Using data analytics to enhance compliance with corporate social media policy
Using data analytics to enhance compliance with corporate social media policy

by Adam Cohen, Karen Cheek and Ben Hawksworth
Introduction: social media risk and data analytics

Social media, the websites and Internet services that allow users to form networks and share information, views, opinions, photos and other media with each other and the public at large, presents unique challenges and opportunities to business enterprises. Businesses may seek to leverage social media to market services, identify buyers, and present a desirable image of the company to users of these services. Although businesses that choose to participate presumably understand that consumers expect current and accurate information, they may not recognize that it can be difficult to manage the tenor and content of their social media presence, or that the proliferation of online communication presents considerable business and legal risk. For example, the company and its employees may, through official or personal accounts, post or transmit information that is inadvertently damaging to the company’s image and its business relationships, or is contrary to positions it has taken in other public statements or in litigation.

Social media has become pervasive in business litigation, as part of the underlying facts of the case, as a subject of discovery disputes, or as evidence. The cases involving social media have spanned the range of substantive areas of law, including everything from intellectual property, employment discrimination, defamation, personal injury, breach of contract to civil rights and even tax. Parties are arguing over the preservation and discovery of social media, as well as its implications for jurisdiction. Regulatory agencies in a variety of industries have issued special rules and guidelines for business uses of social media. In addition, the National Labor Relations Board has issued a number of advisory opinions and determinations involving employee use of social media and has commented on the enforceability of specific provisions in corporate social media policies.

To manage these business and legal risks, companies are establishing social media policies that govern how companies and their employees may use and interact with social media networks, including internal platforms that the company makes available to employees as well as external platforms such as Facebook, Twitter and LinkedIn. However, without mechanisms to monitor and enforce compliance with such policies, they are nothing but paper tigers. Inconsistent enforcement of written policies can give rise to arguments that they are enforced selectively or in a discriminatory manner, or that they are meant to give the false impression of a robust, good faith effort to promote legal compliance when the only effort is creating a document.

There is no question that appropriate communication of the policy, a training program, and signed employee acknowledgement of policy requirements all play a role in establishing compliance with the policy. However, many businesses have struggled in finding mechanisms to test the effectiveness of the policy and measure employee compliance. Fortunately, technology known as “data analytics” is successfully being applied to social media in a way that can respond to these challenges in implementing social media policies.

In general, data analytics involves the application of specialized software to large volumes of electronic information, such as the data generated through social media. Data analytics enables the search and analysis of the massive and growing amounts of social media content quickly. Many companies are using data analytics to inform marketing and other social media targeted business activity purposes. Yet far fewer are taking advantage of data analytics for risk management purposes, such as identifying specific instances of content generated by employees that may violate corporate social media policy.

Managing risk through social media policy

As a first step in managing the risks involved with social media use by employees and third parties, many companies have established social media policies. These policies may govern corporate social media channels as well as employees’ personal use of social media that could impact the company. Before formulating such a policy, a company must consider its particular social media risk profile. Social media risks may vary depending on overarching factors such as industry, legal and regulatory environment, and company objectives for social media use.

A social media policy should balance the sometimes competing considerations of managing risk and promoting behavior consistent with the company’s social media strategy. Most policies will include language regarding employees’ obligations to protect trade secrets and intellectual property as well as sensitive or non-public information. They also typically advise against the use of slanderous or libelous content or from taking a stand on an issue that is inconsistent with the company’s publicly stated position. Such policy provisions demonstrate to courts and regulators the company’s intent to fashion reasonable guidance and set acceptable limits on matters that may trigger legal liability.

Social media policies may also be used to communicate company imposed access restrictions to social media sites or to more informally discourage the use of social media on company time. However, employers need to be careful about what behavior they target and how broadly proscriptions on certain kinds of communications are articulated. Recent opinions by the National Labor Relations Board indicate that policies should not be expressed in a way that could chill employee speech that is protected under the Fair Labor Standards Act.

1 Adam I. Cohen, Social Media Legal Risk and Corporate Policy (2013).
Data analytics can provide an overview of complex, varied and voluminous social media content, as well as answers to specific questions.

Standards Act. Such speech includes, for example, employee discussion of working conditions.3

No policy, however well-intentioned or clearly expressed, can protect a company unless employees comply with the policy. It is reasonable to expect that the majority of employees will comply with the policy, if they are aware of it and understand its content, but also to recognize that a great deal of damage can be done inadvertently or even deliberately by employees bent on non-compliance. Angry exchanges with dissatisfied customers, posts that unintentionally reveal material non-public information regarding a merger, or a damaging review of a forthcoming company product by an embittered employee can potentially have significant consequences. For this reason, an effective method for monitoring employee social media participation and identifying problematic and non-compliant activities is essential. Data analytics can significantly enhance such compliance monitoring efforts.

