BIG DATA

Ben V. Seessel

Shareholder, Carlton Fields

bseessel@carltonfields.com

860.392.5053

Big data is a real buzzword these days. There is even an indie-rock band called "Big Data." As an official from the Federal Trade Commission ("FTC") pointed out in recent remarks, Big Data's hit song is titled "Dangerous."[1] While the FTC, the White House and other federal and state officials and regulators recognize the potential dangers of the use of big data and analytics, they also recognize the potential for it to improve the quality of life for all consumers. This paper, and the accompanying panel discussion, will discuss what is big data, how it is being used in commercial contexts, some practical problems and ethical considerations regarding big data, and introduce what to watch for on the regulatory and litigation front.

I. What is Big Data?

There are many definitions of "big data." For example, "big data" has been defined as:

- "… the massive amounts of data that consumers generate in everyday life through business transactions, e-mail messages, photos, surveillance videos, web traffic, activity logs stored in giant databases, or unstructured text posted on the web, such as blogs and social media." *Big Data: A Big Disappointment for Scoring Consumer Credit Risk*, Nat'l Consumer Law Ctr. (Mar. 2014);
- "[A] collection of data from traditional and digital sources inside and outside your company that represents a source for ongoing discovery and analysis." Lisa A. Arthur, *What is Big Data?* Forbes (Aug. 15 2013), http://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data/(last visited Mar. 1, 2016);
- "Datasets whose size is beyond the ability of the typical database software tools to capture, store, manage, and analyze." James Manyika et al., *Big Data: The Next Frontier for Innovation*, Competition, and Productivity, McKinsey Global Institute (2011).

To get a better grasp on the topic, however, and, in particular, the "big data" that is being collected on consumers in this country, consider the following questions. Do you use Facebook? Twitter? Belong to a shopping rewards club? Use a fitness tracker (e.g., Jawbone, Fitbit)? Subscribe to magazines? Shop online? Use credit cards? This list captures virtually every American consumer.

There is a so-called increasing "volume, velocity, and variety" of data on each of us that is being collected, stored, analyzed, and used. All of these devices that we now use—smartphones and the applications on them, smartwatches, web browsers, email, digital music, digital books, photos, video, telephones, sensors in our homes that control heating and security—leave a digital record that can be stored, analyzed and used. Data is collected on consumers from, among other sources:

- Internet-based transactions, web-page visitation, clickstream analysis, web search queries, email;
- Social networking posts and interactions;
- Fitness bands and smartwatches;
- Smartphones and applications;
- Sensors in homes (the "Internet of Things" ("IoT"));
- Sensors in infrastructure;
- Facial recognition software being used in commercial settings;
- Public records available through federal, state and local government;
- Court records;
- Voter registration information;
- Warranty registrations.

Companies called "data brokers" collect data on consumers from these and other sources, and also share their data with one another. *See Data Brokers, A Call for Transparency and Accountability*, FTC, at iv (May 2014). They combine these data points together to form profiles on consumers that then can be marketed to industry. *Id*.

The FTC reports that:

> ***Data brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction.*** Of the nine data brokers [surveyed], one data broker's database has information on 1.4 billion consumer transactions and

over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases. ***Most importantly, data brokers hold a vast array of information on individual consumers. For example, one of the nine data brokers has 3,000 data segments for nearly every U.S. consumer.***

Id. (emphasis added). In addition to facilitating the collection of data in large quantities from new sources, technology is also enabling companies to mine existing data and to use it in new ways. For example, one Silicon Valley company has developed software that can read virtually any handwritten record. It is partnering with insurance, healthcare, government and non-profit entities to enable them to access, analyze and use data from handwritten records in ways that were previously impossible or impractical.[2]

II. Potential Uses of Big Data

The potential uses of big data are endless, and data analysts and statisticians are working diligently to develop new ways to employ big data analytics. Some ways in which big data is currently being used by commercial enterprise include:

- marketing (understanding customers in order to predict their behavior);
- risk mitigation (detecting fraud, for example);
- optimizing business processes (optimizing operations, distribution, supply chain and delivery);
- optimizing employee performance (monitoring employee performance, and determining optimal methods to improve effectiveness);
- improving healthcare outcomes and predicting disease patterns (for example, big data has been used to predict flu outbreaks before they occur by monitoring web searches, and to predict infections in premature babies before they occur by recording and analyzing every heart beat and breath of the premature babies in a hospital unit);
- optimizing machine and device performance (helping machines and devices become more effective);
- improving security and law enforcement (using big data to detect and prevent terrorist attacks, cyber-attacks and other criminal activity).[3]

Life insurance companies, for example, are using big data to target market to those who can qualify for and afford insurance, to verify information that potential-insureds provide on applications in connection with their underwriting processes, and to retain customers. Insurers are also using big data and analytics to optimize distribution and to improve the efficiency of their operations. Property and casualty insurers are using big data in connection with claims handling and also in setting rates, both of which have garnered the attention of regulators.

