Big Data and Consumer Financial Information

Veronica K. McGregor, Sophia Helena Calderón, Roberta D. Tonelli

About the Authors:

Veronica K. McGregor is of counsel at Jones Day in San Francisco. Sophia Helena Calderón and Roberta D. Tonelli are associates in the same office.

The United States National Security Agency (NSA) has recently been featured in news stories that detail, usually accompanied by a healthy dose of outrage, its data collection efforts. Sources claim that the NSA has been collecting hundreds of millions of records worldwide concerning private financial information, personal e-mail and contact lists, and other electronic data. "Big data," as such data sets are often called, has an increasing presence in the world today. But the news stories raise more questions than they answer. Where does this information come from? Who collects this type of data? Who uses the information? To what ends? Are there laws that limit collection of use of this data? This article attempts to address some of these issues, with a focus on data relating to payment transactions.

What is Big Data?

"Big data" is a broad term that generally refers to the collection of large and complex data sets. Big data is often characterized by three defining characteristics: (1) the high volume of data collected, (2) the rapid velocity of collection and processing rates, and (3) the wide variety of data received and stored. Big data typically describes data sets that are so large that traditional data processing applications are not sufficient to manage and process the information. Instead, companies have developed, and continue to develop, new tools to handle and mine various aspects of the data sets. These tools enable companies to derive useful information from the massive amounts of data.

Big data comes from a variety of sources. The tracking of online

BUSINESS LAW TODAY HOME

DOWNLOAD A PDF OF THIS ARTICLE

DOWNLOAD A PDF OF THIS ISSUE

ABA BUSINESS LAW SECTION

THE LAST LAUGH

shopping and banking give insight to customer preferences and payment information. In-store payment transactions also provide location information. Among other things, social media websites help gauge customer preferences and sentiment. Smartphone applications, online behavioral advertising and tracking, and geolocation services also serve as data sources. Rather than having an intended goal of gathering data, collection sources often create data sets simply as a byproduct of a company's normal course of business.

New big data tools make it possible to aggregate this data from the various sources and to provide a more comprehensive picture of user sets. Often, data collected by a certain source at a specific point in time will have unforeseen uses in the future, especially if combined with data from other sources.

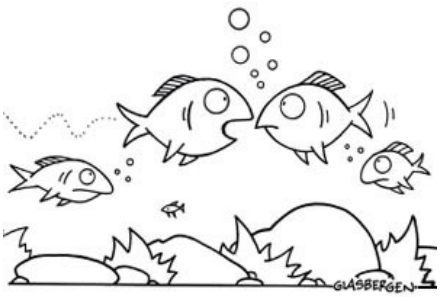
Although the term "big data" can describe a broad array of data collections, this article will primarily focus on a subset of big data – payments data. Payments data tracks purchases by individuals who use non-cash methods of payment, such as credit/debit/prepaid cards or online banking accounts. Payments data can provide information about individual consumers, such as what the individual is buying, how much he or she spends on certain items, where the person is located, and how much available money a particular consumer typically has to spend.

Who is Using It?

Payments data is being utilized by a variety of industries, including card networks, banking, retail, social media, service providers and data brokers, marketing, law enforcement, and intelligence.

The card industry uses payment data to a number of ends, including to cross-sell products, to create card-linked incentive programs, and to detect fraudulent use of credit cards.

Retailers are increasingly relying on big data. Daily deal sites, for example, use digital coupons to collect consumer information and then to analyze consumer supply and demand trends. The companies can track how issuing a promotion affects a business's sales after the promotion has ended – including whether a promotion leads to increased repeat customers and/or a wider customer base. A certain luxury retailer developed both behavioral segmentation and a membership reward program based on information from big data. This has allowed the company to increase purchases of higher-margin products by its more affluent customers. One of the largest online retailers in the world stores information relating to searches, consumer recommendation, and merchandising. It uses information about a consumer's purchases and "views" in order to recommend additional products. As another example, a major kitchenware



"Where is that retirement income stream I keep hearing about?"

