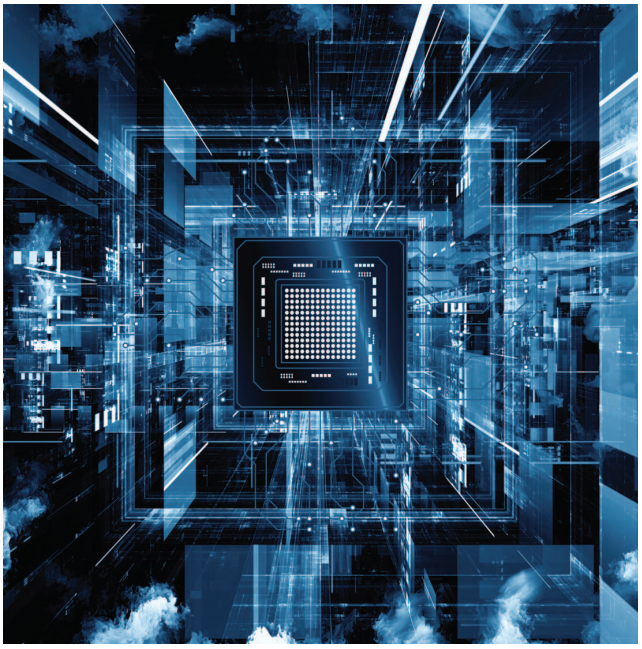

# Cloud Computing and EU Data Privacy Regulations

**Nir Kshetri,** *University of North Carolina at Greensboro*

**San Murugesan,** *BRITE Professional Services, Australia*

**To leverage the cloud's power, EU authorities must revisit policies related to various types of personal data and their associated privacy risks.**

The European Union's Data Protection Directive has been its major legislative instrument for handling consumer data. While the Directive hasn't been revised since its passage in 1995, there have been dramatic changes in the ways personal data is accessed, stored, processed, transmitted, shared, and used. Cloud computing's evolution is among the most influential forces to reshape and modify EU regulations.

While many privacy advocates applaud the EU's data privacy standards, critics are concerned that these standards fail to adequately consider the context of a changing technological landscape. In response to the demands and concerns of various interest groups, the European Commission, which represents the interests of the EU as a whole, has recognized the existing framework's deficiencies and recently announced its new cloud strategy.

However, there are substantial challenges on the horizon for cloud-related EU regulations and their impact on cloud services. These regulations deserve close examination by cloud providers, users, and IT professionals.

## EU DATA PRIVACY REGULATIONS

A key feature of the Directive is that it restricts the transfer of EU citizens' personal data to jurisdictions that lack adequate protection. The Directive is also intended to ensure uniform data protection standards for EU members.

Nonetheless, as a 2003 Gallup survey of European companies revealed, there is substantial heterogeneity among EU member states in implementing and interpreting data privacy regulations. For example, maximum penalties for the misuse of personal information vary considerably. In Spain, the penalty is €600,000; in France, it's €150,000 for a first offense plus five years in prison; and in Germany, it's €250,000 (D.C. Dowling, "International Data Protection and Privacy Law," Aug. 2009; http://tinyurl.com/bgh4fza).

While the EU regulations have several strengths, they also suffer from major limitations (N. Robinson et al., *Review of the European Data Protection Directive*, tech. report, RAND Corp., 2009; http://tinyurl.com/by7swsw).

A key strength of the Directive is its principle-based framework, which provides a model for good practices. Second, the Directive harmonizes data protection rules and to some extent enables EU-wide

 Published by the IEEE Computer Society 

transfers of personal data. Third, it allows EU members to vary requirements to suit local circumstances. A fourth benefit is its technology-neutral approach. Finally, the Directive has increased public awareness of the importance of data protection.

A major weakness of the Directive is that it doesn't clearly link the concept of personal data to real privacy risks. In addition, critics argue that the EU model's outmoded rules and cumbersome procedures hinder data transfer to other countries for storage and processing. Moreover, the Directive lacks consistent and effective measures to provide data-processing transparency through information and notification.

Another drawback is inconsistent accountability and enforcement among member states' data protection authorities. A further criticism concerns the Directive's overly simplistic and static approach to defining entities involved in processing and managing data. Finally, these and other weaknesses pose practical implementation problems.

## THE NEW EU CLOUD STRATEGY

To address the Directive's shortcomings, the European Commission has developed a new cloud strategy (*Unleashing the Potential of Cloud Computing in Europe*, Sept. 2012; http://tinyurl.com/cchnqpz) that focuses on three key areas:

- the European Cloud Partnership, which brings together public authorities and industry bodies to develop a common regulatory framework;
- cloud computing standards and certification, the main component of which is to introduce pan-European certification schemes; and
- model contract terms for cloud computing that address issues such as data preservation after contract termination, disclosure and integrity, ownership, location, transfer and interprovider portability of data, and subcontracting.

