



[print this page](#)

Creating a privacy gameplan for your social media strategy

05.01.2010

By Jay Cline

The rise of social networks as a marketplace is arguably one of the most important economic phenomena of recent years. Companies seeking to exploit these new opportunities will need a privacy gameplan, however, to meet customer and regulator expectations.

Social networks are a huge market. The 400 million users of Facebook alone now comprise the third-largest market in the world, after China and India. Facebook is challenging Google as the top destination on the Web. Online ad revenues--a growing share of which is spent on social networks--now rival print and broadcast ad revenues. As a result, marketing agencies have ramped up their social media expertise, and it is now de rigueur to include a social network component in marketing campaigns.

Where does privacy fit in this new marketing paradigm?

Some would say privacy is passé in the world of social networking, where younger, more cavalier users readily broadcast very private information. But as Facebook found out with its infamous rollout of Beacon--which notified your Facebook friends of things you did on affiliated, non-Facebook Web sites--getting privacy wrong can ground your campaign and dent your brand.

Privacy regulators are also weighing in on privacy in social networks.

Last June, the Article 29 Working Party, the EU body responsible for issuing privacy guidance, released [Opinion 5/2009 on online social networking](#). A month later, the Office of the Privacy Commissioner of Canada (OPC) issued the findings of an investigation of a complaint that Facebook violated that nation's privacy law, and this past February the OPC initiated an investigation into the broader social networking space. In the United States, the Federal Trade Commission is preparing to regulate online-behavioral advertising, a prominent feature on social networks.

Running afoul of privacy regulators' expectations can not only ground a marketing campaign, but also put a company at risk of very public investigations and fines.

What are the components of a privacy gameplan for a social media strategy? A review of the regulators' documents and popular Facebook fan sites provide some reliable starting points.

1. Data Map

Most privacy incidents boil down to whether data practices diverge from regulatory requirements or stated privacy policies. To this end, adopting a social media strategy may introduce new data practices not already disclosed in your organization's privacy policy. To determine if your social media strategy is on solid privacy ground, create a data map detailing the demographics and geographical locations of your target social media users, what data fields you would collect, ideally, from and about them, which social media channels you would use to collect that data, how you would use that data, how you would secure it, and how long you would retain it. A good data map will not only identify the core privacy questions, it should also help the marketing department see in a granular way how to make the most effective use of the available data.

2. Privacy Process Integration

Your organization most likely operates processes for personal data access requests, privacy-choice management, privacy-complaint handling, and personal data deletion. Indeed, the EU and Canadian documents on social network services revealed the importance those jurisdictions place on these user 'rights.' If your organization doesn't have these privacy processes defined, you would be well-served to do so. If they're already defined, your social media strategy will need to integrate with them. For example, if you harvest user data from your social network channels and store that data in a database separate from your other customer systems, you'll want to determine how you'll respond to requests of those users and customers to review copies of their data and to delete their data across both platforms.

3. Site Monitoring and Response Plan

The EU listed among its top concerns with social networks the ability of users to post sensitive data about other people without their consent. Users can also post their own sensitive information, such as dates of birth and account numbers, that could be used for account fraud. The trouble for organizations implementing social media strategies is there is no easy way to prevent these incidents. What are operators of Facebook fan sites doing? Some appear to be manually monitoring their sites for inappropriate posts and complaints and applying a policy for determining which to respond to and how or which to simply delete.

Social media posts can also provide an early warning of customer-service issues. During a review of popular Twitter sites, for example, it became apparent that customers of a financial institution regularly tweet their annoyance at being put on hold by the call center. Privacy professionals tasked with developing the social media privacy gameplan can show additional value by incorporating customer service and antifraud processes.

4. Privacy Policy Update

After you've completed the first three components, you'll be in a position to know if your existing privacy policy needs to be updated. One legitimate option is to create a privacy notice specific to your social media channels. Facebook fan sites, for example, include a default 'Info' tab that is tailorable for this purpose. Canada's report on Facebook showed the high importance the privacy commissioner places on detailed privacy disclosures. Surprisingly, however, in our review of popular fan sites, few posted privacy notices on their fan sites or detailed their social media data practices in their main privacy policies.

5. Regulatory Compliance

EU regulators have determined that operators of commercial social network services are 'data controllers.' This is important because data controllers- compared to data processors- have more compliance responsibilities with regard to EU data-protection regulations. One of those responsibilities, for example, is to register with local data-protection authorities the existence of certain filing systems containing personal data. Depending upon how your social media strategy is implemented, if it involves European users, you may have additional compliance steps to take.

Social media networks have created new marketing opportunities and introduced new complexities into organizations' privacy policies and processes. Marketing departments deploying new media strategies have a new reason to get on the calendar of their privacy office.

Jay Cline, CIPP, is president of Minnesota Privacy Consultants.