BNA

Daily Report for Executives™

Internet

Privacy

Laws in the European Union and the United States regarding government access to personal information in the cloud are more harmonious than many in the EU believe. Those governments specifically authorize derogations from individual privacy rights in the interest of protecting national security, combating terrorism, and investigating serious crime, writes Alan Charles Raul, partner in Sidley Austin LLP's Washington, D.C., office. The United States is not an outlier because Europe recognizes the same imperatives to balance data protection and privacy against security and law enforcement needs, the author says. Raul contends that concerns of an EU parliamentarian from the Netherlands—that U.S.-based cloud-computing providers are more exposed to government intrusion than EU providers—do not acknowledge parallels between U.S. and EU law.

Real Harmony in Cloud Computing Between U.S., EU Closer Than You Think

BY ALAN CHARLES RAUL

Given the supra-territoriality of the ''cloud,'' essentially the use of remote (or outsourced) computing power to store, manage and process data, instead of local servers or personal computers, questions of international jurisdiction and conflict of laws pose complex issues worthy of careful thought. In light of the benefits of cloud computing for innovation, efficiency, and convenience, the quest for international harmony in the cloud is well worth pursuing.

Recently, however, Sophia In't Veld, a leading European voice on privacy and EU parliamentarian from the Netherlands, may have shed more heat than light on the subject. She stated her view that U.S.-based cloud-computing service providers might not be able to comply with EU data protection law because of the U.S. government's ability to seek and obtain national security information about individuals without requiring the cloud provider to notify them.

 ISSN 0148-8155

Specifically, Ms. In't Veld expressed concern about whether the alleged conflict between U.S. and EU legal obligations would diminish the force of the EU's Data Protection Directive, which allows member states to restrict privacy rights in the interests of national security. She demanded a response from the EU Commission, Europe's executive branch, asking, ''Does the Commission consider that the U.S. PATRIOT Act thus effectively overrules the EU Directive on Data Protection? What will the Commission do to remedy this situation, and ensure that E.U. data protection rules can be effectively enforced and that third country legislation does not take precedence over E.U. legislation?''

Ms. In't Veld sees a stark conflict of privacy and national security laws across the Atlantic Ocean, and said ''I hope [EU Justice] Commissioner [Viviane] Reding will respond soon, as this is really a key issue. Essentially what is at stake is whether Europe can enforce its own laws in its own territory, or if the laws of a third country prevail. I hope the Commissioner will ensure that the U.S. and other countries respect E.U. laws in E.U. territory. I don't think the U.S. would be amused if Europeans (or other non-U.S. authorities) were to get access to databases located within U.S. jurisdiction.''

The reality, however, is not as Ms. In't Veld sees it. The fact is that governments on both sides approach the balance between privacy and national security in fundamentally the same manner.

The assumption by some in the EU that the USA PATRIOT Act provides some dastardly carte blanche to probe and acquire personal information in a different manner or degree from the laws prevailing in the EU is simply a canard. The EU Data Protection Directive, which is Europe's overarching privacy law, expressly states that ''restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security . . . .''

Article 13 of the directive also specifically exempts ''national security'' from otherwise applicable privacy protections. The article authorizes ''Member States [to] adopt legislative measures to restrict the scope of the obligations and rights . . . when such a restriction constitutes a necessary measures to safeguard: . . . national security.'' Even after the Treaty of Lisbon, which enshrined the right to protection of personal data in the EU, the resulting constitution for the EU expressly leaves in place the right of member countries to impose derogations on personal privacy where necessary for national security purposes.

Member states have indeed availed themselves of this EU right to restrict data protection for individuals, in the name of national security.

'Safeguarding National Security.'

Ms. In't Veld's own country, the Netherlands, has exempted national security matters from data protection obligations. In the Netherlands, the national data protection law states, in Article 2, that ''this Act does not apply to the processing of personal data . . . by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act [or] . . . for the purposes of implementing the police tasks.''

The Dutch carve-out for intelligence and police matters is not unique in Europe. The U.K.'s Data Protection Act provides, under the rubric of ''national security,'' that ''Personal data are exempt from any of the provisions of . . . the data protection principles . . . if the exemption from that provision is required for the purpose of safeguarding national security.''

