

Social Networking Marketing and Privacy Law

WILLIAM B. BAKER

The author explains that, done carefully and properly, an online social network can monetize its user database without running afoul of current U.S. privacy laws.

Hardly a day goes by without the launch of yet another new social networking or other user-generated content website. As these websites sprout like wildflowers, the amount of personal information being collected by social networks soars at an enormous rate. MySpace claims more than 110 million accounts, while Facebook, its fast-growing rival, has some 64 million members. More than 2 billion videos are viewed monthly on YouTube. And at countless other sites users can participate in or share photographs (Flickr), financial advice (The Motley Fool), political blogs (DailyKos), tags (digg), business networking (LinkedIn), and medical information (Inspire).

With this growth come lofty economic valuations, at least for some sites. For example, MySpace was acquired by News Corporation in 2005 for \$580 million, and some analysts estimate the value of that investment has now grown at least fourfold. Google acquired YouTube for \$1.65 bil-

William B. Baker, a partner in the Washington, D.C., office of Wiley Rein LLP, advises a broad range of clients on domestic and international privacy and security law, with particular emphasis on online and wireless issues; postal rate and mailing matters; and communications law. He can be reached at wbaker@wileyrein.com.

lion, and Microsoft ponied up \$240 million for a stake in Facebook. More recently, AOL entered the fray with an \$850 million acquisition of Bebo, a site with a strong presence in the United Kingdom.

ADVERTISING SUPPORTS FREE CONTENT

These massive valuations create pressure to “monetize” the sites’ user communities to justify the investments financially. Until someone invents a new business model, websites can earn revenue from user fees, from e-commerce transactions or from advertising. The prevailing model for social networks is not to charge membership fees. Even the few content sites that have successfully charged a fee, mostly notably the Wall Street Journal Online, have found a need to reevaluate that strategy. Generally speaking, sites have lowered entry barriers in order to increase their audience.

In a world in which access to information content is free, the potential sources of revenue are commerce (eBay and Amazon.com have had success with the retail model) and advertising. Social networks to date, however, have not earned significant revenue from e-commerce.

Thus, advertising has had to serve as the primary revenue source for social networking sites. In 2007, advertisers reportedly spent \$920 million on social networks, and that amount is expected to soar in 2008. A recent op-ed in *Advertising Age* argued that the advertising industry must swiftly develop new models to take advantage of the opportunities offered by social networks. Among the “opportunities” it mentioned is the vast amount of personal information available through such sites.

PROFILING ASSISTS ADVERTISING

If advertisers are seeking greater access to consumer profiles, what a boon social networks can be! There for the world to see are a user’s preferences, education, interests, often information about where they live — all just the type of data marketers covet. Users tend to prefer sites where they can and do post substantial amounts of data and have large networks of friends. Operators of those sites benefit from the users’ deeper commitment toward those sites. And advertisers find a potentially fruitful target audience.

Targeted advertising offers more value because the advertiser can have greater confidence that the ad will be delivered to a user who might be interested in the advertised product. To identify those persons, the advertising distributor (the website or an advertising network that operates on the network) strives to develop a profile of desired (targeted) recipients. When ads are delivered to persons whose profiles match the advertiser's target, the advertiser knows that the ad is going where it is intended.

A social network can compile a user profile in a number of ways. Many websites, and almost all social networks, collect registration information. In some instances, the website may ask the user to provide extensive amounts of data, sometimes far more than is really needed, although often the user has an option not to provide much of this data. Here, of course, the individual directly contributes to the content of the profile.

Many websites track users of their sites via "clickstream" data, tracking users as they view different pages within a site as a normal practice. They may serve ads based either on the context of the particular content displayed on a screen, or perhaps based on a history of the user's visits to that site. Beyond a single site, network advertising services can track users (although they contend not on a personally identifiable basis) across different websites and thereby develop a profile based on the categories of sites visited. Although this practice has occurred for many years, the Federal Trade Commission ("FTC") last fall directed renewed attention to it in its Town Hall on behavioral tracking and its ensuing proposed principles for self-regulation.

