secret surveillance solution and do not hide tracing behaviour;

- Both 'Designed for Families Program' requirements and Primarily Child-Directed Declaration guidelines have been updated to include **a prohibition on the misrepresentation of the participating apps and their target age group**; and

- User Data and Permissions policies have been updated to include **restrictions on Call Log and SMS permission usage**;

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

Significant Fines and Settlements Over Data Breaches

TOPICS: Data Breach, Consumer Protection, Privacy, Data Security, Electronic Protected Health Information, Health and Human Services' Officer Rights, The UK Information Commissioner's Office, Health Insurance Portability and Accountability Act, Uber, Anthem, Facebook, United States, United Kingdom

ICO Issues a maximum £500k Fine to Facebook over Cambridge Analytica Data Breach

The ICO has confirmed that **it has fined Facebook £500,000 for serious breaches of data protection law following the Cambridge Analytica case in March** (see our related report here). **This fine represents the maximum allowable punishment under the laws applicable at the time of the incidents**.

According to the ICO's investigation, Facebook granted application developers the ability to access its users' data without obtaining their express consent, as well as having failed to impose checks on developers and apps using its platform. Accordingly, developers were able to harvest data of up to 87 million Facebook users and share some of it with organisations, including Cambridge Analytica, which were involved in political campaigning in the US. **Moreover, even after Facebook had discovered the misuse of its users' data, it did not take sufficient steps to ensure that those who retained said data had taken adequate and timely remedial actions, including deletion**. In its investigation, the ICO found

that at least one million UK users' personal information was among the harvest data and who were subject to the risk of further misuse.

Accordingly, the Commissioner has reached the conclusion that Facebook had failed to protect the privacy of its users sufficiently before, during and after the unlawful processing of this data, and that a company of its size and expertise should have been aware and proactive. The ICO clarified that they view these contraventions very seriously, but that since the event occurred before the GDPR (which now gives the ICO the power to issue much higher fines) came into effect, the ICO imposed the highest fine possible under the Data Protection Act 1998. A similar fine was also imposed on the credit rating agency, Equifax Ltd, last month (see our previous report here).

Uber to Pay a Record Penalty of $148 Million in a Settlement Over a 2016 Data Breach

Uber Technologies, Inc. ("Uber") announced it has reached an agreement with the Attorney Generals of all 50 US states and the District of Columbia to resolve their legal inquiries regarding a data breach affecting its customers in October 2016.

Uber agreed to pay a record sum of $148 million as part of this settlement. The investigation, led by state attorneys general across the United States, focused on **whether Uber had violated data breach notification laws by not informing consumers that their information had been compromised**.

The settlement also requires Uber to adopt model data breach notification and data security practices as well as a corporate integrity program for employees to report unethical behaviour. Uber will also hire an outside firm to assess the company's data security and implement its recommendations.

The settlement follows a 10-month investigation into a data breach that exposed personal data from 57 million Uber accounts of both riders and drivers, including names, email addresses and phone numbers of 50 million Uber riders around the world and 600,000 registration numbers of driver vehicles. **Uber did not report the data breach upon discovery, and instead paid hackers $100,000 to dispose of the evidence and for this incident to be concealed. This breach was first disclosed by the company's new Chief Executive, Dara Khosrowshahi, more than a year after the company was hacked**.

The Federal Trade Commission ("**FTC**") had already initiated an investigation after the data breach came to light, and following settlement with Uber, added further provisions by virtue of inadequate data safeguards (see our first report concerning Uber's settlement with the FTC here).

Anthem Pays OCR $16 Million in Record HIPAA Settlement

Anthem has agreed to pay the Department of Health and Human Services' Officer Rights (OCR) $16 million and to take corrective action for its violations of the Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rules. The violations were due to a series of cyberattacks that occurred between December 2014 and January 2015, which led to the largest health data breach in history, impacting nearly 79 million consumers.

In 2015, OCR received a notification from Anthem regarding cyber-attackers who gained unauthorised access to Anthem's electronic protected health information (**ePHI**) of 78,800,000 consumers. **The OCR investigated Anthem's compliance with the HIPAA Rules, and found that Anthem had potentially violated several provisions**. In order to avoid further investigation and formal proceedings, **Anthem has now agreed to pay the amount of $16 million, and to undertake a corrective action plan according to which it will have, inter alia, to:**

- Conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities as to the confidentiality, integrity and availability of ePHI held by Anthem;
- Review and revise, as necessary, its written policies and procedures which are addressed by the Security Rule, namely: information system activity review and access control, and make them available to members of the Anthem's workforce who are subject to them, for example, through its intranet; and
- Submit a written report, which shall include its approval regarding the abovementioned policies and the implementation of procedures.

