



FEATURES

● PRINT ● EMAIL ● DIGG ● DELICIOUS

Privacy Laws, CRM and Marketing: A Potential Mess

Poorly executed efforts like Beacon may not just be embarrassing — they may also be illegal.
By **Pam Baker** on **April 9, 2008**

The showdown at the Not-So-OK Corral, where **customers booed Facebook** en masse for revealing purchases that individual members made on other Web sites, revealed new liabilities found only at the point where CRM, marketing and **privacy laws** collide.

"This is an example of zealous marketing replacing common sense," said Michael Weathersby, attorney and partner at Evert Weathersby Houff. "I can envision legal action being a logical response to false light defamation and misappropriation of image, in addition to privacy-law suits. I can assure you that a jury of offended citizens will seek to award extreme relief to an injured private citizen."

Sears Brand LLC similarly ran afoul of customer goodwill and privacy laws when the company began collecting information — including sensitive banking and health care data — from customers who signed up for the My SCH Community and downloaded software that was actually provided by comScore Inc., an online data-marketing firm. In tiny and confusing print on the license agreement, the retail giant stated that it would do far more than place a cookie on users' computers and would indeed collect anything and everything (including banking log-on information and passwords) on the user's computer. All the data collected was then placed on CRM files for use by Sears Brand, its affiliates and possibly even third parties beyond comScore.

Law Behind the Curve

The problem is twofold: In both cases an opt-out option was nonexistent or hard to find, and the law is too slow in punishing abuses.

"The legislatures are behind the curve in providing remedies that would amount to a commercial prohibition against these abuses," said Weathersby.

"In most jurisdictions, damage awards are quite modest today. Proof of actual damages — opposed to damages to feelings (noneconomic losses) — can be very difficult," he said.

Because of a lack of self-restraint and a hobbled U.S. legal response, corporations will continue to up the ante on data collection for their CRM systems to either use in their own marketing efforts or to sell to third parties for additional revenue. Sadly, even if laws do catch up, the damage cannot be undone, as the information will likely forever be available on the Internet or otherwise too widely disseminated to retract.

In the end, it may be **foreign countries** that safeguard U.S. citizens' private information in a roundabout way. After all, most corporations with enough CRM power to collect such massive amounts of data are likely to be international in scope.

"First, it depends on what data we're talking about. Second, it depends on what country you are talking about. For

example, the EU has much stronger laws on privacy than does the U.S.," said Lonny Nathanson, partner at Levitate IT.

Rules Change at the Border

Staying in compliance with a multitude of privacy laws in many different countries is tricky business for even the best and most honorable CRM programs. When companies like Facebook push the edge of the envelope, they're likely to come back bleeding.

"Laws in the EU, Canada and other privacy-sensitive countries forbid the transfer of personally identifiable information outside of the country. This includes both customer and employee information," said Jennifer Albornoz Mulligan, an analyst at Forrester. "Information that is even viewed on a screen in a different country is considered to have been transferred, even if the database isn't stored in that country."

The resulting penalties against U.S. companies that collect and share such data can be severe, resulting in fines large enough to close some businesses down. Some countries even give jail time to company executives for such offenses.

The problems with mismatched privacy laws and enterprise practices can even lead to foreign companies shunning U.S. companies — as vendors or partners — completely.

"A practical implication of the Patriot Act may be that individuals will choose to deal with businesses that do not share their information with U.S.-linked affiliates or service providers," wrote attorneys Wendy Gross and Michelle Kisluk in an article titled "**Canada's Privacy Laws Vs. the USA Patriot Act**" at FindLaw. "With heightened media attention given to the reach of the Patriot Act, and therefore increasing awareness of the act, as well as its inherently political nature, clients may be scared off by the hype — even if in practice the result is not that different than before the Patriot Act."

Stay Inside the Lines?

The article goes on to explain that Canadian companies could find themselves in compliance with U.S. laws but at fault by Canadian privacy laws and vice versa — hence the veiled recommendation of avoiding working with U.S. companies at all.

In a day and age when even U.S. government agencies are turning to CRM, and privacy laws worldwide are growing more teeth by the moment, perhaps it's time to rethink corporate marketing policies with an eye to the long term and a well-turned ear toward customer concerns.