

# Zoomerang vs. SurveyMonkey: Who has the better privacy?

Our privacy columnist takes a close look at the privacy policies of two leading online-survey vendors

Jay Cline

September 7, 2010 ([Computerworld](#))

Every time I send out a survey using my Zoomerang or SurveyMonkey accounts, there is always at least one wise guy among the respondents who dings me for risking their privacy with these tools. But do they have a point? Last week I decided to finally find out.

Let's call it a privacy-impact assessment (PIA) for online-survey services.

A PIA tries to answer two main questions: Will a system, process or product create risk to personal privacy? And, if so, what can be done to mitigate that risk? When I think about using these tools myself, three more questions come top of mind:

- Will the online-survey company in any way access or use my survey responses or contact lists?
- How will the company secure my survey responses?
- Does the company offer tutorials to users like me on how to conduct a survey that protects privacy?

So those are the criteria I took with me when I visited the Web sites and called the two leading online-survey products, [Zoomerang](#) and [SurveyMonkey](#). What did I find out?

## 1. Similar business models

First, this is another case of a lot of personal data being stored in the northwestern United States. [MarketTools](#) parent company of Zoomerang, is based in downtown San Francisco, while SurveyMonkey maintains headquarters in Menlo Park, Calif., with data operations in Portland, Ore.

Both are survivors of the dot-com bust. Walter Good and three other market-research professionals co-founded MarketTools in 1998 in the San Francisco Bay area. I spoke with Good, who pinpointed the birth of Zoomerang to a Minneapolis meeting his team had with the CIO of General Mills. Their idea was to use the Internet to revolutionize consumer research and bring it to the masses. The CIO loved the concept, and soon General Mills and Procter & Gamble were investors.

Now employing 550 people, MarketTools provides other market-research software products in addition to Zoomerang. Housed in an upscale, downtown San Francisco office building where [Google](#) takes up three floors, MarketTools also maintains concentrations of employees in Minneapolis, Chicago, New York and its European headquarters in London. The company's current leaders joined the firm in 2005 and 2006, and the company's Web site reports that strong growth occurred in 2009. Zoomerang's business model is to attract users to its free service and then entice them to upgrade to packages that run as high as \$600 per year.

For its part, SurveyMonkey followed a similar trajectory. Ryan Finley launched the company in Madison, Wis., after he left college in 1999. After moving to Portland, Finley hired his brother Chris in 2002 and eventually saw revenue hit a reported \$30 million in 2008. A venture-capital fund bought SurveyMonkey in 2009, installed its current management team and moved its headquarters to the Bay area. A former [Yahoo](#) executive now runs the company, which employs 31. The company's business model is also to attract users to its free service and then upsell them to a premium service, which in SurveyMonkey's case costs \$240 per year.

## **2. Privacy programs**

Do the leading online-survey companies maintain privacy programs? It's hard to tell by external appearances. The companies aren't visible in the privacy community, and their Web sites don't indicate that they have someone in charge of privacy. I did find out by contacting the companies that Stuart Loh, corporate counsel for SurveyMonkey, is responsible for

privacy, and Chris Robertson, security manager at MarketTools, handles privacy for Zoomerang.

On the plus side, both companies joined the privacy-seal program of San Francisco-based [Truste](#) and are also self-certified to the [U.S.-EU Safe Harbor](#). Neither has suffered a publicized privacy breach that I could find, in spite of all of the sensitive corporate data they must host.

SurveyMonkey has also recently upgraded its privacy policy. I contacted Anne Raimondi, vice president of marketing, who described the update process. "We took into account customers' concerns and inquiries that we gathered over time, to ensure that our revised version addressed as much of our customers' feedback as possible."

"The revision was discussed and reworked internally by staff across the business," she added, "as well as by external lawyers from DLP Piper and a highly reputable independent privacy consultant, David Flaherty." Flaherty was the first privacy commissioner of British Columbia.

