Montgomery & Hansen LLP

Client Alert February 23, 2016

Recent Privacy Law Developments

By **Daniel Appelman**

A number of recent developments in US and European privacy and security law will affect companies worldwide, particularly those that offer online and mobile services. This Client Alert highlights those important developments and the impact they will have for many of our clients.

FTC's Authority to Regulate Online and Mobile Privacy. Last August, in a ground-breaking decision, a federal appeals court confirmed the Federal Trade Commission's authority to regulate online privacy and to hold companies accountable for deficiencies in their written cybersecurity policies and actual practices.
More in next column

California's Most Recent Amendments of Data Breach Notification Law. In October, California amended its data breach notification law to increase and clarify compliance obligations of companies that collect personal information from individuals.
More on page 2

Safe Harbor Basis for EU to US Data Transfers Invalidated. In October, the European Court of Justice invalidated the US-EU Safe Harbor framework, the set of procedures on which most US companies rely to lawfully transfer personal data from Europe to the United States. In early February, the European Commission announced a replacement for that framework that will require US companies to make significant changes in how they protect personal data from Europeans and how they document their adherence to the new procedures.
More on page 3

New European Data Protection Regulation. In January, the European Commission approved the General Data Protection Regulation, an extensive substitute for the current Data Protection Directive.
More on page 4

****

FTC Authority to Regulate Private Sector Privacy and Cybersecurity Practices Affirmed in FTC v. Wyndham

The United States Court of Appeals for the Third Circuit issued a landmark decision last August in *FTC v. Wyndham Worldwide Corporation*. The decision confirmed the Federal Trade Commission's authority to sanction companies whose cybersecurity practices are deficient or whose privacy policy statements describing those practices are inaccurate, misleading or deceptive. We wrote about this decision in a prior Client Alert and we briefly summarize it here.

Following a hacker attack on Wyndham Worldwide Corporation's servers in which payment card and personal data was compromised, an FTC investigation found that Wyndham's privacy policies, particularly those describing the measures Wyndham employed to secure its data network, were inaccurate, deceptive and misleading. The FTC also identified a number of deficient data security practices by Wyndham that it determined to be deficient, including the use of weak and default passwords, the lack of or improperly implemented firewalls, storing payment card information in plain text, failing to implement procedures that would restrict unauthorized access to Wyndham's network and hotel servers, and failing to follow proper incident response procedures even after experiencing successive cyber attacks.

The FTC then sued Wyndham for engaging in unfair trade practices by failing to provide reasonable security measures and for having a deceptive privacy policy. Wyndham filed a motion to dismiss the lawsuit on the basis that the FTC lacked authority to regulate cybersecurity practices, particularly because the FTC had not issued a list of specific cybersecurity requirements with which it expected companies to comply. The Third Circuit affirmed the FTC's authority to regulate unfair cybersecurity practices, even in the absence of a definitive list of compliance requirements. Although the court's decision did not directly address Wyndham's alleged deceptive descriptions of its cybersecurity practices in its privacy policy, the allegations of false and inaccurate statements appear to have been a critical factor in the court's decision.

Conclusion
The FTC has brought dozens of enforcement actions against companies alleging that their inadequate cybersecurity practices constitute unfair practices under Section 5 of the Federal Trade Commission Act. The Wyndham case underscores the necessity for companies operating online to implement reasonable security measures to protect consumers' personal information, to review those measures periodically, to change them as needed, and to make sure that those measures are accurately described in their privacy policies.

****

California Amends its Data Breach Notification Law

Data breach notification laws require companies that collect and store electronic personal information and suffer a data breach to notify those individuals whose personal information is reasonably expected to have been compromised and to provide additional information and resources to the victims of the breach. Under certain circumstances, companies can comply with the notification requirements by providing "substitute notice" as explained below. Almost every state has adopted a data breach notification law. While there is variation among state laws, most are modeled on California's, which was the first in the nation and is frequently updated. California's data breach notification law is Civil Code 1798.82.

California recently amended its data breach notification law for the third year in a row. The most recent amendment (i) defines the word "encrypted", (ii) imposes new formalities that companies must comply with when informing consumers of a data breach, and (iii) clarifies substitute notice requirements.

When does the amendment become effective?
The amendment came into effect on January 1, 2016, and companies must update their data breach incident response plans to comply with it.

What has changed?

(i) "Encrypted" Defined

Under California law, like most other states' laws, companies do not have to notify consumers that they have experienced a data breach if the personal information they possess is encrypted. Until now, the term "encrypted" was not defined in the California legislation. As a result, companies faced uncertainty about whether the security measures they employed to protect personal data would be considered encryption, thus exempting them from having to disclose their company's data breach as otherwise required.