How data analytics can help mitigate social media risk

Among other uses, the functionality of data analytics can automate the review of electronic information, summarize large data sets into easily understood visual forms such as charts and graphs, and uncover patterns and themes that may otherwise be overlooked. Data analytics can provide an overview of complex, varied and voluminous social media content, as well as answers to specific questions.

More specifically, data analytics can be used effectively to monitor multiple social media channels for such content as: (1) employee chatter on corporate social media platforms (i.e., networking and collaboration sites designed for the exclusive use of the company’s employees); (2) content associated with corporate accounts on public platforms (such as CNN’s Facebook page); and (3) the vast array of public comments on personal social media accounts. While content that users designate as “private” or limited to certain groups of users (e.g., Facebook “friends”) may not be accessible for analysis, this content is subject to the social media services’ privacy policies, which in a variety of ways provide access to certain data by the services and other third parties. Notwithstanding privacy barriers to accessing certain social media content, the huge amount of public social media content suggests that organizations would benefit by promptly identifying and remediating damaging or non-compliant statements made by their employees, customers, partners, competitors and others.

Applying data analytics to social media policy compliance

Compliance-monitoring analytics can filter social media content to identify posts involving topics of interest or concern, as well as key contributors of such content. These contributors can then be further analyzed. For example, they can be grouped and classified based on their connections to other social media users, demographics, message patterns, personal interests and behavioral patterns. This added insight can help companies understand how to properly address potential problems.

The table on the next page provides examples of compliance-monitoring analytics for social media content.

The presentation of social media data to support the identification of facts, topics, patterns, emotions and so forth is equally important. Data visualization tools can be used to present data and specific analyses in a meaningful way, such as a pie chart showing the distribution of customer sentiment (e.g., happy, confused and angry) surrounding a particular product or service. Many visualization tools are also dynamic in that they allow the analysts and other stakeholders to drill down into the detail depicted in the chart on page 3.

Accessing social media data

There are significant differences between sources of social media data that affect how company implements effective monitoring programs. These differences largely relate to the degree of control that the company has over the systems that store social media content. If the company hosts and manages a system used for social media, the challenges associated with monitoring that system may be different to those related to monitoring public platforms like Facebook or Twitter, particularly if the users are employees with personal accounts, and employ restrictive privacy settings. The technology and processes used for monitoring must, therefore, provide a degree of flexibility suitable to the different social media platforms that are of interest.

In order to monitor compliance through the use of analytics, it is first necessary to extract the relevant corporate or public data from the social media website. Most of such data is accessible through an application programming interface (API). An API is a protocol that allows software programs to retrieve data from the social media service provider in a format that permits additional processing, such as data search and review. Many social media service providers employ proprietary APIs, while others may agree to provide data to intermediary data vendors, who in turn, offer a standard API to software developers and data analysts across a number of different social media platforms. It is important to note that an API may not provide access to all data stored by the service. APIs may limit access to data based on such considerations as privacy policies and data volume. The

Using data analytics to enhance compliance with corporate social media policy

<table>
<thead>
<tr>
<th>Policy violation</th>
<th>Relevant analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal use on company time or equipment.</td>
<td>Timestamp(^4) and geolocation(^5) analysis on social media metadata.(^6)</td>
</tr>
<tr>
<td>Antitrust violations.</td>
<td>Social graph extraction to identify and quantify contact with competitors.</td>
</tr>
<tr>
<td>Violation of trademark, copyright, or fair use.</td>
<td>Repeated text block detection.</td>
</tr>
<tr>
<td>Inappropriate political commentary.</td>
<td>Topic modeling(^7) to isolate relevant topics.</td>
</tr>
<tr>
<td>Promotion of competing products or services.</td>
<td>Topic modeling to isolate relevant topics.</td>
</tr>
<tr>
<td>Discussion of sensitive topics, such as future business performance, strategy, legal or regulatory matters.</td>
<td>Topic modeling to isolate relevant topics.</td>
</tr>
<tr>
<td>Failure to disclose professional affiliation when posting on subjects relevant to company.</td>
<td>Topic modeling to isolate relevant topics.</td>
</tr>
<tr>
<td>Failure to provide disclaimer stating that your views do not necessarily reflect the company's views.</td>
<td>Disclaimer detection.</td>
</tr>
<tr>
<td>Insider trading violations.</td>
<td>Insider trading classifiers.</td>
</tr>
<tr>
<td>Inappropriate, unprofessional or derogatory language.</td>
<td>Derogatory and cursing language classifiers.</td>
</tr>
<tr>
<td>Harassment.</td>
<td>Harassment classifiers (cover sexual orientation, gender, race, national origin, age, general harassment)</td>
</tr>
<tr>
<td>Violation of information protection policies/disclosure of Personally Identifiable Information (PII).</td>
<td>Entity extraction(^8) to automatically identify PII.</td>
</tr>
</tbody>
</table>