The Commission's strategy also allows data protection authorities to approve binding corporate rules as well as industry codes of conduct that are specifically tailored to cloud computing. Further, in light of concerns related to the handling of EU citizens' data in non-EU countries, the Commission emphasizes the importance of collaboration and coordination with India, the US, and other countries on issues related to law enforcement agencies' access to data and development of appropriate cybersecurity frameworks.

Finally, the Commission seeks to leverage the expertise and resources of the EU's advisory bodies. For example, the European Network and Information Security Agency (ENISA), a center of network and information security expertise for the EU, is expected to facilitate the voluntary certification schemes in the cloud.

The EU considers cloud computing an enabler of national and regional competitiveness. According to an EU press release, implementation of all the key elements in the new cloud strategy would lead to a net annual gain of €160 billion to EU GDP by 2020 (http://tinyurl.com/b9ovwks). In addition, pressures and ideas generated by various stakeholders are shaping the formulation and implementation of the EU's cloud policy. Table 1 summarizes these forces.

## EU VERSUS US APPROACHES TO DATA PRIVACY

The EU has set a baseline level of data privacy rights irrespective of data location. The US, on the other hand, follows a self-regulatory approach and has sector-specific regulations for handling sensitive data. For example, to comply with the 2002 Sarbanes-Oxley Act, public companies must have controls to ensure that data is accurate and protected from unauthorized changes. Likewise, the 1996 Health and Human Services Health Insurance Portability and Accountability Act requires healthcare providers to have measures in place to protect the privacy, integrity, and availability of patients' data. Those not complying with HIPAA face fines up to $250,000 and 10 years in prison.

In the cloud context, the USA Patriot Act of 2001 has been of particular concern. There's a deep-rooted perception among some EU-based consumers and activists that US cloud service providers are required to disclose data stored in clouds to their government without the data owner's consent or knowledge. Ironically, the veracity of such claims is less relevant than the fear itself, which can be damaging to US cloud vendors' reputation.

While US officials and vendors assert that such concerns are exaggerated, convincing EU-based customers and activists that the Patriot Act doesn't present a risk has been a challenge for US providers (D.S. Rauf, "Patriot Act Clouds Picture for Tech," *Politico*, 29 Nov. 2011. http://tinyurl.com/dy4lhcc).

Some EU vendors exploit this anxiety, declaring that they provide "a safe haven from the reaches of the Patriot Act" (A. Lakatos, "The USA Patriot Act and the Privacy of Data

**Table 1. Key forces driving EU cloud policy.**

| Key players | Motivations | Example actions |
|---|---|---|
| Vendors and industry groups | Bring about changes in cloud-related policies and regulations in the EU and its member states to promote regional competitiveness, flexibility, growth, and innovation. | Oracle, Cisco Systems, SAP, Apple, Google, and Microsoft have all lobbied to streamline EU's fragmented national data protection laws. On 24 January 2011, Brad Smith, Microsoft's general counsel, appealed to the French National Assembly to lower cloud barriers.<br><br>In August 2011, the European Telecommunications Network Operators' Association (ETNO), which represents 41 large telecom operators in 34 European countries, lobbied for an international online privacy standard and simplification of rules governing data transfers. It argued that these measures would enable European companies to compete on the same level as those in the US.<br><br>In January 2012, Andy Mulholland, CTO of Cap Gemini, a Paris-based IT services company, expressed concern that most of the major cloud providers in Europe are US-based companies and argued that revision of EU data laws would help these companies to sell cloud services to European users. |
| Activists, interest groups, and user representatives | Ensure reliability and availability of cloud services as well as a high level of data protection from various threats. | In December 2012, the European Parliament published a report emphasizing the importance of opening EU-US negotiations on data privacy in the cloud.<br><br>In January 2013, Gus Hosein, head of the UK-based NGO Privacy International, declared that US surveillance and spying agencies' possible access to EU citizens' data stored in US companies' clouds is "an irreversible loss of data sovereignty."<br><br>On 25 January 2013, Caspar Bowden, a former Microsoft privacy chief, warned during a panel discussion at the 6th International Conference on Computers, Privacy, and Data Protection (CSDP 13) that new EU data protection law proposals have no provisions addressing data privacy in cloud computing. |
| EU national governments | Prevent EU domination of cloud-related policies.<br><br>Respond to demands to harmonize and align legal systems and enforcement mechanisms with those of other EU member countries. | In an October 2012 questionnaire addressed to the national parliaments of the EU, Romania's Committee for Information Technologies and Communications expressed its view that the new EU data protection framework would significantly increase administrative and financial burdens on private data controllers. The committee also argued that some of the proposed obligations need to be analyzed further to look for the possibility of reducing additional burdens (http://tinyurl.com/bf5u6bd). |
| EU and other international organizations | Respond to pressures from vendors, industry groups, consumers, activists, and others.<br><br>Provide an environment that promotes the use of cloud computing, thereby contributing to the economic growth of member countries.<br><br>Harmonize and align legal systems and enforcement mechanisms. | In September 2012, the European Commission published *Unleashing the Potential of Cloud Computing in Europe*, a landmark report outlining a new cloud computing strategy for the EU. |