The recent amendment attempts to ease that uncertainty. It defines "encrypted" as: "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

While a good start, the new definition leaves open additional questions. The definition does not include minimum standards or examples of encryption measures that satisfy the California law. Nor is there guidance about how California's Attorney General, who enforces the law, will determine whether an encryption method is "generally accepted in the field of information security." Until more guidance becomes available, companies should avoid encryption methods that are not commonly used. But also see the discussion of the FTC's authority to regulate cybersecurity practices in the absence of minimum standards elsewhere in this Client Alert.

(ii) New Notice Formalities

In the event of a data breach, California law imposes substantive requirements on the content of the notices that must be sent to people whose unencrypted personal information was or is reasonably believed to have been compromised. Such notices must include:

- A general description of the breach;
- The name and contact information of the company sending the notice;
- A list of the types of personal information that were compromised by the breach;
- The date of the breach (or an estimate if not known with certainty); and
- Phone numbers and addresses of major credit reporting agencies if social security numbers or drivers' licenses or California ID card numbers were compromised.

The recent amendment imposes specific requirements for the form of those notices. Most notably it requires that notices be titled "Notice of Data Breach," be written in plain language in text no smaller than 10-point type and include the following headings: "What Happened;" "What Information Was Involved;" "What We Are Doing;" "What You Can Do;" and "For More Information."

To help reduce the burden of complying with the new form requirements, the amendment includes a model security breach notice form. Companies are free to develop their own data breach notice forms. However, using the model form reduces the time and cost of developing a form that complies with the new requirements and does much to limit the risk of noncompliance. Companies should carefully review notice forms that diverge from the model form provided by the California legislature before adopting them.

(iii) Substitute Notice Requirements

California law normally requires that the data breach notice be sent by first class mail to each person affected by the data breach, or by email--but only to those who have given their prior consent to be notified by email. However, if the cost of providing such notice would exceed two hundred fifty thousand dollars, or the affected class of subject persons to be notified exceeds 500,000, or the company doesn't have sufficient contact information, the law allows companies to provide substitute notice by email and posting to its website. Companies that provide substitute notice must (i) email notices to California residents for whom the company has a valid email address, (ii) post a "conspicuous" notice meeting all of the law's requirements on the company's website, (iii) notify "major statewide media" of the breach, and (iv) email a link to the web site notice to the California Office of Privacy Protection at privacy@scsa.ca.gov. California.

The new amendment provides further guidance as to what constitutes "conspicuous" notice for purposes of satisfying the substitute notice requirements. It requires companies to provide links to the notice on their "home page or first significant page after entering a company's website, and the link must be in larger type than the surrounding text or in contrasting type, font or color to the surrounding text of the same size or set off from other type by symbols or other marks that call attention to the link. The notice must also remain on the company's website for at least 30 days following discovery of the data breach.

****

Invalidation of US-EU Safe Harbor

Companies that collect or process personal data from European residents and store that data in servers located in the US must comply with the European Data Protection Directive by providing adequate measures to protect and safeguard that data. In 2000, the European Commission approved the EU-US Safe Harbor framework which was intended to bridge the differences between US and EU data protection standards and to provide a streamlined procedure by which US companies could comply with the Directive. Since 2000, many US companies have relied on the Safe Harbor framework as the legal basis by which they are able to transfer European personal data to the US.

In October, the Court of Justice of the European Union declared that framework invalid in large part due to concerns about mass surveillance by US intelligence agencies as revealed by the Snowden disclosures. This threw into considerable doubt the legality of transferring personal data from the EU to the US.

On February 2, 2016, the European Commission announced a replacement framework called "EU-US Privacy Shield," but only described the framework in high level terms with many details left to be fleshed out.

The main features of the new framework are as follows:

(i) Stronger compliance obligations for US companies importing personal data from Europe. Just what those stronger obligations are has not yet been announced.

(ii) US Department of Commerce monitoring of US companies relying on the new framework to ensure they comply with the new obligations, whatever they are; and Federal Trade Commission enforcement actions against those who transgress.

(iii) Stronger compliance obligations for human resource data and genetic information.

(iv) Clearer safeguards and transparency with regard to US government access to personal data originating in Europe. As part of the new Privacy Shield framework, the US has agreed to not conduct indiscriminate mass surveillance of European personal data transferred to the US.

(v) An annual review of the new framework by the European Commission and the US Department of Commerce, including the issue of national security access.

(vi) Enhanced protection of EU citizen's rights and expanded options for seeking redress for any misuse of European personal data. European data protection authorities will be able to refer complaints to

the Department of Commerce and the Federal Trade Commission. EU citizens may employ alternate dispute resolution (presumably mediation and/or arbitration) free of charge. A dedicated US ombudsperson will be appointed to receive complaints relating to possible access to personal data by national intelligence agencies.