SECTION NEWS

New Bi-Monthly BLT Column Introduced: Ethics Corner
Director & Officer Liability Committee Newsletter: November 2013
Free Non-CLE Webinar: "A Leaky Umbrella — Bankruptcy and LLPs Lessons Learned from Big Law Bankruptcies"
40% Off & Free Shipping on 12/2– Cyber Monday Sale
Upcoming CLE: Representing Debtors & Creditors in Individual Chapter 11 Cases
All News

SECTION EVENTS

In The Know: Cognitive Biases, Blind Spots, and Other Impairments of Ethical Vision: How Good Lawyers Can Go Astray
December 17, 2013 at 1:00 p.m. Eastern
Webinar/Teleconference
Free for Section members, 1.5 ethics CLE credits requested

Cyberspace Law Institute & Winter Working Meeting
January 31 - February 1, 2014
Denver, CO

retailer maintains customer databases with information about millions of households. The company tracks the income of a family, the value of its house, and the number of children in a family. This information allows the company to send targeted e-mails and increase the response rate. The company can also distribute different versions of its catalogs based on the preferences of different groups of customers.

As mentioned above, the public sector also collects and utilizes big data. In the United States, the NSA has been in the spotlight for its gathering of big data. News stories have reported that the NSA runs a project named "Follow the Money" that inputs financial data information in a system called "Tracfin." Tracfin contains hundreds of millions of records collected about worldwide transactions, the great majority of which is comprised of credit card transactions.

What is it Used For?

Payments data is currently being used by many different industries toward many different goals, and undoubtedly more uses for this data will continue to emerge. Some applications of payments data include identifying consumers and their spending trends, constructing marketing campaigns, gauging the effectiveness of certain marketing efforts, setting product prices, determining which items to stock and in what quantities, making internal business decisions, preventing fraud, and building new aspects of a business.

Identifying Consumers and Their Spending Trends

Payments data is being used to help companies identify the characteristics of their customers, including their spending trends. This information can be focused on detecting specific patterns in the population at large, or certain large segments of consumers. Big data also enables customer micro-segmentation. Big data technologies allow companies to divide their consumer base into more and more granular segments, enabling marketers to track the behavior of individual customers and utilize this information. One large U.S. retailer has developed a program that can predict a woman is pregnant in the early stages of pregnancy (a so-called "pregnancy prediction score"). By tracking consumers' purchases, and looking for slight changes over time (e.g., – an increased purchase of lotion or certain supplements), the store is able to advertise to and draw in expectant mothers even before the more tell-tale baby purchases occur (e.g., diapers and formulas). One anecdote even touts that the company knew of a woman's pregnancy before her father did, to his dismay.

Thus, payments data can provide a score of information about individual customers, varying from identifying social status to

Four Seasons Hotel

Mergers and Acquisitions Committee Meeting
January 31 - February 1, 2014
Laguna Beach, CA
The Montage

Business Law Section Spring Meeting
April 10 - 12, 2013
Los Angeles, CA
JW Marriott Los Angeles at L.A. Live and the Ritz-Carlton Los Angeles

All Events

COMMITTEE NEWSLETTERS

Cyberspace Law
November 2013

Director and Officer Liability
November 2013

Business and Corporate Litigation
Fall 2013

Business Bankruptcy
October 2013

Legal Opinions
Fall 2013

All Newsletters

OTHER NEWSLETTERS

Miscellaneous IT Related Legal News (MIRLN) 3 - 23 November 2013 (v16.16)

ABOUT BUSINESS LAW TODAY

BLT is a web-based publication drawing upon the best of the Section's resources, including featured articles and other

determining an individual's "pregnancy prediction score." Further, big data technologies allow companies to review this information almost instantaneously, providing the ability to adapt strategies almost in close to real-time.

Constructing Marketing Campaigns

A variety of industries utilize information derived from payments data in order to build marketing campaigns. For example, card transaction data allows banks to more accurately cross-sell its products to specific customers. Credit card companies also use payments data to create card-linked offers. These offers give cardholders savings in return for making specific purchases with a credit card. The payment data lets card companies better tailor the offers to specific customers.

Companies also utilize payments data in order to create loyalty and rewards programs. With this information, the companies can better identify customers' wants and needs, and build programs that incentivize the consumers to spend with their company in order to earn credit toward desired products or services.

