The Hidden Dangers of Big Data

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***You know it when you see it.*** Big Data has proved difficult to define. Lawyers should be concerned with its practical rather than theoretical implications.
- ***Mitigate privacy risks.*** Like any other set of records, Big Data should be subject to your standard information security protocols. This includes anonymizing data, providing agreements for informed consent, and proper monitoring and tracking.
- ***Keep it secure.*** The risks of uncontrolled data can outweigh its usefulness. High-profile leaks carry financial costs but also shake the customer's faith.
- ***Keep it human.*** Unchecked algorithms can lead to embarrassment if they are not monitored closely. Potential issues involve inadvertent discrimination, excessive data scraping or the accidental collection of copyrighted material.

Today's legal departments are standing at the cusp of a game-changing shift driven by the ability of their organizations to collect and leverage huge volumes of data. Big Data offers unprecedented opportunities for commerce, innovation and social engineering. But it also presents new challenges for in-house counsel when it comes to privacy, security and a blurring between what is helpful to consumers and customers, and what crosses the line into intrusive or off-putting behavior.

By harnessing huge volumes of information from different sources, businesses can glean fresh insights and new intelligence. Big Data offers the potential to predict events, from curing diseases to anticipating consumer purchases to more accurately figuring out who may commit fraud. This can drive everything from new business models to real social change.

Many of the game-changing possibilities of Big Data can't be realized until organizations and their legal departments figure out what privacy and security mean in today's everchanging environment. However, laws and regulations are trailing far behind technological and strategic innovations, making it difficult to fully leverage the data and expand uses beyond why it was initially collected.

For legal departments, the issues around privacy and security are numerous, vague and sometimes conflicting. There are obvious risks with data breaches and having to grapple with huge stores of potentially responsive information as part of ediscovery. There are few laws that specifically address Big Data as it relates to businesses, consumers and customers in the United States (although that is not the case in many overseas jurisdictions such as the European Union).

In order to avoid the risks and pitfalls while leveraging all the advantages, you need to understand how Big Data intersects with privacy and security to impact the legal department and the business; how to proactively fulfill the potential of this new information; and anticipate where the barriers might lie.

International Privacy Laws: The EU, UK and China

For in-house counsel, navigating data security and privacy laws in one country is painful enough. However, understanding how to navigate these issues in other jurisdictions can be much more complicated. Even if companies don't have international operations or customers, they may store or access Big Data in other jurisdictions.

One of the most significant laws to consider is the European Union's Data Protection Directive, which deals with the collection, processing and movement of personal data. The directive addresses several matters. One includes the Regulation on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Another one you need to be aware of is the Directive on the Protection of Individuals with Regard to Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data. EU member states may also have their own privacy laws.

The United Kingdom also has the Data Protection Act, which dictates how personal information such as health history, religious affiliations and criminal records can be used.

China also has several laws that protect personal data, including the Law on the Protection of Consumer Rights and Interests, which affects companies that provide goods or services to Chinese consumers. Under this law, companies must notify consumers about how they plan to use their personal data and obtain their consent to collect and use it. China also has other data protection and secrecy laws that operate like blocking statutes and forbid transfer of commercial secrets outside the country.

Implications of Big Data

There are many different definitions of Big Data. According to technology research firm Gartner, "Big data is high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making." Along with Gartner's definition of volume, velocity and variety, you should be thinking about a fourth factor — the veracity of Big Data. Simply having a lot of data doesn't make it reliable or useful.

Rather than getting bogged down in definitions, it's much more helpful to think of Big Data in the context of what it enables, not just its attributes. Like "business records," you know Big Data when you see it. For in-house counsel, the practical implications are much more important than the theoretical ones. The outcome of Big Data, or what it produces, should be your concern.

When used properly, Big Data can provide tremendous insights across a huge range of activities, such as human behavioral or buying patterns, disease behavior, human genetic makeup and the like. The key is pulling together disparate data to gain insights, rather than hoarding petabytes and exabytes of information that just sit on servers or in the cloud. For some companies, Big Data can manifest itself through honed information about future purchases. For others, it can be leveraged to develop new healthcare treatments that help to prevent negative drug interaction. Other uses include: making tax preparation predictive; determining where tourists spend their time and money; tracking crime; and honing search engines to provide more benefits to businesses.