III. Practical Problems & Ethical Considerations

There are a number of practical problems and ethical considerations associated with the use of big data and analytics. Many of these have been discussed extensively in publications and speeches by officials in the White House and the FTC, including:

- Privacy;
- Possibly limiting certain goods and services to vulnerable groups—the poor, minorities;
- Data being used to determine things such as eligibility for credit and insurance without complying with the Fair Credit Reporting Act;
- Accuracy;
- Data security.[4]

In addition to these considerations, there is the larger issue of using big data analytics in highly regulated industries like the financial services industry. Perhaps more than any other industry, the financial services industry, and in particular, insurance companies, thrive on data. The financial services industry, however, is also one of the most heavily regulated industries. Making use of big data analytics within the confines of existing regulation in-and-of-itself is a significant "practical problem."

A. Privacy

A primary ethical consideration in connection with the use of big data and analytics is the invasion of personal privacy. As the FTC has pointed out, consumers are often unaware of the types of data that is being collected, stored and used on them.[5] In addition to the issue of awareness, sensitive data that otherwise would be subject to privacy laws is being collected outside of the scope of any regulatory framework. The following are just a few illustrations.

- If a person visits her doctor and provides information on sleep and exercise habits and has her heart rate tested, this data in the doctor's files is protected by the Health Insurance Portability and Accountability Act ("HIPAA"). The same information, however, collected by the provider of a fitness tracker like Fitbit or Jawbone is not.
- Another, perhaps even more stark example, is that a person might unwittingly have his location tracked by his smartphone or an application on it, revealing that he visits a cardiologist's office once a week.
- One study analyzed Facebook "Likes" in combination with limited survey information and concluded that researchers "could accurately predict … sexual orientation 88 percent of the time … ethnic origin 95 percent of the time … whether a user was a Christian or Muslim (82 percent), a Democrat or Republican (85 percent), or used alcohol, drugs, or cigarettes (between 65 percent and 75 percent)."[6]
- A private company has taken roughly 2.2 billion license-plate photos outside of homes, shopping centers and businesses, that it markets to law enforcement and private enterprise.[7]

B. Possibly limiting certain goods and services to underserved populations.

The White House, among others, has voiced significant concern regarding a "specter of 'redlining' in the digital economy – the potential to discriminate against the most vulnerable classes of our society under the guise of neutral algorithms."[8] The White House has stated that "it is easy to imagine that statistical models could be used to hide more explicit forms of discrimination by generating customer segments that are closely correlated with race, gender, ethnicity, or religion."[9]

C. Data being used to determine things such as eligibility for credit and insurance without complying with the Fair Credit Reporting Act.

The Fair Credit Reporting Act ("FCRA") governs the use of "consumer reports" in connection with determining the eligibility for credit, insurance, employment or housing. See 15 U.S.C. § 1681a(d), (f). The FTC's concern is that big data is being sold by data brokers and others to companies who are using the data for FCRA-governed purposes without complying with the FCRA. The FCRA establishes standards regarding, among other things, accuracy, disclosure, and permitting consumers to access and correct information stored on them. Accordingly, the FTC has made it clear that it is "increasingly bringing cases against non-traditional consumer reporting agencies," noting that, "often, data brokers … sell data for FCRA-covered activities without complying … If a company buys this information… and uses it to make decisions about consumers' employment, credit, insurance or housing … the FCRA applies."[10]

D. Accuracy

A further concern is accuracy.[11] Regulators are concerned, for example, that using big data that is inaccurate for fraud detection purposes could incorrectly influence which consumers are offered or have access to certain financial products and services.[12]

Even if the data is accurate, moreover, it can be misinterpreted. A California insurance regulator provided an apt example at a recent meeting of the National Association of Insurance Commissioners ("NAIC"). He described how he buys 48 packages of hot dogs in a summer from his co-op, which records his purchases in connection

with a customer-rewards program. He posed the question whether this purchase would adversely affect his chance to obtain insurance or obtain it at a favorable rate. The hot dogs, however, were for his son's little league team. The regulator's example is based in current reality. As an NAIC consumer advocate reported to our firm, a small insurer filed with the department of insurance in a Midwestern state the 1,000 data points it used in connection with setting auto insurance rates. The data points used in connection with rate-setting included whether or not the insured drank bottled water.

