Impacting your Company … in just a few months … GDPR!

By Aaron Schildhaus

If your company has, or is contemplating, any business activities or relationships in the European Union (EU), you will be affected by the EU’s General Data Protection Regulation (GDPR), even if your contacts there are minimal. The GDPR comes into full force and effect May 25, 2018, and companies around the world are preparing for it. Failure to be in compliance with this new law will put companies at risk for enormous fines and penalties: up to the greater of 4% of annual global revenues or €20 Million for data controllers and, for data processors, up to the greater of 2% of annual global revenues or €10 Million.

The GDPR is replacing the existing Data Protection Directive 95/46/EC, which has been the standard for data protection and data privacy in the EU since it came into force in December, 1995. US companies now in compliance with the directive, including the 2400 companies which have qualified for the EU-US Data Privacy Shield, and its analogue, the Switzerland-US Privacy Shield, should be aware that compliance with the current data protection regime will not be sufficient, in and of itself, to qualify under the GDPR.

The GDPR was designed to deal with the growing need to further protect the European individual from being compromised by the misuse of personal data in the possession of organizations; it sets to harmonize privacy and data security laws across Europe and to reshape the way organizations across the region approach data protection. Because the GDPR is a regulation, and not a directive, it will be directly applicable in all EU Member States. It should be noted that the UK’s upgrading of its Data Protection Act with the Data Protection Bill essentially conforms to the GDPR so that its businesses can remain competitive with the EU despite Brexit. In any event, the UK’s exit from the EU will not take place before the GDPR takes effect in May; therefore, UK businesses will be subject to the GDPR, too.

Article 1 of the GDPR “lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data … (and it) … protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” (Continued)
The GDPR and its implementation will have a profound effect on data protection and privacy not only in Europe, but worldwide, given the trans-border realities of electronic data management and processing and the regulation’s new, extra-territorial provisions. It applies to all companies, regardless of location, that process the personal data of data subjects residing in the EU. The GDPR also applies to the processing of personal data of data subjects in the EU by controllers and processors in the EU, wherever the processing takes place, whether or not in the EU.

Another extra-territorial provision of the GDPR is that it applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to the offering of goods or services to EU citizens (whether or not payment is required) and the monitoring of behavior that takes place within the EU. Previously, under the directive, territorial applicability was ambiguous, referring to data processing in the context of an establishment. The extra-territoriality of the Regulation is now clear; moreover, non-EU businesses processing the data of EU citizens will have to appoint a representative in the EU.

In addition to its application outside of Europe and the potentially high penalties for its violation, other notable changes in the GDPR over the current data protection regime include:

- A request for the data subject’s consent must be given in a concise, transparent, intelligible and easily accessible form, and the consent must be given for one or more specific purposes.
- The right to erasure (right to be forgotten). Set forth in Article 17, it entitles the data subject to have the data controller erase his/her personal data, cease its further dissemination, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing, or data subjects withdrawing their consent. When considering such requests, controllers are required to compare the subjects’ rights to “the public interest in the availability of the data”.
- The right for rectification set forth in Article 16.
- The right of data subjects to obtain free reports re type and purpose of data, names of data processors;
- The requirement that companies of a certain size have their own internal Data Protection Officers (DPO’s);
- Establishment of DPO criteria;
- The requirement that forms providing for data subject consent be clear, concise and intelligible;
- The requirement that it be as easy to withdraw consent as to grant it;
- Mandatory breach notification within 72 hours where a breach risks individual rights and freedoms;
- Data portability by data subject; right to transmit data to another controller;
- Privacy by design; advance determination of minimum information required by controller. (Continued)
If a data breach occurs, notification must be given within 72 hours from first awareness of the breach in all member states where said breach is likely to “result in a risk for the rights and freedoms of individuals”. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.

Data protection by design under the GDPR means that data protection must be a consideration from the onset of the designing of systems, rather than an addition. 'The controller shall implement appropriate technical and organisational measures , such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation.in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

Under the GDPR it will not be necessary as is currently the case, for data processors to submit notifications / registrations to each local Data Processing Authority (DPA) of data processing activities, nor will it be a requirement to notify or obtain approval for transfers based on the SCCs). Instead, there will be internal record keeping requirements, and the DPO’s appointment will be obligatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale, or of special categories of data or data relating to criminal convictions and offences. The DPO must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices, and may be a staff member or an external service provider. The DPO’s contact details must be provided to the relevant DPA. In addition, the DPO must be provided with appropriate resources to carry out its tasks and maintain his/her expert knowledge. The DPO must report directly to the highest level of management, and must not carry out any other tasks that could result in a conflict of interest.

