Big Data — A Powerful Asset That Comes with Legal Obligations and Limitations

By: Evan Pilchik and Erik Weinick
Otterbourg P.C.

It is not just household names such as Equifax, Saks Fifth Avenue and Chipolte that must vigilantly guard against improper use of, and access to, electronically stored information. Rather, companies of all sizes and across all industries must understand their obligations regarding the collection, use and transfer of private information. Once they understand these obligations, they must take reasonable steps to ensure that these obligations are fulfilled. In particular, companies must take great care when they collect, access, analyze and utilize, what has come to be known as Big Data.

What is Big Data?

"Big Data" is a broad term used to describe the extremely large data sets which organizations collect, analyze and utilize in the course of their operations. The rise of Big Data in recent years correlates with the increased technical and economic ability of companies to capture, store and analyze the data which companies obtain from sources such as point of sale devices, consumer-facing websites and the so-called "Internet of Things (IoT)". The data can be analyzed to reveal patterns, trends and associations, especially patterns and trends relating to human behavior and interactions, enabling, among other things, more customized consumer targeting.

For instance, in 2012, pharmaceutical company Merck modified its marketing strategy for its allergy medication Claritin based on Big Data. Through partnerships with Wal-Mart, Merck created personalized promotions based on zip code data to market Claritin to geographic areas with high pollen counts, resulting in increased revenue.

A Cautionary Tale

The story of inBloom, a now-shuttered data analytics firm founded in 2011 with $100 million in seed money from the Bill & Melinda Gates Foundation along with the Carnegie Corporation of New York, presents a cautionary tale as to how even the perception about the potential misuse of Big Data can have disastrous consequences.

inBloom aimed to store, clean, and aggregate for states and school districts a wide range of student information. The firm would then make the data available to district-approved third parties to develop tools and dashboards so the data could more easily be used by classroom educators. The inBloom database included more than 400 different data fields about students that school administrators could complete. However, some of the details were so personal – including data fields about family relationships ("foster parent" or "father's significant other") and reasons for enrollment changes ("withdrawn due to illness" or "leaving school as a victim of a serious violent incident") – that parents objected, saying that they did not want that kind of information about their children transferred to a third-party vendor.

Unsurprisingly, inBloom became a lightning rod for those concerned about the increased collection, use and sharing of sensitive student information. The backlash prompted a string of withdrawals by planned educational partners in Colorado, Louisiana and elsewhere. Shortly after the withdrawal of New York State, which, through a budgetary measure, took action by prohibiting the education department from contracting with outside companies to store, organize or aggregate student data, the company ceased operations. Following these concerns about the use of Big Data in connection with students, California passed the Student Online Personal Information Protection Act, prohibiting operators of websites, online services, applications and mobile apps from sharing student data and using that data for targeted advertising on students for a non-educational purpose.

The Legal Framework

Of course, it is not just public perception which governs companies' use of Big Data; there are

a myriad of legal obligations as well. These legal obligations may arise in several manners, including by statute, as a result of membership in a particular industry, or by voluntary contracts.

Statutory Obligations

At the federal level, several statutes impose privacy obligations on organizations throughout almost all sectors of the economy. Well known federal statutes include the Health Insurance Portability and Accountability Act (HIPAA), as modified by the Health Information Technology for Economic and Clinical Health (HITECH) Act (relating to the protection of the privacy and security of certain healthcare information), the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act (setting forth rules with respect to unsolicited commercial email) and the Children's Online Privacy Protection Act (COPPA) (regulating the collection and use of children's information by commercial website operators). Some older laws, such as the Family Educational Rights and Privacy Act of 1974 (FERPA) (providing students with control over disclosure and access to their education records), also have implications for the collection and use of Big Data. Other privacy laws with Big Data implications include the Fair Credit Reporting Act (regulating the consumer reporting industry and providing consumers with privacy rights in consumer reports) and the Genetic Information Nondiscrimination Act of 2008 (creating limits on the use of genetic information in health insurance and employment).

