International Privacy – 2013 Year in Review – European Union

By BakerHostetler on December 30, 2013

Authors: Gonzalo Zeballos, James Sherer, and Alan Pate

Fighting the war on two fronts:

External

Outside of the EU, concerns continue after the former NSA contractor Edward Snowden leaks demonstrated issues related to U.S. handling of European data. Beginning in July, 2013, the ongoing Transatlantic Trade and Investment Partnership (TTIP) talks were seen as a focus of cross-border interoperability, with Germany initially applying internal pressure to include commercial spying rules during the negotiation before Viviane Reding, EU Justice Commissioner and vice-president, confirmed that data protection would not be part of the negotiation. In contrast, Ms. Reding stated that the EU expects that the U.S. will pursue “necessary legislative change” by the summer of 2014 to allow EU citizens the “right of judicial redress” to sue in the U.S. if EU citizen data is misused, a right “[e]very U.S. citizen in the European Union already enjoys...irrespective of whether he or she is resident in the EU.”

The European Commission (EC) released a memorandum relating to EU-U.S. data flows on November 27, 2013, focused specifically on “large-scale U.S. intelligence collection programmes,” which “have had a negative impact on the transatlantic relationship.” There, the EC reported on findings of the July 2013 EU-U.S. Working Group and analyzed the function of the current EU-U.S. safe harbor, which has been in place since 2000. In contrast, the United States has indicated that the current safe harbor “remains an effective way of protecting online data for both American and European consumers.”

Despite differences in approach and philosophy, the EU and the U.S. are working toward completing an agreement by mid-2014 that would protect the private data of individuals while still sharing information for law enforcement purposes; this follows talks that began in 2011 and have survived 15 negotiating rounds.

Internal

The Snowden affair has galvanized some internal activity within the EU, where in-process data privacy legislation has been gridlocked for nearly two years due, in part, to U.S. pressure. Previously, the U.S. had successfully lobbied for easing of data transfer rules, but tight data transfer regulation was reintroduced, which proscribes...
those practices unless explicitly allowed. Such lobbying was explicitly noted as sometimes being “counterproductive” in the context of EU data protection that was, instead, strengthened by the European Parliament.

On October 21, 2013, the Committee for Civil Liberties, Justice and Home Affairs’ (LIBE) Members of European Parliament (MEPs) voted 49-1 (3 abstentions) on changes to current EU data protection rules to replace the current patchwork of national laws. The proposed law would take the form of a Regulation, rather than a Directive, and the changes include a number of modifications and clarifications, including:

- Moving from an individual Member State-by-State national regulation scheme to a pan-European “one-stop shop” data protection law.
- Providing an estimated €2.3 billion per year in benefits.
- Reiterating the “right to be forgotten” while still mindful of “the right of erasure,” a lower bar of compliance that recognizes the now-impossibility of entirely removing an individual’s traces from the Internet and provides for the reality of freedom of speech.
- Defaulting to “Privacy by Design” and “Privacy by Default” as “essential principles in EU data protection rules,” where safeguards are built into products and services from the ground-up, and privacy-friendly default settings are the norm.
- Increasing imposed sanctions (fines) of up to 5% of annual worldwide turnover or €100 million (whichever is greater) on organizations that break the rules.
- Seeking limits to user profiling that would require organizations to detail prospective customer data use prior to its use. These requirements focus on the collection of the minimum amount of data to achieve the organization’s purpose in its collection, and a higher bar for the clarity the organization uses to explain the data’s use.
- Requiring EU supervisor approval before unblocking data-sharing with non-EU countries.
- Providing the “same rules for all companies – regardless of their establishment,” requiring organizations based outside of Europe to apply the same rules.
- Easing requirements for the data protection requirements associated with small and medium enterprises (SMEs), where SMEs may be exempt from regulations requiring a Data Protection Officer (DPO) if “data processing is not their core business activity,” and charging for excessive or repetitive requests for data.

The approved legislation will be debated among the European Commission, the European Parliament, and the European Council with the goal of an agreement on major legislative reform prior to the May 2014 European elections and legislation in force by 2016. The European Parliament still needs a subsequent vote and agreement with the 28 EU member states, but despite France’s commitment to fast-track the rules (supported by Poland and the European Commission), other member states, including the United Kingdom and Germany, have stressed deliberation on identified issues with the legislation. Based on the U.K.’s concerns, which included UK Prime Minister David Cameron’s statement that the legislation was “wrong” and that the EU “should hold it up so we get it right,” EU leaders dropped a prior 2014 deadline and instead pledged to push forward in a “timely fashion,” saying instead that the regulation and the cyber security directive were “essential for the completion of the Digital Single Market by 2015.”