Practical Law™
MULTI-JURISDICTIONAL GUIDE 2013/14
OUTSOURCING

Big data and cloud solutions: implications for sourcing

John Barton and Michael Murphy
Pillsbury Winthrop Shaw Pittman LLP

global.practicallaw.com/1-552-4111

Many enterprises are searching for ways to unlock value through data analytics and the use of big data analytical techniques. To do this, enterprises can draw on multiple internal and external sources of data and processing, potentially involving internally hosted data sets, cloud-based processing solutions and traditional externally sourced or outsourced services. These complex projects can create equally complicated contractual relationships. The challenge for sourcing lawyers is to ensure that sourcing procedures and contract terms are adapted to address this complexity.

Big data involves drawing data from a potentially wide variety of data sets that, historically, were not designed to be combined. Big data applies analytical tools and processes to those data sets to see if meaningful correlations and relationships exist. Value is created when actionable insights are drawn from the analysis. The data sets can be drawn from either:

- Separate systems within a single enterprise (for example, from CRM and ERP systems).
- External systems and data sources (for example, market analytics firms, geospatial records, government records and weather systems).

Underpinning big data are the key enablers of cheap and massively scalable computing power and an exponentially growing ecosystem of networked (and therefore potentially accessible) data.

In a big data project, a company may wish to gain insights about its customers by analysing browsing and purchase data drawn from many sources. For example, the company might analyse data from:

- Its internal systems.
- Customer interactions managed by an outsourced call centre.
- Demographic or geographic data drawn from independent websites and data sources.

If the company requires third party expertise to conduct the project, it can engage consultants or take advantage of the many analytics-as-a-service solutions that have emerged. These range from specific data or transaction types to generic capabilities in enterprise platforms including SAP, Oracle and Microsoft.

The company may also wish to use several different cloud-based solutions in conducting its project. For example, the company can:

- Collect data from CRM systems, website comments, social media sites and other systems often hosted in the cloud.
- Store the data collected in a public cloud to obtain optimal pricing and scalability.

These cloud-based solutions raise important issues that should be addressed in the sourcing process.

This article provides checklists of issues that the company should consider when conducting a project of this nature.

BASIC DEAL TERMS

In relation to basic deal terms, the following issues should be considered:

- Is it clear how the service will be implemented? Niche providers of cloud-based solutions offer relatively fast and cheap implementations with minimal up-front investments of time or effort. These solutions can be ideal for companies engaged in rapid, highly iterative R&D. However, niche providers may not be able to integrate with other proprietary solutions, and this could impede later efforts to share and exploit data in new ways. The company should evaluate the adaptability of these external analytics and data sources.
- Does the provider have a robust processing and recovery infrastructure?
- Are there service availability and response time service levels?
- Does the provider's solution and pricing allow the company to scale (up and down) its usage of services and data storage?
- Are pricing/licensing metrics and counting rules clearly defined?
- Does the company have the rights to allow its employees, affiliates, third party contractors, partners and customers to access or use the provider's service?
- Are there limitations on how or where the company can use the service or the deliverables produced by the service?
- Does the company have rights to renew the contract (and/or protection against large price increases)?
- Does the provider commit to provide reasonable disengagement assistance at the end of the contract term, most importantly by returning all company data to the company?
- Does the provider offer performance warranties, indemnities, confidentiality and other basic protections that any company should expect in its service contracts? Most providers insist that their customers work from their form contracts, which typically offer little if any protection to their customers. However, with some negotiating pressure they may be open to negotiating more favourable terms.

DATA USAGE RIGHTS AND RESTRICTIONS

The company should verify that the data is not subject to restrictions that would prevent its use in the project. This requires an understanding of:

- The type and source of the data.
- The specific ways in which the data will be used.
- The scope of disclosure or consent given to or by the data subject (for personal information).
- Any contractual restrictions on its use (for non-personal information).

Personal information raises particularly sensitive concerns:

- **Privacy policies.** Companies in the United States (US) are generally obliged to notify individuals about the data they collect, and to comply

with their published privacy policies. Companies that violate this obligation may face enforcement action by the Federal Trade Commission (FTC). See *www.ftc.gov/opa/reporter/privacy/privacypromises.shtml* for links to numerous legal actions taken by the FTC against organisations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information.

- **Anonymisation of data.** Service contracts sometimes allow the service provider to use its customers' data in an aggregated or anonymous format for the provider's own purposes. This can be problematic. In recent years, computer scientists have demonstrated that anonymised data can be "re-identified" by linking anonymised records to outside information (*Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization; Paul Ohm; 57 UCLA L. Rev. 1701 2009-2010*). Companies that permit their providers to use data in an anonymised manner should ensure that the providers assume the associated risk and liability (through indemnities and exceptions to limits of liability) if the data is ultimately re-identified with the company's customers.
- **EU regulations.** If the data relates to particular individuals in Europe, the company can only use it for the specific purpose for which it was collected and must, among other things:
  - maintain the accuracy of the data;
  - destroy the data when its specific purpose is over;
  - give data subjects access to the data collected and disclose with whom the data is shared; and
  - keep data secure from unlawful processing.
- The primary regulations to consider in this regard include:
  - Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive);
  - Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (E-Privacy Directive).

In addition, a new EU General Data Protection Regulation under consideration that may both:

- Extend protection to new types of data.
- Address inconsistencies in the way in which the existing Data Protection Directive has been implemented and enforced across the EU member states.