Some of these laws may have consequences beyond the sectors they directly regulate. For example, some aspects of HIPAA may impact employers in any industry to the extent such employers sponsor health benefit plans for their employees and to the extent they have in-house health benefits personnel (such as human resources personnel) that address health benefits issues and have access to personally identifiable information (PII). Such an employer may constitute a covered entity or a business associate of a covered entity under HIPAA if it enters into agreements with, and otherwise monitors and interacts with, health insurers, third-party administrators and other health service vendors, makes eligibility determinations, collects and tallies employee medical receipts under flexible spending plans, assists with case management activities and monitors health benefit usage to identify incentives to control health benefit costs. As can be seen, almost any large organization therefore can be subject to at least some of HIPAA's rules.

States have also enacted privacy laws or taken other actions in direct response to incidents where Big Data was perceived to have been, or was perceived to have the potential to be, improperly used. The Student Online Personal Information Protection Act mentioned above is just one example. In addition, each state has a "mini FTC Act". These are commonly known as Unfair and Deceptive Acts and Practices statutes and are usually enforced by the state attorneys general. Most states also have other specialized statutes protecting privacy in the medical, financial, workplace and other sectors.

Common Law Privacy

Apart from statutes, common law is an additional source of privacy law with which companies must be familiar. Plaintiffs can sue under the privacy torts, which have traditionally been categorized as intrusion upon seclusion, appropriation of name or likeness, publicity given to private life and publicity placing a person in false light. Plaintiffs may also sue under a contract theory in certain cases, such as when a physician, financial institution or other organization holding personal information breaches a promise of confidentiality and causes harm.

Industry Obligations

Self-regulatory regimes play a significant role in governing privacy practices in certain industries. Examples include the Network Advertising Initiative (promulgating a code of conduct for member companies in the online advertising industry), the Data & Marketing Association (formerly the Direct Marketing Association) (publishing guidelines and principles for the marketing industry) and the Children's Advertising Review Unit (promoting responsible advertising to children under the age of 12 in all media). Some trade associations also issue rules or codes of conduct for members. In some settings, such as the Privacy Shield program for companies that transfer personal information from the EU to the United States, government-created rules expect companies to sign up for self-regulatory oversight.

Contractual Obligations

In addition to statutory obligations, an organization can face regulatory liability for failing to comply with its own privacy promises as set forth, for example, in a privacy policy published on its website. The Federal Trade Commission (FTC) and other federal agencies have been very active in enforcing these kinds of promises on behalf of consumers, as a breach of a privacy promise, or even a change to an existing privacy

policy that is not consented to by the consumer, can be deemed to be a deceptive trade practice. Settlement orders between the FTC and Facebook, and the FTC and Gateway Learning, specifically address requiring consent before making changes to existing privacy policies. The FTC even went so far as issuing a warning letter to Facebook in connection with Facebook's acquisition of WhatsApp, reminding Facebook that changing the way WhatsApp collected and used consumer data without consumer consent could violate its settlement order.

On the other hand, companies can also be faulted for failing to require by contract that third-party vendors or contractors protect the security and confidentiality of personal information, or for failing to provide reasonable oversight of such vendors' or contractors' security practices. In the case arising out of the highly publicized data breach affecting more than 36 million users of the Ashley Madison dating website, the FTC claimed that the owner of the website failed to determine whether its third-party service providers had implemented reasonable security measures to protect personal information, and that it failed to contractually require its services providers to implement reasonable security measures. In the settlement order with the FTC, in addition to paying $1.66 million to the FTC, Ashley Madison agreed to establish an information security program which provides for the development and use of reasonable steps to retain service providers capable of appropriately safeguarding the personal information they receive from the company, and to require services providers by contract to implement and maintain appropriate safeguards.

Specific Big Data Privacy Risks

There are numerous pitfalls for unsuspecting companies when it comes to the use of Big Data. A few of these are described in the following paragraphs.