E. Data Security

The White House, among others, has voiced concerns over keeping data safe from hackers or unintended disclosure. State regulators are also concerned over the same issue.[13] The Chair of the NAIC Cybersecurity Task Force announced in January 2016 that, in order to implement cybersecurity regulations, it will begin asking questions on insurers' statutory financial exams in order to gauge what sort of data is being collected and stored on insureds.[14]

IV. What to Watch for from a Regulatory and Litigation Perspective

A. Regulatory

In terms of federal regulation, the FTC has taken the lead in regulating the use of big data. It has brought numerous enforcement actions, and has vowed to continue to do so where appropriate.[15] Its most recent report entitled *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues* (the "Report"), the FTC provided "Questions for Compliance" that would be wise for counsel to any company contemplating the use of consumer big data to consider. *See id*. at 24.

In addition to FCRA, the Report discussed other potentially applicable laws, including equal opportunity laws: the Equal Credit Opportunity Act, Title VII of the Civil Rights Act of 1964, the Americans With Disabilities Act, the Age Discrimination in Employment Act, the Fair Housing Act, the Genetic Information Nondiscrimination Act. *Id*. at 17-18. As the FTC points out, these laws "prohibit discrimination based on protected characteristics such as race, color, sex or gender, relation, age disability status, national origin, marital status, and genetic information." *Id*. at 18. The Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in or affecting commerce, also might apply. *Id*. at 21-23. The FTC has noted the "need to encourage self-regulation because so much is happening so fast and government agencies can't do it themselves."[16]

The Consumer Financial Protection Bureau, though not as active as the FTC, has also made it clear that it is tracking issues relating to big data and consumer protection.[17]

State insurance regulators have also become active. During the NAIC's Summer 2015 meeting of the Life Actuarial Task Force ("LATF"), there was a call from a Society of Actuaries representative for regulators to understand and distinguish mortality components being used in life insurers' accelerated underwriting models. The representative expressed concern that life insurers are getting out in front of regulators' ability to understand how underwriting is being conducted with new algorithms using big data. The suggestion was thus made to revise NAIC Valuation Manual-51 to require mandatory data collection on data being used in connection with accelerated underwriting.

In December 2015, encouraged by NAIC consumer advocates, the NAIC's Market Regulation Committee adopted the following broad charge for 2016:

> Explore insurers' use of big data for claims, marketing, underwriting and pricing. Explore potential opportunities for regulatory use of big data to improve efficiency and effectiveness of market regulation. If appropriate, make recommendations no later than the Fall National Meeting 2016 for 2017 charges for the D Committee to address any recommendations identified by the 2016 exploration.

Notably, by including as part of its charge the exploration of "opportunities for regulatory use of big data," the Market Regulation committee has recognized the potential power of big data to help the NAIC become more effective.

The NAIC Casualty Actuarial Task Force released its white paper on "Price Optimization" in November 2015. Eighteen states have banned the practice, which, although lacking an agreed-upon definition, generally refers to property and casualty insurers' practice of using a customer's propensity to shop elsewhere in connection with setting premiums.[18] This propensity to shop elsewhere is often determined by analyzing a customer's big data profile, including their web-based activity.

NAIC advocates are also scrutinizing property and casualty insurers' use of big data in claims handling, which has also been a topic discussed during recent NAIC meetings.

North Dakota Insurance Commissioner Adam Hamm, Chair of the NAIC Cybersecurity Task Force, stated in January 2016 that regulators will begin asking questions on what sorts of data is being collected on insureds during insurers' statutory financial exams, in order to implement regulations on cybersecurity. This data that regulators collect, ostensibly to assess cybersecurity issues, will of course also give regulators a better view into what types of data insurers are now collecting and using.