Regardless of your industry or strategic uses for Big Data, as in-house counsel your focus should be on proactively enabling the advantages of Big Data to help foresee and minimize risk. The legal department can take the lead in envisioning a new future where Big Data is used appropriately and thoroughly. However, just collecting a bunch of data isn't helpful. In fact, uncontrolled data presents more risks if you don't know what you have, where it exists, how to leverage it or if it can be produced.

Big Data should be subject to all your organization's record management programs and data governance policies. And since much of this data tends to have a relatively short shelf life and becomes obsolete or irrelevant very quickly, your organization's data retention policy needs to address this as well. It's important to know what types of data fall into this category, so you can discard the information when it is no longer useful. For example, when home monitoring systems capture information on temperatures, that data will probably no longer be as useful in 12 or 24 months. Even consumer buying habits that are more than two years old may lose their value and usefulness.

Some categories of Big Data, particularly information that is obtained through third parties, may also have restrictions on how it can be used. When organizations purchase data from other companies, the information may be subject to strict usage agreements. When using this type of information, you must be sure that everyone at your organization understands any license agreements that may restrict how it can be parsed or combined with other information. Failing to do so can lead to broken contracts or mistrust between your organization, business partners, consumers and other shareholders.

In order to leverage Big Data, you need to tame it — to parse the signal from the noise. For companies across industries, the key lies in utilizing technologies to collect the data and aggregate it with other information such as transaction data, Internet browsing habits and other data to create a comprehensive picture of individual people's preferences. This allows companies to take what they know about consumers and prospects in an attempt to better target them with information about goods and services based on their individual preferences.

Information from Big Data is also feeding in to the science of social physics. According to MIT's Media Lab, social physics targets how we create organizations and governments that are cooperative, productive and creative. It states: "These are the questions of social physics, and they are especially important right now, because of global competition, environmental challenges and government failure. The engine that drives social physics is Big Data: the newly ubiquitous digital data that is becoming available about all aspects of human life. By using the data to build a predictive, computational theory of human behavior we can hope to engineer better social systems."

Privacy and Big Data

In the realm of Big Data, you must navigate potential regulatory and privacy landmines. Regulatory expectations are evolving in the United States, but those regulations generally center on how users can control their personal data, along with other issues such as a "bill of rights" for customers, privacy by design and other policies designed to improve transparency and accountability.

Other privacy issues involve the loss of anonymity. With so much data being collected and analyzed, companies may not be able to completely guarantee that they can strip away all identifying features of specific people without a proper framework and rules in place. While there are few laws that specifically regulate Big Data, organizations have to abide by a plethora of other regulations that govern privacy more generally. Federal and state regulations that can impact how Big Data is used include:

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FRCA)
- Genetic Information Nondiscrimination Act (GINA)
- Health Insurance Portability and Accountability Act (HIPAA)

- Electronic Communications Privacy Act
- California Online Privacy Protection Act

In 2014, President Obama called on the administration to conduct a broad 90-day review of Big Data and privacy. The review encompassed how these technologies affect the way Americans live and work, as well as how the private sector, universities and the government are using Big Data.

As part of the review, the administration accepted public comments around Big Data and privacy, including the public's level of concern with different data practices and whether they trust different organizations to keep data safe and handle it responsibly.

According to the White House, respondents felt most strongly about data use and collection practices. More than 80 percent of respondents were very concerned with ensuring that proper transparency and oversight is in place. While most respondents said they did not trust government intelligence and law enforcement agencies at all, they were far less negative toward business. Only 42 percent said they trusted businesses "not at all" when it comes to Big Data.

In order to proactively engage with Big Data and address consumer, government and legal issues, you must lay the framework for determining how you own and can use data. This should include agreements for informed consent, along with the ability to terminate that consent. You also need to figure out a way to track and monitor how the data is being used or may be used in the future. Your organization may also need to compartmentalize information into different databases to ensure Big Data isn't mingled together.

Keeping data secure

When it comes to Big Data, losing control is one of the biggest fears for in-house counsel. The list of companies that have experienced data breaches is large, and growing all the time.