Discrimination

According to the Electronic Privacy Information Center (EPIC), "The use of predictive analytics by the public and private sector … can now be used by the government and companies to make determinations about our ability to fly, to obtain a job, a clearance or a credit card." Essentially, illegal discrimination could become automated by collecting and analyzing Big Data and basing negative decisions upon the result. Banks, for example, are careful not to include questions about race on a credit application. However, by using Big Data to gather and analyze the vast amount of other available data about an applicant (such as residence, education and even name), an applicant's race can be inferred, and a negative credit decision and allegations of illegal discrimination could follow.

Similarly, Big Data can be used to target advertising in discriminatory ways. Facebook, for example, is among the many tech companies that have historically taken a "hands-off" approach to the advertising. Unlike traditional media companies that select the audiences they offer advertisers, Facebook and others generate advertising categories automatically through algorithms running Big Data analytics based on what their users share, both explicitly through account details and implicitly through their online activity. It is easy to see how such targeted advertising could be used to illegally exclude certain groups, such as by steering away certain real estate offerings from certain minority groups.

Anonymity

Some laws, such as HIPAA, carve out a safe harbor for certain "de-identified" or anonymized data. However, the growth and sophistication of Big Data analytics has far outstripped the ability to anonymize data. Latanya Sweeney of Harvard University has shown that almost 90% of all Americans can be uniquely identified using only three pieces of information: ZIP code, birthdate and gender. As a result, even anonymized data still raises privacy concerns about which companies should pay particular attention. For example, Netflix created an enormous database of movie recommendations available for study after scrubbing PII from the database, thereby believing the data to be anonymous. However, researchers were able to re-identify the Netflix users by comparing the Netflix data with movie recommendations found on the Internet Movie Database. Although it appears recent technological advances may lead to better ways to anonymize data, the current state of the art may not be helpful to companies looking at anonymity as a way to avoid privacy obligations.

Data Brokers

Data brokers are commercial organizations that buy or collect data on millions of consumers in order to resell that data for use in targeted marketing and sales efforts. The FTC has been active in pursuing data brokers, charging several of them with having knowingly provided scammers with hundreds of thousands of consumers' sensitive personal information – including Social Security and bank account numbers. In its complaints, the FTC alleged that

the brokers collected hundreds of thousands of loan applications submitted by financially strapped consumers to payday loan sites. The data brokers then sold 95% of these sensitive applications for approximately $0.50 each to non-lenders that did not use the information to assist consumers in obtaining a payday loan or other extension of credit, and had no legitimate need for this financial information. At least one of those marketers even used the information to withdraw millions of dollars from consumers' accounts without their authorization.

Privacy Litigation

A recent case before the United States Supreme Court addressed some of the rights consumers have to sue Big Data organizations for violations of privacy rights.

Under the Fair Credit Reporting Act (FCRA), consumer reporting agencies (CRAs) are required to follow "reasonable procedures to assure the maximum possible accuracy of the information concerning the individual about whom the report relates." The act permits a consumer to bring a cause of action against a CRA who negligently or willfully violates any requirement imposed under the FCRA with respect to that consumer. Spokeo, Inc. operates a "people search engine" that, in response to a user's request (e.g., from a human resource department for candidate screening purposes), gathers information from a variety of databases to provide information about a person. Thomas Robins, who was unemployed, claimed that a Spokeo report about him was inaccurate and, he alleged, this inaccurate information harmed his job prospects (among other things).

Spokeo argued that mere existence of a federal law requiring Spokeo to follow certain procedures did not, in and of itself, provide an adequate basis for Robins to sue Spokeo in federal court. The lower court agreed with Spokeo and dismissed Robins' case.