B. Litigation

It's unclear what will develop in terms of litigation involving big data. There are several cases to watch or consider, however. The first is *Spokeo, Inc. v. Robins*, 742 F.3d 409 (9th Cir. 2014), cert. granted, 82 U.S.L.W. 3689 (U.S. Apr. 27, 2015) (No. 13-1339) (oral argument held Nov. 2, 2015). In *Spokeo*, Robins alleged that data broker Spokeo posted inaccurate data about him in violation of FCRA, hurting his employment prospects. The Ninth Circuit held that Robins's alleged violations of FCRA statutory rights was sufficient to satisfy Article III standing requirements. The issue before the Supreme Court is whether Congress can confer standing based on a bare violation of FCRA without a showing of concrete harm. At oral argument, the issue of whether posting inaccurate information constituted "harm" was taken up by several Justices. If decided in Robins's favor, there would likely be a proliferation of FCRA lawsuits, particularly against data brokers but also potentially against those who use the data. State attorneys general, led by MA, submitted amicus briefs in support of Robins (MA, CT, DE, DC, HI, IL, ME, MD, MN, MS, NM, NY, OR, WA).

Another case to consider is *Chabner v. United of Omaha Life Ins. Co.*, 225 F.3d 1042, 1052-53 (9th Cir. 2000), in which a plaintiff suffering from a rare debilitating disorder sued his life insurance company for rating him poorly where the insurer had no actuarially valid basis tying his disorder to increased mortality risk. The Ninth Circuit held that California's unfair discrimination law "prohibited United from charging Chabner a nonstandard premium due to his [rare disorder], unless the premium was based on sound actuarial principles or was related to actual and reasonably anticipated experience." The Ninth Circuit affirmed the district court's decision to grant Chabner summary judgment on his UCL and state civil rights act claims. *Chabner* is an important case for insurers to contemplate because big data is transforming the way in which underwriting is conducted, and life insurers should make sure that these changes are based on "sound actuarial principles" and "actual and reasonably anticipated experience."

A third case to consider is *DeHoyos v. Allstate Corp.*, 345 F.3d 290, 300 (5th Cir. 2003), in which plaintiffs alleged that Allstate used a "credit scoring system" to target non-Caucasian customers, and place non-Caucasians into more expensive policies. After the Fifth Circuit held that federal civil rights claims, brought under 42 U.S.C. §§ 1981 and 1982, were not reverse-preempted by McCarran-Ferguson, the parties settled. The *DeHoyos* case cautions insurers to make efforts to ensure that any big data

model they employ does not produce results that discriminate against minorities or other protected groups.

Plaintiffs may also attempt to proceed in suits brought under unfair trade practices or insurance practices laws that incorporate general principles of "unfairness." Point of sale data collection cases, such as those brought under California's Song-Beverly Credit Card Act, also should also be watched.

Endnotes:

1. See Jessica Rich, Director Bureau of Consumer Protection, FTC, *Big Data: Shining a Light into the Black Box*, remarks at Public Citizen, May 11, 2015 at 2.
2. *See* https://captricity.com, last visited Feb. 29, 2016. For example, Captricity reported at a recent Insurance Analytics conference that it has partnered with a major life insurance carrier to read one-million handwritten death certificates from which the company has extracted 10 million new data points that can be used in the insurers' mortality studies among other business applications.
3. *See, e.g.*, Bernard Marr, *The Awesome Ways Big Data Is Used Today to Change Our World*, https://www.linkedin.com/pulse/20131113065157-64875646-the-awesome-ways-big-data-is-used-today-to-change-our-world (last visited Feb. 29, 2016); Bernard Marr, *Big Data: The Mega-Trend That Will Impact All Our Lives*, https://www.linkedin.com/pulse/20130827231108-64875646-big-data-the-mega-trend-that-will-impact-all-our-lives (last visited Feb. 29, 2013).
4. See generally from the White House: *Big Data: Seizing Opportunities, Preserving Values*, Interim Progress Report, Feb. 2015; *Big Data and Differential Pricing*, Feb. 2015; Report to the President: *Big Data and Privacy: A Technological Perspective*, May 2014; *Big Data: Seizing Opportunities*, Preserving Values, May 2014. *See generally* from the FTC: *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, FTC, January, 2016; Jessica Rich, Director Bureau of Consumer Protection, FTC, *Big Data: Shining a Light into the Black Box*, remarks at Public Citizen, May 11, 2015; *Navigating the "Trackless Ocean": Privacy and Fairness in Big Data Research and Decision Making*, Keynote Address at the Columbia University Data Science Institute Symposium on "Data on a Mission: Transforming Privacy, Cities, and Finance," April 1, 2015; Data Brokers, *A Call for Transparency and Accountability*, FTC, May 2014.
5. *See, e.g.*, *Data Brokers, A Call for Transparency and Accountability*, FTC, May 2014. See also Report to the President, *Big Data and Privacy: A Technological Perspective*, President's Council of Advisors on Science and Technology (May 2014) ("As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data.").
6. *See Big Data, A Tool for Inclusion or Exclusion, Understanding the Issues*, FTC Report, Jan. 2016 at 10 (citation omitted).
7. Conor Friedersdorf, *An Unprecedented Threat to Privacy*, The Atlantic.com, Jan. 27 (2016), http://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/ (last visited Mar. 1, 2016).
8. *See Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President (May 2014).
9. *Big Data and Differential Pricing*, Executive Office of the President (Feb. 2015).
10. Jessica Rich, *Big Data: Shining a Light into the Black Box*, Director, Bureau of Consumer Protection, FTC, remarks at Public Citizen (May 11, 2015) at 5, 7.
11. *See, e.g., Big Data, A Big Disappointment for Scoring Consumer Credit Risk*, National Consumer Law Center (March 2014) at 18 (discussing errors in empirical study of five data brokers, including errors in email addresses, physical addresses, relatives, occupations, and income, among others).
12. *See, e.g., Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, FTC, January, 2016 at 30-31.
13. *See, e.g., Big Data: Seizing Opportunities, Preserving Values*, May 2014, at 9 ("[M]ore and more data will be generated about individuals and will persist under the control of others. Ensuring that data is secure is a matter of the utmost importance.").
14. *See* Danni Santana, *N.D. Insurance Commissioner: Mixed Reviews on Insurance Big Data*, Insurance Networking News, Jan. 14, 2016, http://www.insurancenetworking.com/news/security-risk/nd-insurance-commissioner-mixed-reviews-on-insurance-big-data (last visited Mar. 1, 2016).
15. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues*, FTC, January, 2016 at 33.
16. *See, e.g.*, Allison Grande, *FTC, CFPB Setting Sights on 'Big Data' Enforcement*, Law 360, May 11, 2015, http://www.law360.com/articles/654132/ftc-cfpb-setting-sights-on-big-data-enforcement (last visited Mar. 1, 2016).
17. *Id.*
18. The Federal Insurance Office is also engaged with this issue. For example, in its publication, *How to Modernize and Improve the System of Insurance Regulation in the United States*, U.S. Dep't of the Treasury, Dec. 2013 at 56-57, it pledged to "study and report on the manner in which personal information is used for insurance pricing and coverage purposes."

Atlanta
One Atlantic Center
1201 W. Peachtree Street | Suite 3000
Atlanta, Georgia 30309-3455
404.815.3400 | fax 404.815.3415

Hartford
One State Street | Suite 1800
Hartford, Connecticut 06103-3102
860.392.5000 | fax 860.392.5058

Los Angeles
2000 Avenue of the Stars
Suite 530, North Tower
Los Angeles, California 90067-4707
310.843.6300 | fax 310.843.6301

Miami
Miami Tower
100 S.E. Second Street | Suite 4200
Miami, Florida 33131-2113
305.530.0050 | fax 305.530.0055

New York
Chrysler Building
405 Lexington Avenue | 36th Floor
New York, New York 10174-0002
212.785.2577 | fax 212.785.5203

Orlando
450 S. Orange Avenue | Suite 500
Orlando, Florida 32801-3370
407.849.0300 | fax 407.648.9099

Tallahassee
215 S. Monroe Street | Suite 500
Tallahassee, Florida 32301-1866
850.224.1585 | fax 850.222.0398

Carlton Fields practices law in California through Carlton Fields Jorden Burt, LLP.

Tampa
Corporate Center Three at International Plaza
4221 W. Boy Scout Boulevard | Suite 1000
Tampa, Florida 33607-5780
813.223.7000 | fax 813.229.4133

Washington, DC
1025 Thomas Jefferson Street, NW
Suite 400 East
Washington, DC 20007-5208
202.965.8100 | fax 202.965.8104

West Palm Beach
CityPlace Tower
525 Okeechobee Boulevard | Suite 1200
West Palm Beach, Florida 33401-6350
561.659.7070 | fax 561.659.7368

www.carltonfields.com

© 2016 Carlton Fields. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form on our website at www.carltonfields.com. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.