Separately, search engines have the capability of developing profiles based on the history of a user's search queries. The accuracy of these profiles may well vary, as there is certainly reason to doubt whether a person's past search history necessarily accurately reflects their current interests. What is clear, however, is that one's search history reflects what he or she was interested in at a given point in time. For this reason, the sale of advertising based on search inquiries has proved highly profitable. To date, however, many networks have yet to capitalize significantly on search of their sites.

In addition, any site that collects and maintains data about an identi-

fied person has the capability to combine that data with information from data brokers to develop even more sophisticated profiles. Although it is not clear how often this, in fact, happens in the United States, privacy advocates fear that it happens all too frequently.

All this provides the advertiser with a better chance of reaching its desired audience. At the same time, much of this profiling activity is invisible to the user, who may be unaware that her page views are recorded and her search requests stored. Some contend that profiling in this manner is invasive of individual privacy and that, if consumers were generally aware of the practice, they would protest it vigorously. A survey conducted in February of this year by TRUSTe and Taylor Nelson Sofres plc (“TNS”) found that while more than 70 percent of online consumers were aware that their browsing may be monitored by third parties for advertising purpose, 57 percent of respondents were not comfortable with advertisers using that browsing history to serve relevant ads, even when that information cannot be tied to their names or any other personal information. Similarly, at the FTC’s Town Hall last autumn on behavioral profiling practices, privacy advocates vigorously challenged profiling as secretive and invasive, and even in some circumstances potentially harmful (for example, one speaker suggested that an insurance company could deny coverage based on incorrect conclusions drawn from a policy applicant’s online search history into infectious diseases).

With registration fees minimal or nonexistent and e-commerce revenues slim, social networks must place their hopes on advertising. Yet the advertising options with the most apparent potential are drawing fire in the public policy arena as advocates press for greater legal protections of the user’s privacy. Navigating between the legitimate interests of both users and commerce poses a substantial challenge to social networks. This challenge is made greater by the manner in which current privacy laws apply to social sites.

WHAT LAW IS THERE?

There is no specific “social network” privacy law in the United States. American privacy law is focused on specific sectors, such as

financial services, and certain groups, such as children. Social networks have not been the subject of legislation as a specific sector, at least not at the federal level. On the other hand, a number of privacy laws, written for different purposes, different industries, and even different technologies, by their terms apply almost incidentally to various aspects of social networking sites and their activities.

This U.S. approach contrasts with the approach taken by some other nations, especially in Europe and Asia, whose privacy laws tend to be more comprehensive. As a result, the basic legal environment in which social networks operate can vary dramatically between the United States and the rest of the world. For example, many foreign laws require individual consent to data collection, uses, and disclosures by websites for which American law does not require consent. Thus, practices that are perfectly lawful in the United States can run afoul of privacy laws abroad, to the dismay of sites that desire to operate in a single, unified manner.

CAN-SPAM ACT

For example, the CAN-SPAM Act was enacted to reduce the number of unsolicited commercial emails. That Act authorizes a civil right of action by providers of Internet access services, which at the time meant services such as America Online and EarthLink. However, MySpace invoked that provision successfully in a lawsuit against theGlobe.com, in which it alleged that the defendant had opened some 95 MySpace accounts fraudulently and used those accounts to send nearly 400,000 unsolicited marketing emails via the MySpace messaging capability to other MySpace “members.” Although that litigation settled, it did produce an unpublished opinion from a federal district court in California upholding MySpace’s ability to sue as a provider of an Internet access service. Under this reasoning, a social network would have legal standing to protect its members from unwanted commercial solicitations via a site’s messaging feature. More recently, MySpace won a default judgment under the CAN-SPAM Act in the amount of \$234 million from two defendants for junk messages sent to its members.

Perhaps the most publicized recent marketing/privacy incident

involved the “Beacon” feature on Facebook, where Facebook allowed certain merchants to post notices in a user’s Facebook “news feeds” when a user had made a purchase. As a result, a user’s friends would be alerted to that user’s latest purchases. This arrangement caused an uproar. Users were surprised by this practice and felt that using their purchases for public advertising constituted a gross violation of their privacy. In response, Facebook changed the system to an opt-in.

