VLP LAW GROUP LLP

VLP Partner Michael Whitener Co-Authors Article in *The Privacy Advisor*

In Praise of "Little Data"
April 22, 2013

By Michael Whitener, CIPP/US, CIPP/C, CIPP/E, CIPP/G, CIPP/IT, and Malavika Jayaram

As the media constantly remind us, we're in the age of Big Data. We face a tsunami of data so large we have to keep inventing new terms to measure it—exabytes, zettabytes, yottabytes. According to IBM, which should know, 90 percent of the data existing in the world today has been created in the last two years alone.

New tools for analyzing and visualizing Big Data can help promote business efficiency and responsiveness, combat crime, clean up the environment and provide better healthcare. With information being the currency of the digital age, no wonder we hunger to amass more and more of the stuff.

But when personal information is involved, Big Data can bring big headaches. Both customer expectations and privacy laws obligate collectors of personal data to maintain its security and provide notice and choice regarding how it is obtained, used and shared. The costs and consequences of data breaches can be colossal, and the "informed choice" approach to privacy compliance is often just a fantasy when massive data sets are involved.

In the hoopla over "Big Data," it can be forgotten that "Little Data" has its virtues. Better known as data minimization or collection limitation, Little Data can be a practical and effective strategy for meeting privacy compliance obligations.

Little Data means going on a data diet. While limiting rather than expanding data hoards would seem contrary to everything that makes Big Data so appealing, it is both well-established in law and a sensible business practice.

Data Minimization in Law and Policy

Data minimization is hardly a new concept. In fact, it has long been enshrined in privacy principles and related laws.

The Code of Fair Information Practices, first developed nearly 50 years ago and still undergirding modern privacy laws, provides, "There should be limits to the collection of personal data." The OECD Guidelines similarly include a "Collection Limitation Principle." The EU Data

Protection Directive addresses data minimization in Article 6: Personal data may only be "collected for specified, explicit and legitimate purposes."

In the Asia-Pacific region, the APEC Privacy Framework dictates that collection of personal information should be limited to information that is relevant to the purposes of collection. In the U.S., the White House's report last year promoting a Consumer Privacy Bill of Rights included "a right to reasonable limits on the personal data that companies collect and retain."

Despite this broad recognition of data minimization as a fundamental privacy principle, it has been overshadowed—particularly in the U.S.—by the "informed consent" model, which dictates that individuals must be informed regarding how their information will be used before collection and their consent obtained to such uses. But Big Data poses a serious hurdle to obtaining informed consent—not only because the data sets are so large, but because the uses to which the data will be put are often not known at the time of collection.

The EU regulation proposed last year, however, may signal a sea change that will give data minimization new prominence. Article 23 of the draft regulation requires data protection "by design and by default" and goes well beyond previous data minimization requirements by requiring that "by default, only those personal data are processed, which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage."

The proposed EU regulation specifically empowers the European Commission to lay down both technical standards and design requirements to accomplish the data minimization goal.

Data Minimization in Practice

The beauty of Little Data is that it can be accomplished, as the draft EU regulation says, "by design and by default." The kinds of sophisticated design and analytical tools that power Big Data can also be employed in the service of limiting unnecessary personal data collection and reducing the amount of personal information in the data that is collected.

There is a growing array of tools for engineering privacy into data collection methodologies. The link between data collected and an identifiable individual can be severed, or at least made difficult to reestablish, by using such techniques as random identifiers and collection of personal characteristics at a low level of granularity. Data can be aggregated so as to preserve its usefulness without allowing for the targeting of specific individuals. Client-centric, as opposed to network-centric, architectures can provide individuals with the ability to store data preferences on their own systems and restrict data disclosure.

The merits of this "privacy by architecture" or Privacy by Design (PbD) approach are increasingly being recognized. If the information being collected is not personally identifiable, it is not necessary to provide complex privacy notifications and choices to customers and others whose data is being collected. Privacy-friendly architectures can render "informed choice" largely irrelevant.

To date, privacy-enhancing technologies focused on data minimization have not gained widespread traction. But the renewed attention on Little Data evident from the proposed EU regulation, together with the privacy challenges posed by Big Data, is likely to force greater

marketplace acceptance. We can expect to see PbD getting embedded into new business systems and IT transformation initiatives on a much wider scale.

Conclusion

The emergence of Big Data has highlighted the challenges of meeting privacy obligations in a world where data—including personal data—is the lifeblood of business. The informed consent model of protecting privacy rights too often provides just a fig leaf. Effective individual notice and choice simply is not realistic when massive data sets get manipulated and transformed in unforeseeable ways. Little Data can provide big dividends as a tool for ensuring privacy compliance.

***Michael Whitener**, CIPP/US, CIPP/C, CIPP/E, CIPP/G, CIPP/IT, is a partner at VLP Law Group, based in Washington, DC, and serves on the IAPP Publications Advisory Board.*
***Malavika Jayaram** is a partner at Jayaram & Jayaram, based in Bangalore, India. They conduct privacy risk assessments, draft corporate privacy policies and advise on cross-border data transfers.*

This story was first published by the IAPP in *The Privacy Advisor* and is reprinted here with permission.

View this article on-line at The Privacy Advisor