Trend to Watch in 2013: Reining in Data Brokers

Published on 21 January 2013 by Angela Bosworth in By The Way (BTW)

As 2012 drew to a close, two federal agencies made it clear that they intended to continue their focus on web-based information providers—so-called "data brokers". On December 14, 2012, The FTC issued orders for information from nine companies (Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, Peekyou, Rapleaf, and Recorded Future). The firms were asked to provide the FTC with information about how they collect and use data (namely criminal record data) about consumers: The agency will use the information to make recommendations about the accuracy, collection and use of the information.

The FTC requested details about:
- **the nature and sources of the consumer information the data brokers collect;**
- **how they use, maintain, and disseminate the information; and**
- **the extent to which the data brokers allow consumers to access and correct their information or to opt out of having their personal information sold.**

This order followed other actions taken last year, starting with the March 2012 FTC report 'Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers'. Data brokers were called out in the report and were asked to improve the transparency of their practices and set forth a voluntary framework of best practices based on privacy, consumer control, and increased transparency for the collection and use of consumer data.
Commissioner Julie Brill told the New York Times that data brokers were one of the agency's top three concerns. "I would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used."

The agency upped the ante in June of 2012, when the FTC spanked Spokeo with an $800,000 fine for selling information to employers without taking the required steps to protect consumer information under Fair Credit Reporting Act (FCRA). The Spokeo case was on the heels of letters sent by the FTC to three mobile application marketers, warning that their background screening apps may be violating the FCRA.

To be sure, data brokers are no longer below the radar. A new agency charged with overseeing consumer financial products and services, the Consumer Financial Protection Bureau (CFPB), is jumping on the bandwagon. Created by Dodd-Frank financial reform, the CFPB now shares regulatory authority over the FCRA and data brokers with the FTC. Only data brokers with more than $7 million in annual receipts resulting from relevant consumer reporting activities are subject to CFPB supervision, but there is no minimum annual receipts requirement with respect to enforcement powers under FCRA. And the CFPB has been granted very broad enforcement authority that would allow them to enact new laws to regulate data brokers.

On November 29, 2012, the CFPB flexed some muscle by issuing a bulletin to nationwide specialty consumer reporting agencies (NSCRAs) reminding them of their obligation under the FCRA to provide consumers with free annual consumer report. The CFPB's enforcement team issued warning letters to several NSCRAs, urging them to review practices and procedures to ensure compliance.

What does this mean for businesses and consumers?

Data brokers are certainly being cast as the villains—spies who are stealing your personal information while stalking your every move on Amazon or e-bay. And the FTC and the CFPB are taking steps to expand the

definition of a CRA to include more companies selling data. The reality is that we all benefit from the information sold by data brokers. One example—employment background checks. Companies like EmployeeScreenIQ rely on data brokers to provide information needed and requested by our clients. But while consumer reporting agencies are clearly subject to federal regulation under the FCRA, many data brokers fall between the cracks. For employers, be aware that all background sources are not considered equal. Not sources fall under FCRA jurisdiction, and not all are compliant. Regulators have made it crystal clear that they want greater accuracy and transparency in data collection and use practices, and they want greater consumer control over their information. And at the end of the day, I think that's a good thing.