Critics were quick to cite privacy law that they contended could apply to Beacon. For example, some suggested that state statutory or common law prohibitions against the appropriation of the name or likeness of a person for commercial benefit could apply. However, these legal theories have not been tested.

VIDEO PRIVACY PROTECTION ACT

As another example arising from the same program, in April a class action lawsuit was filed in Texas against Blockbuster Inc., whose blockbuster.com website had participated as an advertiser in the Beacon program. The lawsuit claims that Blockbuster’s transmission of personally identifiable information to Facebook violated the Video Privacy Protection Act (“VPPA”)¹ because Blockbuster did not have the informed, written consent of the individuals affected. Originally enacted in response to the leaking of Judge Robert Bork’s video rental records during his controversial Supreme Court nomination process, the VPPA’s possible applicability to the Beacon program provides a good illustration of how an older statute can be dusted off and applied, surprisingly, to a very new and different technology.

COPPA’S APPLICATION

One law that does apply directly to networking sites (although the law was enacted in response to chat rooms) is the Children’s Online Privacy Protection Act (“COPPA”) of 1998, which governs the collection by social networks of personal information about children under the age of 13. So if a 12-year-old attempts to register on a site, COPPA — which requires verifiable parental consent as a precondition to the data collection — would

apply. And earlier this year, the social networking site Imbee.com settled FTC charges that it violated COPPA by collecting personal information from children under the age of 13, paying a civil penalty of \$130,000. What's more, the FTC alleged that Imbee.com had advertised itself as "purposely designed to ensure the greatest level of safety...for young members" but in fact failed to live up to that representation.

However, COPPA does not apply to the collection and use of personal information collected from teenagers — perhaps the leading category of users on many social networks. Within the past year, a number of state attorneys general expressed concern that such sites do not do enough to guard against sexual predators. Last October, New York Attorney General Andrew Cuomo announced an agreement with Facebook on new safeguards to protect members, particularly teenagers, from sexual predators, obscene content, and harassment. Even more recently, MySpace announced an agreement with the attorneys general of 49 states on new child protection principles that could enable a safer online experience for kids. One provision in the MySpace settlement provided for the creation of a task force to work on improved authentication techniques, and Facebook has just joined that group as well.

FEDERAL TRADE COMMISSION ACT

General consumer protection laws apply, such as Section 5 of the Federal Trade Commission Act which prohibits unfair and deceptive trade practices. This language provides the FTC flexible authority to protect consumers as services and technologies change. Under its Section 5 authority, for example, the FTC over the past few years has developed a body of law holding websites to the commitments made in their privacy policies and has created standards for data protection. Thus, if a social network promises not to share a user's private data with third parties for marketing, the FTC's action against Gateway Learning Corporation in 2004 stands for the proposition that the network cannot later change that policy and give the change retroactive effect.

Data protection, of course, is a vital component of an online website. This past winter Sears Holdings became the target of a class action law-

suit claiming that the Sears website had compromised the privacy of its customers on its online ManageMyHome.com community site by failing to protect users' identities adequately. Exposing your users' personal data (except, of course, for that which the users want to publicize) is a constant worry.

Finally, the law in this area is likely to evolve rapidly. For example, as this publication has reported previously, the FTC staff in December shed light on its views by proposing a set of principles designed to serve as a basis for self-regulation not only of behavioral tracking, but also of search and network advertising. Approximately 60 comments were filed on those proposals in April, and the Commission is considering how to proceed. Its goal, however, is to establish principles to guide data collection and consumer tracking practices in the online advertising industry. For operators of social networking sites, paying attention to developments in this area is essential.

SO WHAT TO DO?

The pressure to justify a social network's lofty financial valuation by monetizing the user database is strong. Done carefully and properly, it is possible to do without running afoul of current U.S. privacy laws (again, foreign laws often may impose additional burdens). Importantly, however, one is well-advised to monitor legal and regulatory developments closely in this area. Federal action on matters as disparate as behavioral tracking, data protection, and even spyware could easily make major changes to the rules of the road.

NOTES

¹ 18 U.S.C. § 2710(b).