Bloomberg Law®

bloombergbna.com

Reproduced with permission. Published April 23, 2018. Copyright © 2018 The Bureau of National Affairs, Inc. 800-372-1033. For further use, please visit http://www.bna.com/copyright-permission-request/

COMPLIANCE

A Tale of Two Data Sets

By Hui Chen

The unfolding story of Cambridge Analytica and Facebook is among the latest reckoning of how much data has been collected by corporations and the use to which they are put. It seems that commercial and political interests are motivated and adept at harnessing the power of data to understand and influence our behavior: where we have been, what we have bought/read/viewed, when we go online and what we browse, how we spend our money and our time, etc. In fact, even before we had heard of Cambridge Analytica or even Edward Snowden, a New York Times article in early 2012 recounted the story of how a data analytics program at Target knew a teenager was pregnant before her father did, based on the pattern of her purchases.

There is, however, another set of data in which corporations seem to show little interest - the data that would be indicative of their own behaviors: how is the enterprise spending its money? What kinds of vendors does it have for what products and services? Who are making what kinds of purchases and when? How are those decisions made? While many corporations collect data to analyze and predict their customers' behaviors, they do not do so with their own behaviors.

The irony first struck me when I worked in the financial services industry. Surely, I presumed, a bank would have very robust financial data. To my astonishment, I discovered that while financial services firms might know everything about their customers' finances, they were not so knowledgeable about their own. Even as they actively monitor the activities of their customers, they seem to have lost all that capability when it comes to monitoring their own activities: how money is spent, who is spending them, what goes on in chatrooms, etc.

This irony is by no means a phenomenon isolated to the financial services industry, but has been a recurring theme among the companies I have seen in my compliance career: business intelligence firms overlooking publicly available information relating to their markets, risk assessment firms failing to grasp data implications on their own risks, technology firms oblivious to compliance applications of the very technology they sell to their customers.

Recently, in a room full of approximately a hundred compliance officers from among some of the most well-known and sophisticated companies, I asked how many of them had real-time visibility to all financial transactions in their enterprises. One person raised his hand. One!

When I worked at the Fraud Section in the Criminal Division of the U.S. Department of Justice, a frequent question from the prosecutors was: ''Is it really that hard for [companies] to get [corporate data such as number and types of disciplinary actions, number and types of vendor, spending in certain categories, etc.]?!'' The incredulity that usually accompanied this question was understandable: many of these firms knew exactly how their customers were spending money, but struggled to even count how many vendors they themselves had. When I have requested such enterprise data from companies, I have often been told ''we just don't have the ability to track these.''

At what point will this ''inability'' be interpreted as ''unwillingness''? In light of all the recent attention on

Hui Chen (www.HuiChenEthics.com) was the Justice Department's first-ever compliance counsel expert before leaving in June to start her own private compliance consulting service. Before she joined the DOJ, Hui served in global senior compliance lead positions at Microsoft, Pfizer, and Standard Chartered Bank.

COPYRIGHT © 2018 BY THE BUREAU OF NATIONAL AFFAIRS, INC.

corporate abilities to collect, analyze, and use data, we may have arrived at that turning point. Prosecutors, regulators, and investors now have mounting reasons to believe that the ''inability'' to monitor its own spending and behavior may be a deliberate choice companies make: yes, we obviously have the technology, know-how, and resources to track and use data to predict and influence behavior, but we will only use them make money, not to prevent fraud or misconduct.

Many have rightly interpreted the Cambridge Analytica story as yet another blaring alarm on data privacy and cyber security fronts. What companies seem to have missed is that it is also a wake-up call to the effectiveness of their own compliance and control functions. The world is becoming increasingly aware of how data and technology can be used to predict and influence purchasing and voting behavior. The question is: why are they not being used to prevent and detect lying, cheating, and stealing?

COPYRIGHT © 2018 BY THE BUREAU OF NATIONAL AFFAIRS, INC.