

Client Alert

Data, Privacy & Security Practice Group

June 24, 2014

FTC Data Broker Report Recommends New Consumer Protection Legislation

Report Outlines Best Practices for Data Broker Industry

The Federal Trade Commission (FTC) released its report, *Data Brokers: A Call for Transparency and Accountability*, based on an in-depth study of nine data brokers, which the FTC defines as companies that collect consumers' personal information and resell or share that information with others.¹ The report calls for increased regulation and new consumer protection legislation, to address the FTC's concerns about consumer privacy. The FTC also called on the data broker industry to adopt the FTC's best practice recommendations.

In December 2012, the FTC initiated a study of data broker practices and issued Orders, pursuant to section 6(b) of the Federal Trade Commission Act, to nine data brokers seeking information about their data collection and use practices. The nine data brokers that received the Orders are Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future. The *Data Brokers* report summarizes the detailed information provided by the nine data brokers, including the nature and sources of consumer data they collect; how they use, maintain and disseminate data; and the extent to which the data brokers allow consumers to access and correct data about them.

The FTC report criticizes data brokers for a "fundamental lack of transparency."² The FTC also emphasizes consumers' lack of knowledge about the industry's data collection practices and lack of access to the information maintained about them.³ In a press release about the *Data Brokers* report, FTC Chairwoman, Edith Ramirez, commented that "[t]he extent of consumer profiling today means that data brokers often know as much—or even more—about us than our family and friends, including our online and in-store purchases, our political and religious affiliations, our income and socioeconomic status, and more," and noted that the FTC believes "[i]t's time to bring transparency and accountability to bear on this industry on behalf of consumers, many of whom are unaware that data brokers even exist."⁴

The FTC suggests that it may police unfair and deceptive data broker practices under Section 5 of the FTC Act, but it also calls for legislation to

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Elizabeth K. Hinson
+1 404 572 2714
bhinson@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

regulate the data broker industry.⁵ The FTC recommends that new legislation should:

- Create a centralized Internet portal where data brokers can identify themselves, describe their information and collection and use practices, and provide links to access tools and opt outs;⁶
- Require data brokers to increase disclosure of their data collection practices;⁷
- Require consumer-facing sources to obtain affirmative consent prior to collecting sensitive information with the purpose of selling it to a data broker;⁸
- Require consumer-facing websites to notify consumers that they sell data to data brokers;⁹
- Require data brokers to provide consumers with access to information collected about them, including the option to modify or correct that information;¹⁰
- Require data brokers to clearly disclose their sources of information;¹¹
- Require consumer-facing companies that rely upon a data broker's risk mitigation product to identify the data broker upon whose data the company relied if that risk mitigation product adversely impacts a consumer's ability to complete a transaction or obtain a benefit.¹²

The FTC also recommends that the data broker industry adopt certain best practices. First, the FTC suggests that data brokers take steps to comply with the 2012 Consumer Privacy report by adopting privacy by design principles.¹³ Those principles require a data broker to consider privacy issues at every stage of product development, assess collection practices, collect only the data needed, and properly dispose of data as it becomes less useful.¹⁴ Second, the FTC suggests that data brokers "implement better measures to refrain from collecting information from children and teens, particularly in marketing products."¹⁵ Finally, the FTC recommends that data brokers take steps to ensure that a "downstream entity" does not use the consumer information for unlawful purposes, suggesting that data brokers contractually limit the purposes for which clients use their data or audit their clients to ensure proper use of the information.¹⁶

In response to the *Data Brokers* report, companies have announced efforts to increase transparency about data collection practices and improved consumer controls. Earlier this month, Facebook, Inc. announced that it will share users' web browsing data with advertisers to enable targeted advertising, but the company will also allow users to change, add or delete the information that Facebook collects about their "likes" and interests.¹⁷

Some states are not waiting for Congress to act on the FTC's call for legislation. The California State Senate recently approved a bill requiring online data brokers that sell or offer for sale the personal information of any California resident to permit the consumer to "review his or her personal information . . . by means of an electronic search through an online system" and "correct his or her personal information." If signed into law, the California bill would also require those data brokers to "conspicuously post an opt-out notice on its Internet Web site, as specified, that would include specific instructions for permanently removing personal information from the online data broker's database by making a written demand requesting to have the information permanently removed."¹⁸

Clients should regularly revisit data collection and use practices in order to ensure the accuracy of current disclosures. Given the FTC report's focus on the over-collection and over-retention of personal information, entities should revisit their personal information collection policy and consider limiting such collection where there is not a demonstrable business need. Clients that do collect and resell information about consumers should reassess what level of

transparency they offer to consumers and consider whether or not they give consumers the ability to exercise control over the accuracy of the information and how that information is used.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

Celebrating more than 125 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 800 lawyers in 17 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality and dedication to understanding the business and culture of its clients. More information is available at www.kslaw.com.

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered "Attorney Advertising."

¹ FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY (2014), available at <http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

² *Id.* at vii.

³ *Id.* at 46.

⁴ *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information* (May 27, 2014) available at <http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more>.

⁵ See FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY at 49-54.

⁶ *Id.* at 50-51.

⁷ *Id.* at 52, 54.

⁸ *Id.*

⁹ *Id.* at 52.

¹⁰ *Id.* at 51, 54.

¹¹ *Id.* at 51.

¹² *Id.* at 53-54.

¹³ *Id.* at 54-55.

¹⁴ *Id.* at 55.

¹⁵ *Id.* at 55-56.

¹⁶ *Id.* at 56.

¹⁷ *Making Ads Better and Giving People More Control Over the Ads They See* (June 12, 2014), available at <http://newsroom.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/>.

¹⁸ S.B. No. 1348, 2013-2014 Reg. Sess. (Cal. 2014) available at http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1301-1350/sb_1348_bill_20140429_amended_sen_v96.pdf.