While data breaches are one issue, using Big Data for predictive analytics can lead to embarrassing mistakes or revealing information that consumers would rather keep to themselves. One highly publicized incident featured Target's ability to use analytics to figure out when customers are pregnant. According to media reports, one of those customers was a high-school girl, and her father furiously called his local store to complain about coupons delivered to his house for a crib and baby clothes. The store manager followed up to apologize, only to learn from the father that the daughter was pregnant after all.

Major data breaches over the last few years, from LexisNexis to Anthem

When it comes to Big Data, one of your biggest fears is probably a data breach — and if it isn't, it should be. Here is just a snapshot of the biggest or most significant security breaches, based on information from the Privacy Rights Clearinghouse:

- LexisNexis, March 10, 2005 — 310,000 records affected
- TJX Companies, Jan. 17, 2007 — 100 million records affected
- Heartland Payment Systems, Jan. 20, 2009 — more than 130 million records affected
- Epsilon, April 2, 2011 — 50 million to 250 million records affected
- Target Corp., Dec. 13, 2013 — 40 million records affected
- The Home Depot, Sept. 2, 2014 — 56 million records affected

- Sony Pictures, Nov 24, 2014 — 47,000 records affected
- Anthem, Feb. 5, 2015 — 80 million records affected
- Sheer numbers don't always tell the entire story. While the Sony breach was relatively small, it included extremely sensitive information, including the Social Security numbers of famous actors, entire movie scripts and emails that turned out to not be quite as funny as the authors probably thought they were while writing them.

You should also be concerned about data being misappropriated, particularly if it is collected through online methods. These issues can range from inadvertently misusing copyrighted information to "scraping" data from websites that expressly disallow the practice.

Losing control of Big Data can trigger investigations by regulatory agencies and lawsuits by consumers who have been affected. Within a week of Anthem's massive data breach, the company was facing potential class-action lawsuits accusing the company of failing to properly protect consumer data by not encrypting information.

There are also less obvious risks of Big Data. One risk can include discrimination. While companies may never deliberately discriminate based on race, gender or sexual orientation, analytics could figure out those factors without a human even knowing about it. Based on those analytics, companies may take recommended actions that could lead them into legal trouble.

Practical implications

Now that you know of the risks involved with Big Data, what can you do? Of course, you can ignore it and deal with problems as they arise. This may be the most tempting option, considering how much else you have to do. But the smarter approach is to become proactive and figure out how your organization can take control of Big Data. This will allow you to head problems off before they begin, and it will also position you as a thought leader and problem solver. Among the steps to take:

Know what you have.

In many companies, departments may be collecting and using Big Data without the legal department even knowing about it. The first step should be to reach out to colleagues across the business, IT and marketing departments and other areas to find out what information they have or intend to gather and what they plan to do with it.

Understand the specific risks your company faces

Different industries collect and leverage different types of information. Some of this data may be specifically protected by laws and regulations, such as financial and health information. You need to know how your company may be impacted, so you can plan thoroughly.

Break down silos

When it comes to Big Data, marketing should be talking to IT, the business should be in communication with compliance, and everyone needs to be talking to you. This will not only give you

better insights into potential problem areas, it will allow your colleagues to reduce redundant efforts and could spark new ideas.

Establish policies and procedures

The next step is letting everyone who handles information and analytics know what they need to do, and how they need to do it. Policies and procedures should be regularly reviewed and updated to keep pace with changing technology, regulations, case law and best practices.

Incorporate privacy and security controls

These should be part of all the relevant processes before anyone in the business ever sees the analytics or puts them to use.

Leverage technology

While there are invaluable nuggets of information in Big Data, there's also a whole lot of junk. Without a way to sift, sort and manage these records, they will only accumulate. This drags down servers, costs money and will make conducting discovery of potentially responsive information even more of a headache than it already is.

Communicate, communicate, communicate

As best as possible, inform your customers about the data you collect about them and how you intend to use it. Be sure to gain their consent — and when something changes, communicate again to provide them with updates.