One marketing technology company reportedly will begin to roll out a new product that allows marketers to connect a person's "digital persona," despite discrepancies in the name used at various times or locations (whether due to a name change, use of a nickname, etc.). This will enable marketers to pull information from different databases (i.e., online sales databases and social media databases) for a more complete picture of the target consumer.

Assessing the Effectiveness of Marketing Efforts

Using payments data, a company can gauge the effectiveness of specific advertising efforts or incentive offers. Payments data enables companies to track customer purchases back to the originating source, whether it be Google, Yelp, or any of the countless other online advertising sources. This is known as "closing the loop" and allows merchandisers to identify, and perhaps increase the emphasis on, the most profitable sources of marketing.

Price and Assortment Optimization

Payments data enables a company to optimize its merchandise pricing; including decreasing the time it takes to make pricing decisions. Based on the granular data available on sales, retailers can employ the information available to assess past pricing decisions and to adjust future pricing. Retailers can also use big data to determine the inventory for specific stores based on information about local consumer demographics. Moreover, retailers can receive this information and make adjustments to price and inventory assortment almost instantly.

Making Internal Business Decisions

The use of payments data also allows companies to pursue a number of business objectives. A company can better predict trends and detect cost-savings sources. Analysis of such data can lead to greater efficiency and speed in a company's business, as well as provide for improved monitoring of inventory for safety and quality.

Prevention and Detection of Fraud

Payments data may also help financial institutions and card companies to detect and prevent fraudulent card use. By identifying costumer characteristics and spending patterns, a company may be able to determine when certain transactions deviate from established patterns. A company could then investigate the questionable transactions further, and potentially prevent fraud before more damage has been done.

Generate New Business

A company may be able to generate a new business model for itself in the course of its collection of data. For example, a payments provider might create a new business by selling consumer insights based on the data it already generates while processing payments. There is talk of one digital coupon company doing just this. With an influx of competitors, it is possible that the company has maxed out its profits from the deals business, but along the way has gathered an expanse of data. The company has considered shifting its business model to increase the focus on providing consumer information to merchants and marketers.

What are the Relevant Laws?

The regulatory obligations regarding big data have been in effect for almost a decade. They include regulations concerning privacy and security, notice and consent, the collection of data and the targeting of that collection, access, and participation. The regulations come from both federal and state law.

The Federal Trade Commission (FTC) is the primary enforcement agency in the United States for privacy and data security issues. The FTC's enforcement authority in these areas arises under Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices. Pursuant to this authority, the FTC has imposed data security obligations on all industries. The FTC also monitors data breaches and can file suit against a company for a broad range of allegedly unfair or deceptive practices, including privacy policies. The FTC established a division of Privacy and Identity Protection and issued its "Final Privacy Report" in March 2012, which includes guidelines and best practices for business and recommends a baseline federal legislative approach, but which

does not contain legal requirements.

The FTC and several other federal agencies issued a joint Final Rule that imposes additional regulatory requirements on businesses, including employers, that provide consumer information to consumer reporting agencies. The Final Rule both requires businesses to ensure the accuracy of such information, and provides for challenges and dispute resolution.

The FTC enforces privacy policies and initiates enforcement actions against companies that do not abide by privacy and data security promises, or simply fail to implement "reasonable data security measures." An FTC enforcement action may result in a settlement order that includes: statutory penalties to settle allegations of violations and requirements that the company establish, implement, and maintain a comprehensive information security program; obtain, every two years for the next 20 years, an audit from an independent third-party professional to ensure that its security program meets the standards of the order; remain subject to standard record-keeping and reporting provisions to allow the FTC to monitor compliance; and avoid future misrepresentations of the company's security practices.

The Gramm-Leach-Bliley Act (GLBA) is a federal law that requires companies that offer consumers financial products or services such as bank accounts, loans, investment advice, or insurance, to notify consumers of their information-collecting and sharing practices. The GLBA also requires that they explain how the information they collect is used, as well as how it is protected. Several federal regulating agencies, including the FTC, have issued a model privacy notice form.

The Fair Credit Reporting Act (FCPA), also a federal law, regulates the collection, disclosure, and use of information that businesses use to make important decisions about consumers. Such information includes that pertaining to credit, insurance, check writing, insurance, medical records, and tenant history. The FCPA is enforced by the FTC and private parties.