### **3. Use of survey data**

If you answer a survey hosted by Zoomerang or SurveyMonkey, is it safe to assume that no one except the survey sponsor will access or use that data, and that when the sponsor deletes the data, it's gone? Their privacy policies tell markedly different stories, with SurveyMonkey's offering more details.

I combed through Zoomerang's privacy policy, and I couldn't find any clear statement along the lines of "We will not access or use the content of survey-taker responses for any statistical or other purpose." In fact, most of the privacy policy seemed to be focused on account holders, not survey takers. I didn't see anything in the policy that would prevent Zoomerang from mining surveys for keywords, accessing results and individual responses of surveys that interested it, and using those results for its internal purposes.

The Zoomerang terms and conditions did, however, address this topic. It states:

"We agree not to use any of your Confidential Information (defined below) for any purpose except to operate the Site and Services in accordance with this Agreement. We agree not to disclose any of your Confidential Information to any third party other than to our employees and consultants who are bound by confidentiality obligations and are required to have access to the Confidential Information in order to operate the Site and Services."

In a phone interview, Robertson and the MarketTools heads of marketing and product development told me that it was against company policy for MarketTools staff to access client information without client consent or a court order.

So, Zoomerang is doing the right thing, but the privacy policy doesn't get you to that conclusion.

On this point, the SurveyMonkey commitment is easier to find. Its privacy policy states:

"We will never use your survey questions or responses other than in accordance with this privacy policy unless we have your consent, and then only anonymously and by aggregating them with questions and responses from other surveys. You may be asked whether you wish to opt in to allowing us to use your survey questions and/or responses in this way at the time of creating your account or your survey. If you opt in, we may use the anonymized and aggregated survey questions and/or responses to create data services or content."

The phrase "other than in accordance with this privacy policy" could be used as a Trojan horse to allow all kinds of uses. But I read the policy top to bottom, and didn't see a way SurveyMonkey could mine and use survey content. When I signed up for an account, SurveyMonkey didn't ask me to opt in to allow it to use my survey content as it had reserved the right to do in its policy.

One advantage SurveyMonkey has over Zoomerang in the data-use category is its prominent way to opt out of all SurveyMonkey surveys. If you find that you're getting too many SurveyMonkey surveys from your friends and colleagues, you can go to [surveymonkey.com](https://surveymonkey.com), click on the "E-Mail Opt Out" link on the home page footer, and then enter your e-mail address.

Neither privacy policy gave details, however, about how long your survey content might reside on the companies' servers and backup media after you delete them from your account. SurveyMonkey explained to me that in practice, they overwrite deleted data every 30 days. To the other extreme, SurveyMonkey's terms and conditions when I signed up included an ominous warning that it could purge my surveys at any time.

#### **4. Disclosure of survey data**

One way the online-survey companies could monetize the vast stores of data they're hosting is to mine it, package it and sell it. Do their privacy policies prevent this scenario?

For its part, Zoomerang's policy includes this ambiguous statement: "We may share your information with affiliated companies for reward redemption and/or other market research opportunities."

What information might be shared, and who are these affiliated companies? The privacy policy doesn't tell you.

The MarketTools team explained to me that in practice this statement only applies to people who voluntarily sign up to earn and redeem loyalty points for participating in panel surveys. To redeem their points, MarketTools shares their information with a third party.

The only scenario in which MarketTools shares the personal information of survey account holders with third parties is when the account holders purchase a premium service. In these cases, Cybersource processes the payment, allowing MarketTools to not retain any credit-card information.

On this topic, SurveyMonkey's privacy policy is clearer. It states: "SurveyMonkey does not ever disclose your survey questions or responses

unless you permit or request for us to do so. SurveyMonkey may disclose survey questions and responses anonymously and by aggregating them with other users' survey questions and responses on an opt-in basis."

It's not clear how the "anonymous" disclosure of survey content would work and how the opt-in process would work, but it's a step in the right direction.