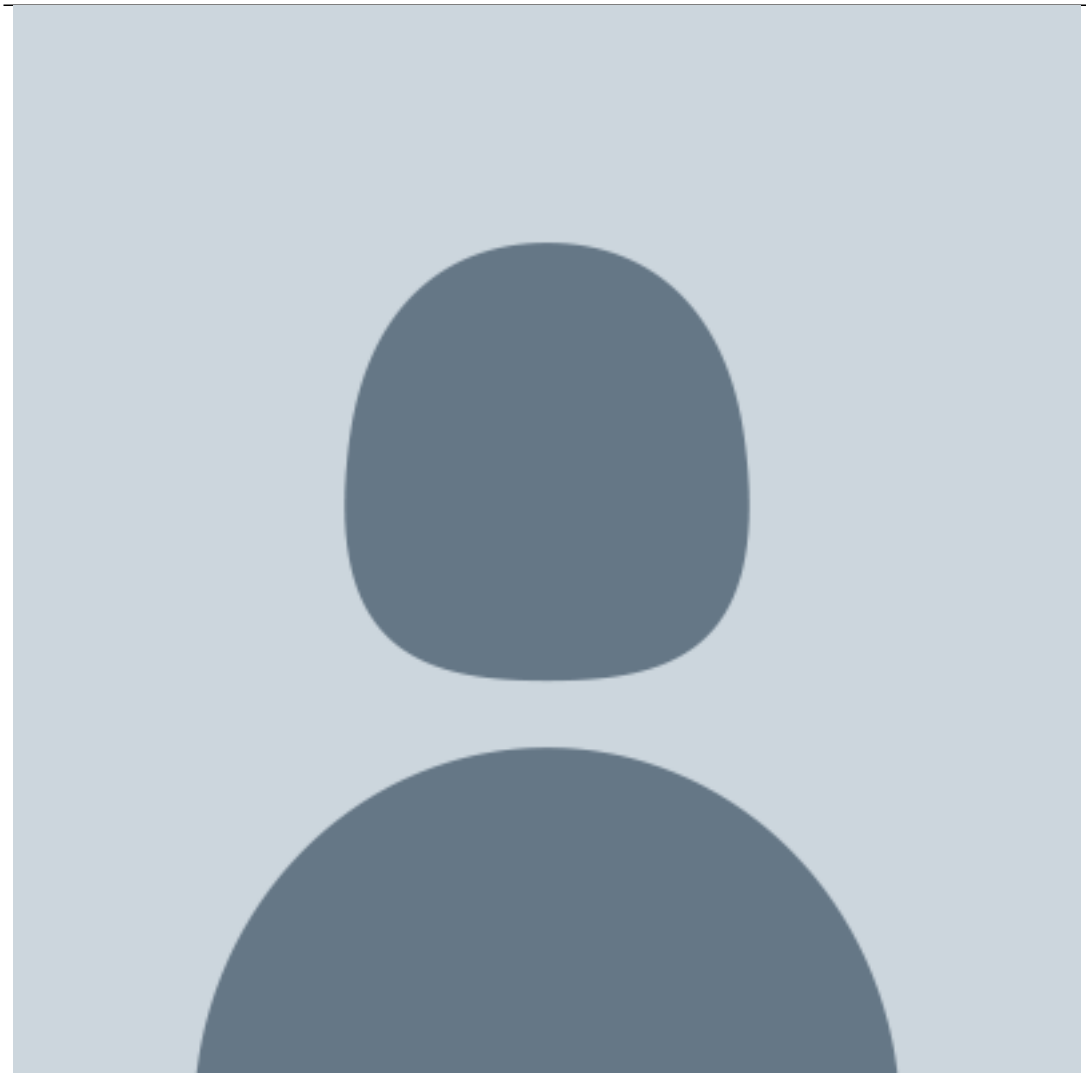
The world of Big Data means that customers and consumers will need to negotiate a new deal with the companies they engage with. In order to gain convenience and improved service, customers need to understand that they will need to exchange their data.

Conclusion

Prediction is one of the hallmarks of Big Data — and the more robust the data set, the more accurate predictions will be. This not only applies to buying habits, but medical treatments, scientific breakthroughs and other areas.

While this is tremendously exciting on many levels, Big Data also presents serious legal, privacy and security concerns. These issues will only grow more complicated. So the sooner you get in front of them, the easier it will be to avoid risk and make use of all this information.