The European Commission Publishes New Guidance on Geo-Blocking Regulation

TOPICS: Geo-Blocking, European Commission, European Union

The European Commission ("EC") has published updated guidance in order to help Member States and e-commerce businesses to comply with the new rules against unjustified geo-blocking (see our related report about the new regulation here).

The EC has issued an updated version of the Questions & Answers document, which supersedes the document released in March 2018. The aim of the updated document is to provide practical guidance on the main provision of the Geo-Blocking Regulation, as well as a general evolution of certain aspects of the EU e-commerce framework, that is addressed to traders, consumers and Member States.

For instance, the document states that the Geo-Blocking Regulation applies to both online and offline sales of goods and services, as well as in cases where both channels are integrated (omni-channel); details the sectors that are excluded from the scope of the

regulation; and that the consent required in order for a trader to be able to redirect a customer to a specific version of their website, does not necessarily need to be provided every time the customer visits the same website, while the customer should have the opportunity to withdraw that consent at any point of time.

In addition, the EC has published a factsheet, which further explains the meaning of **unjustified geo-blocking**, the importance of the Geo-Blocking Regulation, and the services that are not covered under the regulation.

We would be happy to advise on any questions that may arise regarding the Geo-Blocking Regulation.

The Canadian Mandatory Breach Reporting Rules to Come Into Force

TOPICS: Data Breach, Personal Information Protection and Electronic Act, Canada

As of 1 November 2018, organisations subject to the Canadian Personal Information Protection and Electronic Act (PIPEDA) (previously amended in March), will be required to comply with the new privacy breach reporting rules. Any breach of the reporting rules obligations may result in the business being charged with an offence, which could result in a fine of up to CAD 100,000.

Such reporting rules require all organisations, regardless of their size, to notify the Privacy Commissioner, as well as affected individuals, of any privacy breach that poses a genuine risk of "significant harm". Significant harm is defined as humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effect on credit record, or damage to or loss of property. **Organisations are also required to maintain a record of all breaches for two years, whether or not there is a real risk of significant harm.**

According to the PIPEDA, the report to the Commissioner will have to include a description of the breach, when it occurred, the personal information that is involved, the estimated number of individuals affected and the steps that the organisation will take in response. Private sector organisations should use the PIPEDA breach report form.

We would be happy to advise on any questions concerning Canada's mandatory breach reporting rules as well as other compliance requirements stemming from PIPEDA.

The UK Publishes a Code of Practice for Consumer IoT Security

TOPICS: Security Standards, Internet of Things, Department for Digital, Culture, Media and Sport, United Kingdom

The UK's Department for Digital, Culture, Media and Sport ("DCMS") has released a voluntary code of practice to help Internet of Things companies to achieve a "secure by design" approach, including to comply with applicable data protection laws, such as the GDPR, from the earliest stages of the design process. This publication comes after the announcement of a new law in California regarding the security requirement in IoT devices (see our previous report here).

The Code of Practice contains thirteen **outcome focused guidelines** which are aimed to help companies protect their customers' privacy and safety. The most important guidelines, according to the DCMS, are the following:

- Device Manufacturers are responsible for ensuring that **IoT devices must have unique passwords**, which cannot be restored to any universal factory default value;
- Device Manufacturers, IoT Service Providers and Mobile Application Developers shall have **a vulnerability disclosure policy** in order that security researchers and others are able to report them; and
- Device Manufacturers, IoT Service Providers, Mobile Application Developers are responsible for **software updates, which should be easy to implement**. In addition, the period of software update support shall be made clear to a consumer when purchasing the product.

Some of the other guidelines concern the credentials applicable to storing, encryption of security-sensitive data, the "principle of least privilege" and making installation and maintenance of devices more straightforward. The UK government has also published a mapping document in order to make it easier for other manufacturers to sign up to the new code, and a document for consumers with guidance on securing IoT devices in the home.