\(^4\) A timestamp is a sequence of characters, or encoded information, reflecting the time at which a computer recorded a certain event. [http://en.wikipedia.org/wiki/Timestamp](http://en.wikipedia.org/wiki/Timestamp).

\(^5\) Geolocation data reflects the physical, geographic location of a person or an object. There are a variety of technical means to obtain such data. Social media services may also provide users the option of providing this information. [http://en.wikipedia.org/wiki/Geolocation](http://en.wikipedia.org/wiki/Geolocation).

\(^6\) Metadata is often described as “data about data.” Different types of content on different social media services includes different fields of metadata. [http://en.wikipedia.org/wiki/metadata](http://en.wikipedia.org/wiki/metadata). For example, example of metadata associated with Twitter posts may include, among other metadata: created_at (the timestamp of tweet creation), user_id (the user name of the poster), handle (the user’s screen name) and place (the geolocation from which the user tweeted). See, [http://articles.forensicfocus.com/2012/04/25/key-twitter-and-facebook-metadata-fields-forensic-investigators-need-to-be-aware-of/](http://articles.forensicfocus.com/2012/04/25/key-twitter-and-facebook-metadata-fields-forensic-investigators-need-to-be-aware-of/).

\(^7\) Topic modeling is a technique involving the use statistics to identify topics in content. For example, topic modeling may use the frequency of the appearance of certain words to identify a topic. Topic modeling and other text-based analytics can also derive meaning from varied language sets, including colloquialisms and slang. [http://en.wikipedia.org/wiki/Topic_model](http://en.wikipedia.org/wiki/Topic_model).

\(^8\) Entity extraction involves identifying and classifying text elements into categories such as names of persons, locations, times, quantities, etc.

The dynamic nature of these factors, such as frequent modifications to privacy policies, can also lead to dynamically changing API functionality. Data analysts should be mindful of these changes to understand the limitations on their access to social media data.

Most APIs extract data from social media service providers in a highly structured format. That is, the data will be presented in columns and rows that can be filtered and sorted. It will not, however, be presented in a format that mimics the appearance of the messages on social media websites or in document format. Thus, the extracted data is not readily suitable for review in document management systems or software specifically designed for legal and investigative review purposes. The extracted data will include the social media site content as well as other data attributes, such as a timestamp for each user posted message.

Organizations that host their own social media sites for their employees’ exclusive use will need to assess their technology solution and any related support agreements to determine the feasibility of data extraction and the format in which the data can be presented for additional analysis.

**Limitations on access to social media data**

Strictly private data on social media websites is generally not accessible in the absence of a subpoena, formal discovery request or court order. Such data would consist of content as to which the account holder has specifically...
limited access to a defined, i.e., non-public group. Moreover, several states have passed or proposed legislation prohibiting employers from demanding social media usernames and passwords from employees as a condition of employment. Of course, some may be tempted to gain entry to a user's circle of friends or followers by subterfuge, but such activities would create ethical dilemmas and could potentially have legal consequences. These particular risks may not exist if the company itself hosts the social media service and is clear about its right to monitor the service (though beware of entanglements in privacy law, particularly if nationals of countries with strict privacy laws use the service).

Obtaining social media content by subpoena to social media services

It is abundantly clear from numerous reported judicial opinions that parties to a litigation must preserve and produce relevant social media content. However, while social media services may be required to comply with a subpoena for private data in criminal cases, recent case law suggests that this may not be the case for civil matters. Facebook offers the following information on civil subpoenas:

Federal law prohibits Facebook from disclosing user content (such as messages, timeline posts, photos, etc.) in response to a civil subpoena. Specifically, the Stored Communications Act, 18 U.S.C. § 2701 et seq., prohibits Facebook from disclosing the contents of an account to any non-governmental entity pursuant to a subpoena or court order.

Parties to civil litigation may satisfy discovery requirements relating to their Facebook accounts by producing and authenticating contents of their accounts and by using Facebook’s “Download Your Information” tool, which is accessible through the “Account Settings” drop down menu.

