Foreword

The past few months have been very busy in the field of privacy, with the official launch of the EU-US Privacy Shield framework on 1 August 2016 and Microsoft winning its landmark appeal over the seizure of foreign emails.

There is no indication that things will slow down either, with the strong growth of the cloud (see, for example, Johnson & Johnson targeting 85% of Apps in Cloud by 2018, TechCrunch's analysis of the email, data and privacy implications of Microsoft’s acquisition of LinkedIn and of course the recent “Pokemon Go” fever).

Data is now growing at an exponential rate, with 50,000 GB of data expected to be created every single second by 2018. Pew Research found that 91 percent of American adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies. Some are attempting to fight back, as demonstrated by the recent cat-and-mouse game between Facebook and the ad-blocking community. The increasing number of data breaches reported in the media does not help to alleviate concerns, the recent examples being the breach of UK software company Sage as well as the separate data breach at Oracle’s MICROS division.

Some companies are already jumping on the privacy bandwagon, such as Apple with its recent announcement (in June 2016) to soon begin using a technique called “Differential Privacy” to improve the privacy of its data collection practices. The fact that a company like Apple is exploring a technology that attempts to collect more user information while increasing the privacy protection of its users indicates how important privacy, and more importantly consumer trust, has gradually become in the industry.

We hope that you enjoy reading this newsletter as much as we enjoyed preparing it. Please do not hesitate to contact us about any ideas you may have for this newsletter.

Paul Lanois

Microsoft wins landmark appeal over seizure of foreign emails

On 14 July 2016, the United States Court of Appeals for the Second Circuit reversed an earlier District Court ruling that ordered Microsoft to turn over Outlook.com emails sought by the U.S. Department of Justice that were stored on in a data center located in Ireland.

According to the ruling, "the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers."

Microsoft’s chief legal officer, Brad Smith, wrote in a blog message: "The decision is
important for three reasons: it ensures that people’s privacy rights are protected by the laws of their own countries; it helps ensure that the legal protections of the physical world apply in the digital domain; and it paves the way for better solutions to address both privacy and law enforcement needs.

First, this decision provides a major victory for the protection of people’s privacy rights under their own laws rather than the reach of foreign governments. It makes clear that the U.S. Congress did not give the U.S. government the authority to use search warrants unilaterally to reach beyond U.S. borders. As a global company we’ve long recognized that if people around the world are to trust the technology they use, they need to have confidence that their personal information will be protected by the laws of their own country.”

Source:
Microsoft Blog - Our search warrant case: An important decision for people everywhere

UK medical practice fined £40,000 for data protection breach

The UK’s privacy regulator, the Information Commissioner’s Office (“ICO”), has issued Regal Chambers Surgery, a surgery practice in the UK, with a fine of £40,000 for unlawfully disclosing the personal data of two individuals in response to a data subject access request (“SAR”) from a third person.

In this case, a woman warned the surgery that its staff needed to take particular care to protect her details, but the surgery failed to do so when her ex-partner made a subject access request for the medical records of the former couple’s son.

In its public statement issued on 11 August 2016, the ICO criticized the surgery for not having adequate systems or training in place to ensure that its staff is equipped to deal with SARs properly. In particular, the ICO noted that a SAR is a request for an individual’s personal data only and does not authorize the disclosure of full copies of an individual’s file in its entirety. The fact that the woman had given prior warning to the surgery before the disclosure took place was an aggravating factor.

Source:
Information Commissioner’s Office - Monetary penalty notice against Regal Chambers Surgery

Article 29 Working Party issues statement on the EU-US Privacy Shield

On 26 July 2016, the Article 29 Working Party (the WP29), which is composed of representatives of the national data protection authorities in the European Union (DPAs), issued a public statement on the decision of the European Commission in relation to the EU-US Privacy Shield.

The WP29 commended the EU and US authorities for having taken their comments into consideration in the final version of the Privacy Shield documents. However, the WP29 indicated that a number of these concerns remain outstanding, in particular in relation to the commercial aspects (e.g. the lack of specific rules on automated decisions and of a general right to object, as well as the uncertainty on how the Privacy Shield Principles would apply to processors) and the access by U.S. public authorities to data transferred from the EU (e.g. stricter guarantees regarding the powers of the Ombudsperson mechanism and the lack of concrete assurances regarding potential mass and indiscriminate collection of personal data).

In light of the above, the WP29 stated that the first joint annual review will be a “key moment” to assess the robustness and efficiency of the Privacy Shield mechanism. The WP29 stressed especially on the need to clearly define the role of the DPAs in the course
of the upcoming joint review and on the need for all members of the joint review team to have access to all information necessary for the performance of their review, for example, the necessity and proportionality of the collection and transfer of data by public authorities. The WP29 also indicated that the results of the first joint review regarding access by US public authorities to data transferred under the Privacy Shield may also impact transfer tools such as Binding Corporate Rules and Standard Contractual Clauses.

As of August 1, companies may begin self-certifying under this new Privacy Shield framework. According to the The Wall Street Journal, roughly 40 US companies have now signed on to the US-EU “Privacy Shield” agreement. According to some reports, more than 200 applications are now being processed by the Commerce Department.

Source: Press release WP29 - Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield

**Police Body Worn Cameras Use in the US**

At a time when police across the U.S. are being scrutinized, law enforcement agencies across the country are rapidly adopting body-worn cameras for their officers. One of the benefits for these cameras is to be able to document the police's interactions with the public and discourage violence against officers. A recently released scorecard from the Leadership Conference, together with a coalition of civil rights, privacy, and media rights groups, examined 50 U.S. police departments.

The survey found that police departments are quickly moving to deploy body-worn cameras. However, the survey found that departments that have a strong policy in one area often falter in another — it appears that every police department in the country has room to improve. At the same time, the survey found examples of strong policy language currently in use for nearly all of their criteria.

Source: Police Body Worn Cameras: A Policy Scorecard

**Future events**

**The Low Down on Flying High: Risks and Legal Issues for Drones**

This webinar will highlight the latest developments applicable to the use of drone technology for construction and other industries. The program will explain this evolving technology, how it is being utilized today and what is around the corner for tomorrow. The webinar will also cover the current regulatory framework and other legal issues including insurance, data security, confidentiality and privacy issues. The speakers, two nationally recognized experts on drones, will also provide insights on cloud based applications and other helpful tools and software.

**Format:** Webinar  
**Date:** August 16, 2016  
**Time:** 1:00 PM - 2:30 PM ET  
**Credits:** 1.50 General CLE Credit Hours  
**Panelists:** Grant Hagen and Stephen Palley

Register here for the “The Low Down on Flying High: Risks and Legal Issues for Drones”

**Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears**
This program will explore the unique nature of cyber risk in construction with a discussion of key exposures (emphasis on the potential compromise of sensitive corporate data and client information) and technical strategies. The panelists will provide a practical, day-to-day perspective of the general counsel/risk manager; balancing cost concerns and limited resources with the need for robust safeguards and risk transfer. The program will also examine the role of insurance and strategies for maximizing risk transfer, with a focus on the nuances of standalone cyber insurance (i.e., you've just purchased a cyber insurance policy, now what?).

**Format:** Webinar  
**Date:** November 15, 2016  
**Time:** 1:00 PM - 2:30 PM ET  
**Credits:** 1.50 General CLE Credit Hours  
**Panelist:** Gregory Podolak  
**Moderators:** Brian Patrick Rice and Linn Foster Freedman

[Register here](#) for the “Assessing the Situation: How to Identify and Evaluate the Cyber and Data Risks that a Contractor Bears”