Next Steps: The Department of Commerce and the European Commission have agreed in principal to a greater level of protection for European personal data, but the actual rules and regulations that companies can rely on have yet to be revealed. The European Commission must also prepare a formal decision that compliance with the Privacy Shield will provide an adequate level of protection that the EU Data Protection Directive requires. That decision must be adopted by the College of EU Commissioners after consulting with EU Member States and taking the advice of the Article 29 Working Party, an advisory group of EU national data protection authorities. The European Commission, the US Department of Commerce and the Federal Trade Commission must also implement the features and procedures described in the initial announcement. All of this will take time; and the final version of the new framework may undergo considerable change between now and then. It is also possible that the new framework will face legal challenges by those in Europe who feel it does not go far enough in protecting privacy.

What does this mean for me?
It will be some months before US companies can rely on the Privacy Shield when transferring the personal data collected from Europe to the United States. Since the Safe Harbor principles have been invalidated, complying with them no longer suffices. The European Data Protection Directive provides a few other means of compliance, including adopting certain model clauses approved by the Commission or binding corporate rules, or obtaining the consent of each data subject in advance (opt-in). Adopting the model clauses as part of the terms of use or the standard terms and conditions of contracts with customers may be the best option for many companies in the short term.

****

New EU General Data Protection Regulation

For the past twenty years, the movement of personal data between the members of the European Union and from the European Union to other countries, including the United States, has been regulated under a set of guidelines called the EU Data Protection Directive. Each EU Member State has implemented its own interpretation of the directive under its own laws, and enforced those laws under its own judicial and regulatory systems with little consistency among the states in so doing. This has led to considerable uncertainty and has substantially increased burden of compliance on companies that are subject to those laws. In addition, many Europeans concerned with data privacy have called for increased legal protection for their personal information obtained by online and mobile service providers.

In late December, the European Commission, European Parliament and European Council reached agreement to replace the Data Protection Directive in its entirety with the EU General Data Protection Regulation ("GDPR" or "Regulation"). This will entail significant changes to the data protection regime in Europe.

When will the GDPR become effective?
The GDPR will go into effect two years after the European Parliament and the European Commission formally adopt it, which adoption is expected early this year. Until then, the laws of the individual EU Member States that were promulgated under the EU Data Protection Directive will remain in place.

Reach of GDPR. The GDPR, once it becomes effective, will apply to all companies worldwide that collect or process any personal data belonging to EU residents, even those companies that do not have an EU presence. The GDPR applies, for example, to any company worldwide that offers a web or mobile application that collects personal data from Europeans and maintains it using cloud services, even if the cloud servers are located outside the EU.

Processing and Consent of the Data Subject. The GDPR prohibits companies ("data controllers" and "data processors" in the terminology of the GDPR) from collecting or processing personal data of EU residents (called "data subjects"), including moving data to servers outside the EU, without the affirmative consent of each data subject or unless one of five exemptions listed in the Regulation applies. Consent from the data subject must be freely given, specific, informed and unambiguous, and it must be given either in a written statement or indicated by "clear affirmative action". Under the GDPR, data controllers cannot process the personal data of a data subject unless that data subject "opts in".

In the United States, by contrast, companies can generally process and move personal data unless the data subject "opts out".

Personal Data Defined. The definition of "personal data" in the GDPR is much broader than in the privacy laws in the United States. In the EU, personal data includes any data from which a living European can be identified by anyone else – not only names, addresses and phone numbers but also any identification number, location data, online identifier, device identifier, cookie ID or IP address. Genetic and biometric data is subject to even more stringent conditions than other forms of personal data.

Rights of Data Subjects. The GDPR codifies the rights of data subjects much more broadly than do the privacy laws and regulations in the United States. Those EU rights include (i) the right to receive information about the processing of one's personal data in a concise, transparent, intelligible and easily accessible form, using clear and plain language; (ii) the right to receive information about the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (iii) the right to be informed of the legitimate interests pursued by the data controller or by a third party in obtaining, processing and moving the personal data; (iv) the right to know the intended recipients of the personal data, the intended destination of the data if the intent is to transfer personal data to a third country or international organization, and the period for which the data controller or third party recipient will store the data; (v) the right to request access to one's own personal data; (vi) the right to request correction of inaccurate data and erasure of that data in certain circumstances; (vii) the right to place certain restrictions on the processing of personal data; (viii) the right to receive one's own personal data from the data controller in a structured and commonly used and machine-readable format; (ix) the right of the data subject to transmit those data to another controller without hindrance from the controller to which the data have been provided; (x) the right to object to certain processing of one's personal data where the use of that data is for profiling or marketing purposes; and (xi) the right to object to decisions based solely on automated processing such as profiling. The GDPR also codifies the recent decision of the European Court of Justice confirming the so-called "right to be forgotten." Data controllers who have made personal data public are required to delete that data and to notify others of the data subject's request for erasure of his/her personal data. Search engines are required to delete links to old, outdated and misleading personal information upon the request of the data subject.

