Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Key Legal Issues In Contracting For SMAC Services

Law360, New York (June 03, 2014, 10:04 AM ET) -- This article is a scan of key legal issues for companies sourcing what are popularly called SMAC: an acronym for social media, mobile computing, "big data" analytics and cloud computing. SMAC service providers deliver insights that sell products, increase efficiency, improve outcomes and otherwise generate value by capturing the digital exhaust from social media interactions and mobile devices and then analyzing that digital exhaust with specialized software powered by cloud computing engines.

The convergence of the SMAC technologies is having a revolutionary impact on business, creating enormous opportunities for those that embrace them and serious risks for those that fail to do so, or that overlook the legal pitfalls that SMAC technologies introduce. While the full ramifications of SMAC services in any area or industry are not yet known, we do know that SMAC and the big data output from SMAC services have, and will continue to have, a substantial disruptive effect on businesses and, as with other major shifts in technologies, some companies will be winners and others will be losers.

None of these SMAC services is entirely new. For example, credit reporting agencies have for many decades generated insights for lenders by using powerful computer systems to analyze the digital exhaust of transactions by consumers in various locations. The difference now is in the recent, extraordinary growth in volume, variety and velocity of the data being generated and analyzed, and the stunning reductions in the cost of doing so. Statistics abound. For example, IBM estimates that 90 percent of the data ever stored was stored in the last two years.[1]

Laws written before these SMAC technologies and capabilities existed are ill-designed to address some of the risks from SMAC services. Similarly, many companies are unprepared to deal with the issues that evolved along with these technologies. Our goal in this article is to help identify those legal issues and associated risks and to provide recommendations on how to be among the winners in the SMAC revolution.

Reduce Restrictions on Your Rights to Use Data

When your company wants to use, analyze and commercialize data gathered in the course of its business, will it have the rights to do so under its contracts? There are a number of traps that can block a company's right to use the data, including confidentiality and intellectual property provisions and restrictions on use of data. Some of these restrictions may be in signed contracts, but others may be in your company's own publicly stated privacy policies. We recommend reviewing your contracts and stated policies now to reduce the risk that old provisions will restrict use or analysis rights that will be important for your company as you increase your use of SMAC services.

Reduce Data Value Leakage and Increase Data Value Gains in Supplier Contracts

With the broad expansion of third-party service contracts, ranging from full outsourcing of IT and business process functions to SMAC services, there is a risk that the rights to valuable data generated about your company's business could be forfeited to service providers, or that you could enable service providers to gather and use the most valuable insights from the data. We recommend reviewing your service provider contracts and forms and developing provisions for addressing data rights and licenses to preserve value for your company. In addition, we recommend considering your prospective service providers as a valuable source of data and analytics as a result of their provision of similar services for others, and making that a part of the value measures you will be evaluating in choosing service providers generally.

Protect Your Databases

Intellectual property protections for data and insights vary by country. The laws in European countries confer IP rights in databases but also give protections to individuals, referred to as data subjects, to obtain information about, and in some cases require the removal of, their data in your databases. EU laws also limit the use and transfer of personal data, though these restrictions do not apply to anonymized data. These IP rights in databases, as well as the data subject rights, do not exist in the United States, which instead relies on a patchwork of federal and state laws to protect data rights and the privacy of individuals.

Consequently, the protection of competitively sensitive information data in the United States relies on practical security protections and trade secrecy laws. Unlike copyright protection in the United States, trade secret laws (which vary by state) require that the data actually be secret, and that it be subject to reasonable measures to preserve that secrecy in your company's handling of that data and in the contracts that enable access of that data to any third party. In some cases, it may be more practical to use these protections for the distilled, integrated or analyzed data and insights resulting from SMAC analytics.

As is common with new technologies, enthusiasm for the possible value of SMAC services runs ahead of caution about the risks. There are a host of technical issues in distinguishing between insights and errors, including the accuracy of the data and the proper interpretation of correlations found in the analysis.

With the variety of laws across countries and the rapid expansion of SMAC services, managing data protection and compliance with laws in an international economy is becoming increasingly challenging.

Caution in Applying Results of Analysis

As is common with new technologies, enthusiasm for the possible value of SMAC services runs ahead of caution about the risks. There are a host of technical issues in distinguishing between insights and errors, including the accuracy of the data and the proper interpretation of correlations found in the analysis. There are also reputational and legal risks associated with errors, particularly when used to make decisions that affect individuals or customers.

Errors are a real problem. A recent study found material errors in 26 percent of the 1,000 consumer credit reports analyzed, these being problems serious enough to affect consumers' credit scores.[2] While consumer credit agencies are protected against liability under the Fair Credit Reporting Act, so long as they comply with its requirements, other users of SMAC data do not enjoy the same statutory protections against errors.

Even if the data and insights are accurate, actions taken based on the insights could still violate laws. A recent Reuters news article reported that an upcoming White House report will focus on concerns about how big data technologies "could end up reinforcing existing inequities in housing, credit, employment, health and education."[3]
There are numerous possibilities where social media activities or mobile device locations could be profitably correlated with business decisions but result in historically disadvantaged groups facing further disadvantages. We likely will see new laws and expanded interpretations of existing laws that make companies liable for activities that today appear permitted by law.

Due to the risk of errors in SMAC data and analysis, and the increasing regulatory attention paid to these issues, lawyers should ensure appropriate compliance oversight when using and applying the output of SMAC data. This compliance oversight should focus not merely on current laws, but on avoiding harm that might later be found to result in legal liability.

Risks in Amassing Big Data

If you read the business and IT press, you come away with the conclusion that more data is always better than less data. Legally, however, that conclusion is less clear. Privacy laws have minimization standards requiring that personal data not be retained longer than the period of its usefulness and not be used for unintended purposes. The cost of a data breach depends on the amount and value of data. Similarly, the cost of electronic discovery is directly proportional to the amount of relevant electronically stored data. Also, the more data your company has, the harder it will be to argue that you did not have reason to know of product defects and other dangers, potentially increasing the range of foreseeable harm.

For these reasons, companies should pay careful attention to their data retention policies. You may find that those policies were written before you began collecting data generated by social media and mobile devices, and, thus, require an update. You might find that you can materially reduce risk without materially reducing value by anonymizing data, though it is becoming increasingly difficult to anonymize data in a way that cannot be de-anonymized by combining it with other available databases.

Conclusions

You can help your company succeed in our evolving economy through smart contracting for SMAC services. However, to mitigate the risks while delivering the value of SMAC services, we recommend that you review your contracts to secure the data rights you need, protect data with contractual, operational and legal defenses, and manage the legal risks that can come with amassing SMAC data and acting on the findings gleaned from that data.

—By Brad L. Peterson and Paul J.N. Roy, Mayer Brown LLP

Brad Peterson and Paul Roy are partners in Mayer Brown's Chicago office.

[1] John Marshall School of Law Information Technology & Privacy Law Journal, Vol XXX, Prism & European Union's Data Privacy Protection, p. 230; see also Joe Pappalardo, NSA Data Mining: How It Works, Popular Mechanics (Sept. 11, 2013).

[2] How the Fair Credit Reporting Act Regulated Big Data by Chris Jay Hoofnagle; Future of Privacy Forum, September 10, 2013, Stanford Law School, The Center for Internet and Society.

[3] How While House looks at how 'Big Data' can discriminate, Reuters Mobile, April 26, 2014, reporting by Roberta Rampton; http://www.reuters.com/article/idUSBREA3Q00M20140427.