If a user cannot access content because he or she disables or deleted his or her account, Facebook will, to the extent possible, restore access to allow the user to collect and produce the account's content. Facebook preserves user content only in response to a valid law enforcement request.

Outside the context of discovery in litigation, and without voluntary disclosure by a social media user, a company will only be able to obtain publicly available data, which is obtained most effectively by using the service's API, if available. Nevertheless, public data can prove a treasure trove, particularly in terms of monitoring what employees covered by applicable policies are saying publicly. Most Twitter feeds are made public (and even archived by the Library of Congress), and so Twitter data is generally more accessible and potentially more useful for this purpose than, for example, Facebook data, where users limit dissemination to Facebook “friends.”

Storing and searching social media data

Various database and analytical software packages are already commercially available that provide some capability to store and search social media data. These tools may, for example, enable users to search and navigate websites, highlight responsive terms, or “cluster” or group data by topic. Typically these tools can be applied to a variety of file types.

Because social media users often employ colloquialisms and slang to reflect the relative informality of social media interaction, and employees may speak different languages, the monitoring technology should have the ability to work with data in all languages relevant to its employees and customer base. Moreover, the analytic capabilities of the technology must go beyond “key word” searches. Key word searching almost always returns results that are over inclusive in some ways (i.e., providing results that are outside the scope of relevance) and under inclusive in others (i.e., missing relevant results). They may be useful for certain purposes, but typically have critical limitations. For example, key word searching may have difficulty identifying relevant communications that include slang and colloquialisms. This type of language is common in social media posts.

Data analytics technology used for social media analysis should have the ability to perform sentiment analysis and topic clustering. Sentiment analysis helps determine the attitude and emotional state of the writer (or state they wish to convey) in general or with respect to a message topic. In order to evaluate a writer’s sentiment with respect to a topic, data analytics tools identify the key message topics and the words employed in association with the topic. These words are evaluated according to their positive or negative connotation, and the degree to which they relate to the topic, in order to determine the sentiment expressed in a post (such as anger or happiness). Topic clustering uses multi-topic modeling, latent semantic analysis or other such algorithms to extract and group together documents and messages that are related to similar topics, such as a new product that the business plans to release to market.

Presentation of social media data for compliance analysis

The presentation of social media data to support the identification of facts, topics, patterns, emotions and other characteristics is critical. Assessing a confusingly arrayed mass of data is a cumbersome task. Effective visualization

9 Source: “https://www.facebook.com/help/473784375984502/"

10 Latent semantic analysis analyzes relationships in a set of content by examining the words it contains and generating a set of concepts related to the content and terms. It operates on the assumption that words with similar meanings occur in similar pieces of text. http://en.wikipedia.org/wiki/Latent_semantic_analysis.
of the data is essential to rapid analysis, particularly in the context of monitoring, where vast amounts of data may be processed and reviewed daily. Visualization tools can be used to present data in a dynamic form that the analyst, compliance or legal professional can use to view the information in a variety of ways that make trends and patterns easier to observe and identify. Where a detailed review of records is necessary, document review software can be used to present social media text as individual “documents” to facilitate review.

Using the results of a social media policy compliance analysis

By applying data analytics to social media, organizations can take informed steps to address issues of non-compliance with employees, present its perspective and potentially change the direction of conversation, or to learn from feedback and make changes to policies, products, and services. Taking a holistic and proactive approach to compliance monitoring through the integration of data analytics has benefits beyond risk mitigation. For example, such an approach can also generate operational insights that can be leveraged for growth, brand recognition, employee and customer retention and competitive advantage. As a result, there is oftentimes a measurable return on the investment in using data analytics for compliance monitoring.

Conclusion

Social media represents significant global risk for business enterprises. Companies have responded to this risk by establishing social media compliance policies, but establishing policies is only the beginning of an effort to mitigate social media risk. The massive volume of social media data and the rapid proliferation of a wide variety of social media services necessitates the use of advanced technology to identify and aggregate relevant social media content and understand its implications. Data analytics holds great promise in meeting this need. By understanding what data analytics capabilities are available and how they can be used for compliance purposes, companies can begin to transform their risk and compliance programs, including the design, distribution, and interpretation of relevant analytics on a routine basis.
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About EY’s Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the industry sector. With our more than 2,000 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide.

© 2013 Ernst & Young LLP.
All Rights Reserved.
SCORE No. WW0312
1307-1103706 BSC
ED 0114

ey.com