Reorganization of the Regulatory Authorities. One of the most significant changes in the GDPR is the overhaul of the European data protection structure. The Data Protection Directive was not itself enforceable but provided guidelines for the data protection laws that each Member State was required to enact according to each such State's interpretation of the Directive. The GDPR, by contrast, is law itself, to be enforced throughout the EU. The GDPR creates a European Data Protection Board and supervisory authorities from each EU Member State. Companies will only have to report to one lead supervisory authority instead of being subject separately to each of the national data protection authorities as is currently the case under the Data Protection Directive. This is intended to reduce compliance costs and increase efficiency and consistency.

Data Security. The GDPR requires companies to report security breaches to their supervisory authorities and to the individuals whose personal data may have been compromised. The notifications to the supervisory authorities are required if the breach is likely to result in a risk to individuals; and individuals must be notified only if the breach is likely to pose a "high risk" to them.

Damages and Penalties. Data subjects may sue to claim compensation from data controllers and data processors if they have been damaged by a violation of the GDPR, and the companies have the burden of proving that they are not responsible. Where multiple controllers or processors are involved, the GDPR provides that any one of them may be liable to the claimant for all the damages awarded. Supervisory authorities can also impose monetary penalties against data controllers and data processors for violations of the GDPR. The maximum fine is 4% of a company's worldwide annual sales of goods or services.

Filings and Record-Keeping. The GDPR requires data controllers and data processors to keep detailed internal records of the personal data they collect from each data subject, and to provide each such data subject with the following information at the time the personal data in question is collected: (i) the name and contact information of the data controller, (ii) the purposes for which the data subject's personal data is being collected, (iii) the legal basis for collecting that personal data, (iv) the recipients and intended recipients of the data subject's personal information, (v) if applicable, the data controller's intent to transfer the personal information collected to a third country and whether the European Commis-

sion has or has not determined that the destination country has instituted adequate measures to protect that personal data, (vi) the period during which the data subject's personal data will be stored by the data controller, the data processor and (if applicable) the identified recipients in the destination countries, (vii) the right of the data subject to request the correction or deletion of personal data of the data subject or to object to further processing of that personal data, and (viii) the right of the data subject to withdraw consent previously given.

What Does This Mean For Me?
Most of our clients collect personal information from visitors to their websites or users of their mobile apps. Most often, that information resides in the United States, either on our clients' servers or on servers maintained by third party cloud service providers, such as Amazon. If your company collects any personal information from European residents, the GDPR will apply to you, and your company will be either a data controller or a data processor (as defined by the GDPR) or both.

When the GDPR becomes effective, it will impose significant compliance requirements on every company worldwide that collects any personal data from European residents. Violators of those compliance requirements may be subject to lawsuits by data subjects for which European courts may award monetary damages; and the new European supervisory authorities may levy fines and penalties.

There are many open questions regarding the scope of the new rules and how they will be interpreted by the European data protection authorities. For example, it is not clear what types of "clear affirmative actions" by data subjects will qualify as consent to the collection and processing of their personal data. Is consent as indicated by accepting the terms and conditions of a website or mobile app sufficient? Does an initial consent suffice for all subsequent data collection by the data controller or must separate consents be manifested for each transaction? And what type of breach will trigger the notification obligations to supervisory authorities and the data subjects themselves?

The uncertainties surrounding the scope and interpretation of the GDPR's new requirements will be clarified in court cases and regulatory actions after the new rules become effective. Undoubtedly, companies that collect personal data from Europeans will have to revamp their privacy policies, terms of service and privacy and security procedures to bring them into compliance with the GDPR.

****

For more information about the recent developments described in this Client Alert, contact Daniel Appelman or your M&H attorney.

Montgomery & Hansen s a corporate law boutique located in the heart of Silicon Valley. Our goal is to help clients build the best companies in the world. We combine decades of legal expertise, strong values, a practical approach, and an extensive network of business experts to support entrepreneurs and investors as they start and grow successful companies.

Our practice is intentionally focused on start-up companies and the corporate and transactional advice they require, both legal and strategic. Every client has its own dedicated team which delivers top quality service. We get involved – and we stay involved. Building a successful business takes focus. And that's exactly what you receive from us.