Stored in the Cloud," *Mayer Brown*, 18 Jan. 2012; http://tinyurl.com/b2bqh53). Others offer EU's strict regulations as a selling point. For example, online data storage provider HiDrive emphasizes that its data is hosted in Germany and its services conform to strict German laws.

US vendors' responses to these efforts have sometimes only reaffirmed Europeans' apprehensions. For example, during the Office365 launch

in 2011, Microsoft UK's managing director reportedly admitted that the corporation's UK subsidiary was subject to the Patriot Act (A. Lakatos, "The USA Patriot Act and the Privacy of Data Stored in the Cloud"). Such comments can undercut faith in US cloud vendors. In December 2011, for example, the UK's BAE Systems opted not to use Office365 due to concerns about the Patriot Act (C. Saran, "BAE Systems: Office365 Doesn't Fly," *ComputerWeekly*, 5 Dec. 2011; http://tinyurl.com/bbhjl2a).

## IMPACT ON EU AND NON-EU CLOUD PROVIDERS AND USERS

A significant disparity exists in the EU between cloud vendors' claims and users' views of the cloud's security, privacy, and transparency. According to Cisco's summer 2011 *CloudWatch* report for the UK, 76 percent of respondents cited security and privacy as a top barrier to cloud adoption, and 64 percent were concerned about data location (http://tinyurl.com/b4atybp). Critics also argue that the regulatory compliance requirements have imposed inefficiencies and acted as a barrier to the cloud's development. They also note that market fragmentation and the lack of economies of scale make pursuit of innovative solutions unattractive.

These concerns are reflected in the relatively slow growth rate of the EU's cloud industry. IT research firm Gartner estimates that, by 2016, North America, led by the US, will account for 58 percent of global public cloud spending of $779 billion, compared to 22 percent for Western Europe (E. Anderson et al., *Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 2Q12 Update*, Aug. 2012; http://tinyurl.com/bzkpcen).

Europe also has far fewer established cloud providers. While US-based providers must customize applications to meet EU requirements, they're often in a better position even after considering adaptation costs due to their experiences in the home country (unclear EU cloud regulations have led to low adaptation costs). Further, EU regulations have enabled US providers to revise their privacy policy and practices (K.J. O'Brien, "Dismayed at Google's Privacy Policy, European Group Is Weighing Censure," *The New York Times*, 7 Dec. 2012; http://tinyurl.com/bgxwt8b).

The European Commission's proposed cloud computing strategy would directly address cloud users' risk perceptions. Its standardization and certification initiatives would make it easier to signal and verify compliance. Further, the Commission supports the development of cybersecurity standards and will assist with EU-wide voluntary certification schemes in the area of cloud computing, while taking into account the need to ensure data protection (http://tinyurl.com/adnt583). In addition, the possible increase in compliant cloud services due to the new regulations will raise competition and might decrease the cost of cloud services for EU users.

The new cloud strategy also addresses the market fragmentation inherent in EU countries' multiple jurisdictions, which could lead to the growth of local cloud firms. A further mechanism contributing to the development of local cloud providers is the increased demand for their services as they address users' privacy, security, and reliability concerns.

The proposed cloud regulations could have both negative and positive effects on foreign cloud firms offering their services in the EU. On one hand, local cloud firms could emerge as strong competitors to foreign companies due to better knowledge of local market needs and preferences. On the other hand, certification of compliance with EU regulations could ameliorate the negative bias against US-based firms regarding data privacy.

In response to the growing demands and concerns of stakeholders in the EU cloud computing scene, new initiatives are likely to emerge that address major shortcomings in current practices. To leverage the cloud's power, EU authorities must revisit policies related to various types of personal data and their associated privacy risks. They must also address existing inconsistencies in interpreting and enforcing data privacy laws among member countries.

***Nir Kshetri*** *is an associate professor at the University of North Carolina at Greensboro and a research fellow at the Research Institute for Economics and Business Administration at Kobe University, Japan. Contact him at nbkshetr@uncg.edu.*

***San Murugesan****, Cloud Cover column editor, is the director of BRITE Professional Services, Australia, and an adjunct professor at the University of Western Sydney. Contact him at san1@internode.net or follow him on Twitter @santweets.*