Compliance possibilities by entities continue to include the use of Binding Corporate Rules (BCR) and Standard Contractual Clauses (SCC).
By Michael Licker and Christopher Hart, Foley Hoag LLP

Twice last year, the SEC’s newly created Cyber Unit has shut down an initial coin offering. To understand the importance of these actions, some background is in order. Historically, the SEC has addressed cyber threats through enforcement actions aimed at entities and individuals that threaten market integrity, either by failing to take necessary cyber precautions or engaging in cyber-related misconduct, and through regular cyber examinations of registered entities by the SEC’s Office of Compliance Inspections and Examinations (“OCIE”). The Commission’s Enforcement Division created a new Cyber Unit in September 2017. This unit has a broad mandate to target all forms of cyber-related misconduct, including market manipulation schemes involving false information spread through electronic and social media, hacking to obtain material nonpublic information, violations involving distributed ledger technology and initial coin offerings (more on that to follow), misconduct involving the dark web, intrusions into retail brokerage accounts and cyber-related threats to trading platforms and other market infrastructure. The Market Abuse Unit previously handled the SEC’s cyber investigations, but the Commission deemed the threat important enough to create a separate unit (the Enforcement Division’s first newly created unit since 2010).

The first charges filed by the Cyber Unit were in December against Dominic Lacroix and his company PlexCorps, for what the SEC alleges is a fraud of $15 million from thousands of investors through an ICO. Just weeks later, the Cyber Unit struck again, taking an enforcement activity against Munchee, Inc., a California-based developer of an iPhone application for people to review restaurant meals, for its ICO. These enforcement activities follow several policy statements and warnings regarding ICOs. The Munchee order was also issued the same day that SEC Chairman Jay Clayton issued renewed warnings to both main street investors and market professionals regarding ICOs and cryptocurrencies.

The Munchee ICO involved the sale of digital tokens to be issued on a blockchain, or a distributed ledger. Munchee hoped to raise $15 million through this sale. The SEC caught wind of the ICO and halted it after approximately 40 sales because it determined that the ICO constituted the unlawful sale of unregistered securities.

The SEC has emphasized that the test for determining whether a coin or token is a security for federal securities registration purposes is no different than the test applicable to other potential securities. The key question is whether the investor had a reasonable expectation of deriving profits from the entrepreneurial or managerial efforts of others. In determining that Munchee’s coins constituted securities, the SEC cited efforts by Munchee to increase the value of the tokens and make them available for sale on secondary markets. (Continued)
Munchee also made statements on social media and on podcasts suggesting that the tokens would increase in value. Importantly, the SEC emphasized that even if tokens had a practical use at the time of the offering, it would not preclude them from being a security.

Munchee started selling tokens on October 31, and by November 1 the SEC had contacted Munchee, leading to the end of the ICO. Munchee also agreed to return all proceeds it had received to token purchasers. In exchange for Munchee’s cooperation, the SEC did not take further punitive action.

The enforcement action is yet another reminder that the SEC will continue to be extremely active in all areas of cyber regulation. It is also an important reminder that “securities” come in all different forms and that even newer, more modern iterations of securities must be registered with the SEC. In Chairman Clayton’s ICO policy statement, he noted that while not all ICOs implicate securities registration requirements, a large majority of them involve the sale of securities and require registration. Chairman Clayton concluded the policy statement by noting that he has asked the SEC Division of Enforcement to “police this area vigorously,” and take appropriate enforcement action, strongly suggesting that there is more enforcement activity in the future.
Carpenter privacy case vexes justices, while tech giant Microsoft battles Government in second U.S. Supreme Court privacy case with international implications

By Richard J. Peltz-Steele

Last quarter’s committee news reported the first of two major privacy cases with international implications to reach the U.S. Supreme Court this term, Carpenter v. United States. Now a second such case pits the Government against Big Tech in United States v. Microsoft.

Carpenter v. United States. Carpenter is a criminal case involving federal seizure of cell phone location data from service providers. Arising under the “reasonable grounds” provision of the Stored Communications Act (SCA), the case accentuates Americans’ lack of constitutional protection for personal data in third-party hands, in contrast with emerging global privacy norms.