The Payment Card Industry Data Security Standard (PCI DSS), which is a data security standard set by the payment card networks, has also been explicitly incorporated into law in some jurisdictions. For example, Nevada law requires Nevada businesses to comply with the PCI DSS in any transaction where the business accepts a credit card (or other payment card) for the sale of goods or services. The same law also requires Nevada businesses to encrypt any personal information the business transfers outside of its secured systems (e.g., PDA, thumb drive, lap top, e-mail, etc.).

Regulation of big data at the state level stems from multiple sources. Some state regulation is actually enforcement of federal

law. For example, the state attorneys general have authority to enforce several federal statutes. States have also enacted their own laws regulating big data. These laws include unfair and deceptive trade practices acts (sometimes referred to as "baby FTC acts"), as well as state privacy and data security acts. State laws generally prohibit requiring an individual to transmit his or her social security number (SSN) over the Internet unless the connection is secure or the number is encrypted. Similarly, they also generally prohibit requiring the use of a SSN to access a website unless a password or other unique personal identification number is also required.

California has long been on the forefront of privacy and data protection development, often serving as a bellwether on these issues. The recent Do-Not-Track Bill is one of the state's latest steps to strengthen consumer privacy protection. Amending the California Online Privacy Protection Act (CalOPPA), the Do-Not-Track Bill (A.B. 370) was unanimously passed by the California Senate and Assembly in late August of this year. The bill adds new disclosure requirements for operators of commercial websites and online services concerning (1) how they respond to "do not track" mechanisms exercised by consumers, and (2) whether third parties may collect personally identifiable information on their websites when a consumer uses such a website.

Prior to the August amendments, CalOPPA generally required the conspicuous posting of a privacy policy that describes (1) the categories of personally identifiable information that the operator collects about individual consumers who use or visit its website or online service, (2) third parties with whom the operator shares the information, (3) the process by which consumers can review and change the collected personally identifiable information, and (4) the process by which the operator will notify consumers of changes to its website's privacy policy. A party violates the statute only if it fails to post its privacy policy within 30 days after being notified of noncompliance. These requirements remain in place even after the amendments.

In order to heighten consumer awareness of online behavioral tracking, the Do-Not-Track Bill adds the following two disclosure requirements to CalOPPA for operators of commercial websites and online services that collect personal information from consumers who visit their sites:

1. Disclose how the operator responds "to 'do not track' signals or other mechanisms that provide consumers a choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across different Web sites or online services;" and
2. "Disclose whether other parties may collect personally identifiable information about an

individual consumer's online activities when a consumer uses the operator's Web site or service."

Despite its popular name, the CalOPPA amendments do not actually impose a "do not track" (DNT) standard on websites. The bill merely calls for the disclosure of how a website or online service operator will respond to a consumer's DNT request. The Do-Not-Track Bill permits an operator to satisfy this disclosure requirement by posting a hyperlink "to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer [the ability to make a DNT request]."

It is clear that big data, and especially consumer payment data, is a valuable commodity. As more uses for consumer payment and behavior data are developed, we can look forward to more laws to regulate how such data is collected and used.

Additional Resources

For other materials on this topic, please refer to the following.

Business Law Today

Demystifying Big Data
By John Pavolotsky
November 19, 2012

ABA Web Store

Privacy, Security, and Information Management: An Overview

Information security and privacy issues are not new, but mass attention and compliance efforts are at an all-time high, and are increasing as litigation and high-profile security breaches continue to draw attention. Current hot topics in information security and privacy include pretexting; financial privacy; privacy litigation; outsourcing to foreign countries; electronic health and personal records; and social networking. With these issues, a large number of laws have been passed to regulate the information security and privacy issues.

Compliance with these laws is a legal reality as well as a business necessity. *Privacy, Security and Information Management* will help you decipher that laws that regulate these issues and help your clients and business comply with the requirements to avoid security and privacy breaches. Topics covered include internet privacy, financial privacy, unauthorized access to networks and information, wiretapping and privacy in electronic communications, identify theft, spyware and phishing, video and cable privacy, data security and destruction, and much more.