Bennie Smith

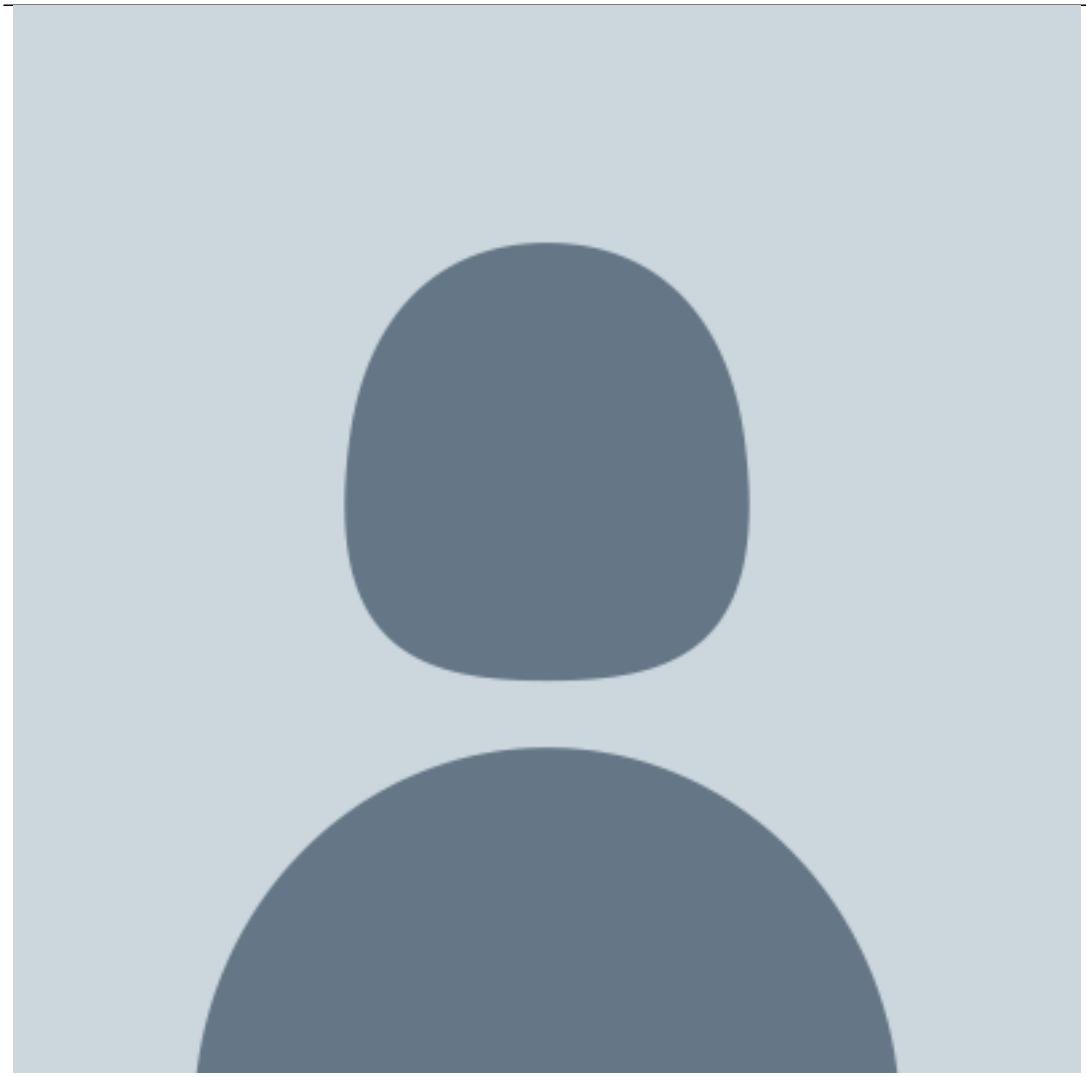


Vice President

Fan Duel

Bennie Smith has spent more than 15 years in the online advertising and advertising technology space. His previous roles have included chief privacy officer, DoubleClick, Inc.; VP platform policy & operations at Right Media Exchange/Yahoo! He is currently leading Fan Duel’s efforts in building and operating a trust-based marketplace as vice president.

Ronké Ekwensi



Managing Director in the Legal Management Consulting Practice

Duff and Phelps

Ronké Ekwensi leads the records and information governance service line. Ekwensi focuses primarily on executing and implementing information governance and records management solutions for clients.