Does the US need an EU-style data protection law?

Randy Sabett, Special Counsel at Cooley LLP (US), and Ann Bevitt, Partner at Cooley LLP (UK), look at the two different approaches to data protection regulation in the EU and US, and consider whether US needs EU style regulation — or whether a mix of both styles is in fact preferable

As the European Union moves into the final stages of implementing a new data protection framework, it seems timely to consider whether other countries or regions should be looking to adopt a similar regime.

Some countries have, of course, already followed in Europe's footsteps. Just in the last 15 years for example, Angola, Argentina, Australia, Benin, Burkina Faso, Canada, Cape Verde, Colombia, Costa Rica, Kyrgyzstan, Macau, Malaysia, Mauritius, Mexico, Morocco, New Zealand, Peru, the Philippines, Senegal, South Korea, Taiwan, Tunisia and Uruguay have all adopted what are commonly described as 'EU-style' data protection laws.

Notably absent amongst the countries to adopt a comprehensive data protection law is the US. Should the US follow suit and review its privacy legislation and regulation with a view to moving towards a more 'EU-style' framework? How would that look and —more importantly — is it even desirable?

What is an EU-style data protection law?

There are certain components in both the current Data Protection Directive (95/46/EC) and the proposed Regulation, and in the legislation in the countries referred to above, that are missing from current US privacy legislation.

These include:

- a law which applies across all sectors and to all types of information that identifies individuals (personal data);
- an independent national regulator responsible for enforcing data protection legislation;
- restrictions on cross-border transfers of personal data to countries that do not have an adequate level of data protection;
- the requirement to have a legal basis for processing data;
- enhanced protections for certain categories of (sensitive) data; and
- specific rights of individuals in relation to their own personal data, including the right to request access to and also correct their data, and the new (very heavily publicised and somewhat controversial) right to be forgotten.

It is clear from even a cursory review of these elements that the protection of an individual's personal data, regardless of where those data are and what is being done to them, is at the heart of this type of legislation.

Potential downsides to an EU-style approach

Although it is very difficult to argue in principle against such a framework, there are potential downsides to the EU's very broad and prescriptive approach to the protection of personal data. For example, a 'one-size-fits-all' approach could potentially hinder a company's ability to innovate in today's global economy.

The EU has nonetheless taken the view — not just in the data protection arena, but also in the context of its recent discussions about the Digital Single Market — that a piecemeal approach is a drag on growth and a threat to innovation.

Another criticism often levelled at an EU principles-based approach is that the standards are vague. For example, what exactly are 'appropriate' technical and organisational security measures? In contrast, the US has a plethora of much more developed data security laws, providing detailed and specific security requirements.

Furthermore, the practical impact of the EU's restrictions on the free movement of data can be frustrating, with none of the options available for legitimising cross-border transfers (for example, consent, Safe Harbor, Model Contracts and Binding Corporate Rules) proving attractive, or in some cases even workable.

Can the EU learn from the US approach to privacy?

Given where we are with the adoption of the Regulation, it is too late for the

(Continued on page 4)

(Continued from page 3)

EU to adopt a more US-style approach, at least for the next twenty years or so. Has the EU missed an opportunity in this regard?

Breach notification

One area in which the US does have significantly more expertise than the EU is breach notification. The US has data breach notification laws in the vast majority of states, whereas the EU currently has breach notification requirements only in the telecoms sector (although a minority of Member States, such as Austria and Germany, have implemented national breach notification legislation).

The Regulation will introduce a general breach notification requirement and there has been much discussion about how this will work in practice, in particular about the appropriate timeframes for reporting. The US has a wealth of experience demonstrating what is practicable and appropriate when it comes to reporting breaches on which the EU could, and should, draw.

Proactive security

Similarly, the US has experience with other approaches to privacy and security. The first of these involves a trend toward legislating proactive security. For example, the federal Gramm-Leach-Bliley Act ('GLBA'), Health Insurance Portability and Accountability Act ('HIPAA'), and Sarbanes-Oxley ('SarbOx' or 'SOX') all contain provisions that require a company to proactively implement a variety of security measures, including technical ones.

"Congress has historically been hamstrung when it comes to data security and privacy. Numerous bills have been drafted, debated in committee, brought to the floor, and ultimately failed. Data protection legislation requires a careful balance of the interests of a number of stakeholders and achieving such a balance has been difficult for the US."