(See *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final (25 January 2012).*)

- **US regulations.** In contrast to the broad-based approach taken in Europe, the regulations that govern the use of big data in the US are focused on particular industries and data types. For example:
  - the following regulate protected health information of individuals:
    - Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 *et seq.* and 42 U.S.C. 1320d *et seq.*;
    - Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (17 February 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq..
  - Fair Credit Reporting Act (FCRA) and Fair and Accurate Credit Transactions Act (FACTA) 15 U.S.C. § 1681 et seq. are designed to promote the accuracy, fairness and privacy of information in the files of consumer reporting agencies, and to regulate the use and dissemination of consumer reports;
  - Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (Pub.L. 105–277, 112 Stat. 2581-728, enacted 21 October 1998) is designed to protect the privacy of children under 13 on the Internet;
  - Gramm-Leach-Bliley Act (Public Law 106-102, 15 U.S.C. § 6801, et seq. and 16 C.F.R. § 313, 65 Fed. Reg. 33646 (24 May 2000)) requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data. Financial institutions include companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance;
  - Additional industry standards and rules may also apply. For example, the company will have additional restrictions on its right to use customer data under the Payment Card Industry Data Security Standard imposed by the card networks.
- **Regulatory trends.** Lawmakers continue to revise and supplement existing regulations to balance individual privacy rights and the commercial and societal benefits that can be derived from data analytics and data sharing. The European Commission, the US government, US Federal lawmakers, the FTC and numerous states are considering further changes to laws that affect big data, including laws relating to:
  - data subject notice and consent;
  - do-not-track rules;
  - data retention and the "right to be forgotten".

CONTROL AND PROTECTION OF DATA

In relation to the control and protection of data, the following issues should be considered:

- Where will data be stored and who can access it (and from where)? Data that is accessed or stored offshore can raise regulatory issues, intellectual property risk and business continuity challenges.
- Does the provider maintain adequate security controls and verify those controls through external certifications (for example, ISO 27001) or regular audit reviews (for example, SSAE 16)? Does the company have the right to audit these controls?
- Does the company have an absolute right to get its data back in a usable format without conditions, even when breach of contract is alleged?
- Are there restrictions on the provider's right to subcontract services? If the provider has the right to subcontract:
  - how will the company know who is accessing and managing its data?
  - does the contract require the provider to flow-down applicable terms to its subcontractors? Typical flow-down provisions include terms relating to data protection and data security, disaster recovery, ownership of data and intellectual property, indemnity and insurance.
- Subcontracting may trigger additional regulatory compliance requirements. For example, a HIPAA business associate agreement may be required if the provider will access protected health information. Companies operating in Massachusetts must require their providers to commit to implement and maintain security measures when their services access personal data (*see The Massachusetts General Law Chapter 93H and its new regulations 201 CMR 17.00*). Companies operating in the EU will need to ensure their providers are safe harbour compliant or include model clauses before allowing a transfer of data outside the EU.
- Are the risks associated with a data security incident fairly allocated? For example, can the company recover the costs of conducting forensic audits to identify compromised data files, notifying customers, providing credit monitoring services and identify theft insurance, and similar costs likely to be incurred? The cost of a data breach in the US averages US$188 per record or a total of US$5,400,000 per incident, according to

the Ponemon Institute's 2013 Cost of Data Breach Study. Companies that fail to use adequate security measures to protect customer data may also be subject to FTC enforcement action (*Federal Trade Commission v. Wyndham Worldwide Corp., NO CV 12-1365-PHX-PGR. Filed in US District Court, D. Arizona, March 25, 2013 (FTC Complaint)*).

- Are there limits on the provider's right to use the company's data? The use of anonymised data could raise privacy concerns if that data can be re-associated with individuals. Further, analysis of aggregated data could provide insights into the company's business, market strategies or market position.
- Does the company and/or provider have cyber-insurance that covers loss and liability resulting from data breaches?

CONTROL OF ANALYSIS AND LOSS OF COMPETITIVE ADVANTAGE

If the service provider's proprietary processes or data are used in the analysis, the provider may expect to own or have usage rights in the resulting analysis. In those cases the company should assess whether:

- Its intended use of any data or analysis might exceed the scope of use permitted by the provider. Many providers prohibit or restrict the repackaging, recombination or resale of their proprietary data and analysis.
- There could be a leakage of business intelligence that is of competitive value to the company.
- The company may find itself dependent on critical data or processes that it cannot obtain from any other source.

Big data analytics, combined with the power of cloud computing, offer tremendous potential benefits and opportunities in commerce, research and government. Although the sourcing arrangements can be complex, they are manageable. The regulatory environment, particularly relating to the protection and privacy of personal data, is fluid and lawyers will need to monitor regulatory trends closely.

Practical Law Contributor profiles

John Barton, Partner

Pillsbury Winthrop Shaw Pittman LLP
T +1 202 663 8703/+1 713 276 7600
F +1 202 663 8007/+1 713 276 7673
E john.barton@pillsburylaw.com
W www.pillsburylaw.com

Professional qualifications. Attorney, California, District of Columbia and Texas

Areas of practice. Technology; IT; outsourcing; data privacy.

Michael Murphy, Partner

Pillsbury Winthrop Shaw Pittman LLP
T +1 415 983 1303
F +1 415 983 1200
E michael.murphy@pillsburylaw.com
W www.pillsburylaw.com

Professional qualifications. Attorney, California and New York

Areas of practice. Technology; IT; global sourcing; data privacy.