In oral argument in November, the Government positioned itself squarely within the third-party doctrine. Justice Kagan pushed back, finding analogy in United States v. Jones. In Jones in 2012, the Court held unanimously that law enforcement violated the Fourth Amendment by surreptitiously attaching a GPS tracker to a suspect’s car. The Government sought to distinguish Jones as involving (literally) hands-on intrusion.

Just as she expressed misgivings about the third-party doctrine in her Jones concurrence, Justice Sotomayor raised the alarm about waning informational privacy in the digital age. She suggested that the Court might carve out an exception to the doctrine, as it has for medical records. Justice Breyer seemed receptive to the comparison; Justice Alito did not. Chief Justice Roberts seemed to search for a middle ground, wanting to connect the dots from cell phone content—which requires a search warrant—to location data.

In sum the Court majority seemed ill disposed to discard the third-party doctrine and invigorate privacy in constitutional law. The takeaway from Carpenter is likely to be that Congress still holds the key to bringing U.S. search and seizure into accord with European data protection.

United States v. Microsoft. The second major privacy case headed for Supreme Court decision in 2018 also arises under the SCA, involves criminal investigation and new technology, and implicates collision between the third-party doctrine and European privacy law. In United States v. Microsoft, however, the implications for international law looming larger.

In Microsoft, federal law enforcement officers in a narcotics investigation obtained a probable-cause warrant for the content of a Microsoft user’s email. The user’s identity, residence, and nationality are not in the public record. What is known is that the user’s email resides in Ireland. (Continued)
Microsoft maintains only one virtual “copy” of a user’s email (with some immaterial exceptions), usually geographically near the user or where the user purports to be.

Carpenter and Microsoft implicate different subdivisions of SCA § 2703. Carpenter involves a court order predicated only upon reasonableness, ostensibly meant to compel production of information about a user. Microsoft involves a court-sanctioned warrant predicated upon probable cause to compel production of information of a user. When the Government wants to look inside email messages, the SCA ups the stakes, more or less analogizing to a postal package.

Microsoft surrendered metadata stored on servers in the United States, but moved to quash the warrant for email contents stored on servers in Dublin. Microsoft asserted that the SCA does not authorize compelled production outside the United States. The Government retorted that production is not extra-territorial if data can be summoned from a terminal in Redmond, Washington, without anyone in Dublin lifting a finger. The Second Circuit ruled for Microsoft, citing the canon of presumption against extraterritoriality, and an equally divided bench denied rehearing en banc with dissents.

The Court heard oral argument in February. According to analysis by Amy Howe for SCOTUSblog, the court was divided. Chief Justice Roberts and Justice Alito were skeptical that Microsoft’s choice to place data overseas should control the government’s reach. Justices Ginsburg, Gorsuch, and Sotomayor seemed more sensitive to the impact of overseas reach on international comity. Justice Breyer seemed in search of a case-by-case middle ground, of which Microsoft counsel wanted no part.

In a lucid concurring opinion in the Second Circuit, below, Judge Lynch posited that the case perhaps should turn on a fact we do not have: the user’s nationality. It matters, he reasoned, whether the case is about an American warrant for an Irish national’s email, located in Ireland, held by an American company selling services to Irish users, or about an American warrant for an American’s email located in Ireland only because the American misrepresented residence.

Nevertheless, Judge Lynch concluded that the key to resolving conflict between international law enforcement and comity rests, again, with Congress.
Privacy, Cybersecurity and Digital Rights Committee

Co-Chairs:
Cecil Sae Hoon Chung
Daniel McGlynn
Kenneth N Rashbaum

Vice-Chairs:
Shruti Chopra
Carlos Eduardo Eliziario de Lima
Daniel McGlynn
Daniel Meyers
Joseph D. Prestia
Lauren Schmidt
Anahita Thom

Newsletter Editor:
Shruti Chopra

Committee News

- Beginning FY2018, the Committee name has been changed to Privacy, Cybersecurity and Digital Rights from Privacy, E-Commerce and Data Security.

- Committee FY2018 Appointment (September 2017 to August 2018)

  Co-Chairs
  Cecil Chung – 3rd year (cschung@yulchon.com)
  Daniel McGlynn – 1st year (dmcglynn22@yahoo.com)
  Ken Rashbaum – 3rd year (krashbaum@bartonesq.com)

  Vice Chairs
  Shruti Chopra - Publications
  Carlos Eduardo Eliziario de Lima - Programs
  Daniel Meyers - Policy
  Joseph D. Prestia - Membership & Communications
  Lauren Schmidt – Diversity
  Anahita Thomas - Programs