At the state level (starting with Assembly Bill 1950 in California), several laws have been passed that explicitly require companies to maintain reasonable security measures. Massachusetts is viewed as setting a high water mark, with its 'Standards for The Protection of Personal Information of Residents of the Commonwealth.'

In recent sessions of Congress, the focus has been on legislation intended to strengthen standards and guidelines in the area of cyber security. Often, the Bills associated with such efforts involve the National Institute of Standards and Technology ('NIST'), and require the NIST to support development of industry-based standards and guidelines. Much of this extends from the first version of the NIST Framework, released in February of 2014 (copy at www.pdpjournals.com/docs/88448).

The NIST Framework, a direct result of Executive Order ('EO') 13696 (not Congressional action), provides a structural framework around which a full security programme could be built. Whilst not a true standard in the sense of a universally recognised accreditation, like such cybersecurity standards as ISO 2700x or the PCI Data Security Standard ('DSS'), the NIST Framework has received relatively broad-based acceptance.

Consumer Privacy Bill of Rights Act

As another example of executive-branch activity, on 27th February 2015 President Obama released a draft of a proposed Consumer Privacy Bill of Rights Act ('Proposal'). The Proposal focuses on protecting the privacy of individual consumers by:

- establishing baseline expectations for companies that collect and use consumer data on the internet; and
- encouraging businesses to voluntarily adopt public codes of conduct for how they handle consumer data.

These protections would ultimately be enforced by the Federal Trade Commission ('FTC') or State Attorneys General.

Congress has historically been hamstrung when it comes to data security and privacy. Numerous bills have been drafted, debated in committee, brought to the floor, and ultimately failed. Data protection legislation requires a careful balance of the interests of a number of stakeholders and achieving such a balance has been difficult for the US.

Not wanting to be slowed down by Congress, the Obama Administration has identified internet privacy as an important issue for the United States economy. The discussion draft of a Consumer Privacy Bill of Rights represents one of the Administration's most concrete efforts to date for creating a comprehensive legal framework regulating online privacy. It aims to fill in the gaps left by prior more targeted executive orders and laws that discuss the issue, and create a consistent nationwide policy governing privacy issues.

The Proposal requires businesses to adopt 'reasonable' privacy practices which are evaluated according to seven key factors. It also encourages businesses to participate in a multi-

stakeholder process that may tailor targeted codes of conduct for specific industries.

If the Proposal is enacted, many businesses may want to contribute to the development of the codes of conduct so that they can reduce the amount of disruption that the law's requirements would create. If a business follows an approved code of conduct, it will not be liable for violating the Proposal. Finally, while the Proposal does not permit private lawsuits, the FTC would have the power to impose significant fines on companies that violate it.

Notwithstanding the chances of the Proposal becoming law, it does signal the Administration's position on commercial data use and collection. Therefore, it will be important for businesses to engage in any discussion leading to revisions of the draft Proposal and understand its requirements. Businesses may also want to incorporate the basic principles articulated in this Proposal into their current privacy practices, since the Administration may try to implement some of these requirements through other government agencies despite the current gridlock in Congress.

Other executive level action

The Federal Communication Commission ('FCC') has dramatically increased its enforcement of data security practices and breaches resulting from what the FCC sees as inadequate security measures.

For example, the FCC entered into a $25 million settlement with AT&T Services, Inc. ('AT&T') resulting from the unauthorised access to personal customer information by employees of foreign-based call centres under contract with AT&T. The FCC again stressed that it expects telecomm unications companies, which now includes broadband internet access providers, to take 'every reasonable precaution' to protect their customers' data.

Where does it go from here?

At a macro level, the US provides an opportunity to see whether sector-specific laws, coupled with industry self-regulation, executive-branch action, and tough and active regulators like the FTC and FCC, make for a more nimble, freer and more commerce-friendly environment than the uniform and blanket approach adopted by the EU.

One possible outcome is a 'meeting-in-the-middle' kind of result, where the US takes a more data subject centric approach, while the EU takes further action on reactive types of activity (e.g. data breach notification).

Perhaps at that point we will begin to speak a common privacy and security language.

Ann Bevitt and Randy Sabett
Cooley (UK and US) LLP
abevitt@cooley.com
rsabett@cooley.com