## **5. Security of survey data**

Most large corporations now have vendor-compliance programs in place. If the corporations host any kind of confidential or privacy-restricted information with third parties, they require those third parties to make contractual commitments to protect that information, and demonstrate proof of their internal security controls.

Both MarketTools and SurveyMonkey report that they have in place the physical- and network-level security you'd want to see. But the Zoomerang privacy policy doesn't offer the kind of proof vendor-assurance professionals look for. The one paragraph dedicated to security starts off: "Transmissions over the Internet are never 100% secure or error-free. We do, however, take reasonable steps to protect your personal information from loss, misuse, and unauthorized access, disclosure, alteration and destruction."

My phone interview with the MarketTools team clarified this point as well. They provided me a list of security and compliance measures in place, including a SAS 70 Type II certified data center with biometric access controls, multiple layers of firewalls and intrusion-prevention sensors, quarterly third-party security audits of externally available systems and Web sites, annual third-party onsite audits, and HIPAA, PIPEDA, and U.S.-EU Safe Harbor compliance assessments. Zoomerang also passed a privacy and security audit to be listed on the [Salesforce.com AppXchange](https://salesforce.com/appexchange) for cloud-computing products.

In this area, SurveyMonkey does a better job telling its story on its Web site. The company dedicates a separate page for a [Security Statement](#). But it shares the most details in a Help section [response](#) to a question about

security. That response indicates that surveys are stored in a SAS 70 Type II certified Sungard data center protected with biometric access controls, among other things, a firewall that restricts access to all ports except 80 and 443, QualysGuard network scans run weekly and McAfee HackerSafe scans run daily, and data backups run hourly.

The only company I've seen do better than what SurveyMonkey promises in its security statement is San Francisco-based Salesforce.com, which dedicates a Web site -- [www.trust.salesforce.com](http://www.trust.salesforce.com) -- to its corporate privacy and security commitments.

## **6. User training on privacy**

Before Zoomerang and SurveyMonkey came along, market-research professionals and statisticians conducted most consumer surveys. Now, anyone with a Web [browser](#) and contact list can launch a survey, ask any question under the sun and share that data with anyone. In that sense, Zoomerang and SurveyMonkey can't control how account-holders use their platforms.

But they can make privacy training available on their sites, and even require users to complete some basic level of training when they open or upgrade accounts. [Facebook](#) and MySpace have taken these kinds of measures, for example. SurveyMonkey does make available a "Best Practices for Survey Design" guide, but the only privacy topic it addresses is spam. Zoomerang also offers tutorials for constructing effective surveys, but doesn't address the topic of how to respect privacy when you're creating a survey.

So who does better on privacy? I have to admit I started the analysis biased against SurveyMonkey just because of its name. I don't want anyone monkeying around with my data. But on every topic I looked at, they both offered about the same level of protection in practice. SurveyMonkey gets the nod, though, for codifying these practices into clear online disclosures and commitments.

Are the wise guys who ding me for using these tools right, after all? There are many things to ding me on, but this doesn't turn out to be one of them. On security, both companies are taking measures I see Fortune 500 firms taking. On privacy, they need to do a better job clarifying in writing what their good practices are. But the internal practices they represented to me are what I'd look for to pass a privacy audit.

If you want to further reduce your organization's risk when using these tools, take three steps:

- Don't load survey-taker e-mail addresses into the tools. Just e-mail survey links to your survey takers through your own e-mail account.
- Avoid asking for sensitive intellectual property on surveys.
- Don't ask for sensitive personal data through these tools.

Zoomerang and SurveyMonkey are revolutionary American inventions. Their growth into new geographies and lines of business, such as health care, may depend on continued improvements to their privacy and security and how they tell their stories in these areas.

**Jay Cline** is president of [Minnesota Privacy Consultants](#). You can reach him at [cwprivacy@computerworld.com](mailto:cwprivacy@computerworld.com).