Similarly in Spain, the privacy law states that ''the system of protection of personal data laid down by this Organic Law shall not apply to: . . . files established for the investigation of terrorism and investigation of serious organised crime.''

Article 24 of that law (''Other exceptions to the rights of data subjects''), addresses precisely the issue most troubling to Ms. In't Veld, namely the risk of denying notice to a data subject under circumstances parallel to the those of the PATRIOT Act. The law in Spain holds that data protection rights ''shall not apply to the collection of data when informing the data subject would affect national defence, public safety or the prosecution of criminal offences.'' In fact, terrorism investigations are *per se* excluded from privacy requirements. Spanish law states that: The system of protection of personal data established herein shall not be applied to files and processing . . . established for the investigation of terrorism and serious forms of organised crime.''

None of this analysis is meant to suggest that privacy must be sacrificed in name of national security—to the contrary. Numerous protections exist in the United States, and presumably also in Europe, to counterbalance and oversee national security investigations. In the U.S., the Constitution, Fourth Amendment, Foreign Intelligence Surveillance Act and other laws and executive orders govern and protect personal information privacy, generating considerable pro-privacy litigation and extensive congressional debate on the proper limits and balance. President Obama is expected to reestablish the White House Privacy and Civil Liberties Oversight Board that Congress mandated to help ensure the right balance.

Numerous other significant safeguards exist in America to constrain, deter and punish excessive government intrusion, including inspectors general, congressional oversight committees, departmental privacy and civil liberties officers, and highly engaged nongovernmental organizations like the American Civil Liberties Union and Electronic Privacy Information Center.

The provisions in the EU legislation demonstrate, however, that the concerns expressed by Ms. In't Veld that users of U.S.-based cloud-computing are inherently more likely to face privacy torments greater than users of European clouds are simply without substance. All governments must try to protect their citizens and lands from terrorism.

National security laws and domestic data protection regimes across the Atlantic, the English Channel, and throughout the euro zone, exempt their respective governments from applying the full measure of personal privacy rights in cases involving terrorism, counterintelligence and serious crime. While the exercise of these powers calls for profound oversight and scrutiny to prevent abuse, the existence of potentially intrusive investigative authority is hardly unique to America. Whether or not some might characterize government surveillance as a ''necessary evil,'' the fact is that it occurs routinely in Europe, as in America.

  DER ISSN 0148-8155

Benefits of Cloud Computing.

This is not idle supposition—Google actually publishes statistics on the number of requests it receives for the personal data of its users from governments around the world. For the most recent period reported, from July to December 2010, the governments of France, Germany, Italy, Spain, the United Kingdom, and yes, the Netherlands, all submitted significant numbers of requests for user data; and their requests do not seem disproportionately more privacy protective than the number of requests received from the U.S. government.

Accordingly, it not useful or accurate to single the United States out as significantly more intrusive on the internet than other governments. The evidence simply does not bear that out, and the rhetoric will only impede digital progress to the detriment of all the world's consumers and information seekers.

Reding, the commissioner invoked by Ms. In't Veld, has herself written that ''consumers and companies benefit from storing information on remote servers, no matter where they are, and then pulling it back when they need it. Our societies have been transformed as users embrace social networks, blogs, newsfeeds and shared bookmarks that are kept in the cloud. Companies cut costs by outsourcing data storage tasks.'' She also acknowledges, of course, that ''data protection is a fundamental right in the European Union [and that] . . . a cloud without robust data protection is not the sort of cloud we need.'' But there should be little disagreement between the U.S. and EU that simpler, more predictable, transparent and harmonized safeguards will foster international data transfers to everyone's benefit—without subjecting either hemisphere to unfair advantage or unwarranted opprobrium.

Cloud computing offers great benefits for individuals, organizations, businesses and governments, and it would be unfortunate to constrain supra-national development of the cloud because of a mistaken view that U.S. national security law is more intrusive and less sensitive to individual privacy than EU law. The facts do not support such a hypothesis, so countries should recognize and promote harmony in their internet policies in order to cultivate innovation and growth in the global digital economy.