On appeal, the Supreme Court held that while a mere violation of the FCRA's procedural requirements might not be enough to produce a "concrete" and "particularized" harm which a federal court could redress, the lower courts must apply the facts of the case to determine whether the statutory violation could have produced an "injury in fact". According to the Court, for an injury in fact to be "particularized", it must affect the plaintiff in a personal and individual way, and for an injury to be "concrete", it must actually exist and it must be real and not abstract.

While the Spokeo case continues to wind its way through the federal court system, critics of the decision say that the Supreme Court's decision merely created checkboxes for plaintiffs to tick in order to survive a motion-to-dismiss challenge. This strategy may be used by other consumers hoping to bring lawsuits against any company required by statute to follow privacy procedures, so long as the plaintiff can show that the failure to follow the statute resulted in an injury in fact which is both concrete and particularized.

Complying With Privacy Obligations

Organizations should confer with outside counsel regarding compliance with privacy obligations and the use of Big Data. In addition, companies may wish to appoint a chief privacy officer (CPO). If the organization is not large enough to justify a full-time CPO, then it should empower someone of suitable authority within the organization to fill the role. At a minimum, there should be one leading and authoritative voice within every organization when it comes to privacy (and cybersecurity as well, but that deserves its own article).

A CPO should be cognizant of the types of PII an organization maintains, how it does so, and what its obligations are with respect to the data. A CPO also should be involved in educating other members or employees of an organization as to their privacy responsibilities. Written privacy policies are not just helpful to this process, they are essential.

Further, old IT guidelines for data safekeeping, privacy and security may not be adequate for Big Data compliance efforts, and organizations may be publishing privacy and security statements to stakeholders and customers based on these old guidelines. An up-to-date policy must also address privacy, security and ownership if the organization elects to sell the data.

In the mergers and acquisitions context, acquirers must have policies in place prior to acquiring data assets. One of the first steps that should be taken (if it was not already done during the due diligence process before the acquisition) is to assess what PII exists, what systems are in place to protect and manage it, and whether those systems are legally and technically sufficient.

Of course, some PII, such as that found in marriage records and real estate records, is freely available and therefore is not considered private. Additionally, companies in privacy-sensitive, regulated industries like banking, insurance and healthcare are very aware of

privacy issues, and organizations in these sectors are required to issue privacy policy statements to their customers and tell their customers what information may be shared with other organizations. On the other hand, companies in other industries that are collecting large amounts of non-public data might find themselves in a position to directly monetize their data by selling, for example, consumer data to a vendor looking to improve its product offerings. Before using collected data for such purpose, however, the collector of the data must carefully review its privacy policy and determine whether it is clear to consumers that this would be a permitted use of their data.

Fortunately, a number of privacy-focused associations, as well as industry-specific groups, are available to help organizations using Big Data to meet their privacy obligations. The International Association of Privacy Professionals has a number of resources, and sponsors regular conferences, dealing with compliance issues. Many groups across all industries are active in the legislative process with respect to laws and regulations that affect their particular industries, such as the Better Business Bureau, which offers a sample privacy policy.

Conclusion

The use of Big Data is firmly entrenched in corporate America. Therefore, organizations eager to use Big Data to improve efficiency and profitability must be wary of the pitfalls that accompany its use, be they reputational or legal risks. Only by carefully monitoring their policies, programs and compliance obligations can companies maximize the benefits Big Data offers, without incurring the legal and reputational costs that have been associated with its use to date.

About the Authors:

Both of the authors are certified as Information Privacy Professionals (CIPP-US) by the International Association of Privacy Professionals (IAPP) and co-founders of the Privacy & Cybersecurity practice group at Otterbourg P.C., which counsels firm clients on privacy and cybersecurity matters.

***Evan Pilchik** is also a member of the firm's corporate restructure and finance departments and represents banks and other financial institutions in structuring, negotiating and documenting a diverse array of financing transactions and workouts.*

***Erik Weinick** is also a member of the firm's litigation practice group and regularly represents a diverse group of clients (including many commercial and specialty lenders) before state and federal courts, regulatory authorities, and alternative dispute resolution tribunals.*