

# Surprise: You're in the privacy headlines

Jay Cline

October 4, 2002 ([Computerworld](#))

Your CEO is on the phone for you, the CIO: "I want a report in 30 minutes on why we're in *Computerworld* and what you're going to do about it." The story says thousands of your customer profiles have been posted to the Web through a business partner. So what are you going to do? The first people you turn to, and the first steps you take, could make the difference between a forgotten news item and a multiyear public relations fiasco.

**Minute No. 1:** Ask the CEO for a few more hours. You need time to get the facts straight.

**Minute No. 5:** Form your response team. You'll need the company's general counsel to get the Web site shut down and identify your legal options. You'll also need the head of PR and a human resources representative to make sure your employee investigations are legit. Your chief technology officer will hunt down the forensic facts. Finally, you'll need a vice president from the business unit where the customer profiles originated.

Oh, and has your administrative assistant cleared your calendar?

**Minute No. 30:** Hold a teleconference with your team. The brand is at stake, and privacy watchdogs in New York and Washington are already taking aim at your deep pockets. Don't start creating e-mails that could be taken out of context. Your goal with the teleconference is to form a hypothesis about what has occurred and what your options are -- and to assign tasks. You'll speak together every half-hour to modify the hypothesis as new facts come in.

**Hour No. 2:** Meet with your team. You'll write the press release together on a whiteboard. You've already asked PR to arrive with two alternate drafts, and you've asked the legal representative to arrive with a decision tree that maps out where each route could take you. Did you think not talking to the press was an option? Sorry; welcome to the Information Age.

**Hour No. 3:** Meet with the CEO. If she's out of town, consider flying to her. Yes, it's that important. Millions could be at stake -- ask Eli Lilly, US Bank or DoubleClick. Your CEO will want to look into your eyes to see how confident you are about the strategy you've chosen.

The strategy should hinge on whether you've committed one of the three deadly sins of data privacy: lax security, rogue data collection or inappropriate data sharing. In the past three years, roughly 90% of the privacy-related headlines and lawsuits I've tracked around the world have fallen into one of these categories.

If your situation resulted from lax security, your best course is to fix the problem, put best practices in place to make sure it doesn't happen again, compensate affected consumers and issue a mea culpa. The story will die. But if you've collected personal information without full disclosure -- or if you've shared personal information with other companies for marketing purposes, without consent -- you have more than a technical glitch on your hands. You have a business strategy that may fall afoul of the law and your customers' expectations for social responsibility. Your own conscience should be speaking up.

Be prepared to abruptly terminate these business relationships and others like it, transform your business strategy and take your lumps in court. Denying or resisting at this point would add fuel to the PR fire. Releasing a public apology and admission of guilt, while legally risky, could save your brand by taking the edge off the story.

The best way to avoid all this in the first place is to implement a privacy checkpoint for all new projects and deals. Mom was right: An ounce of prevention is easier than a pound of cure. But the cure for those who don't get it won't be so kind.

*Cline manages data privacy at [Carlson Companies Inc.](#), a Minneapolis-based group of businesses in the travel, hospitality and marketing industries. Contact him at [privacy@computerworld.com](mailto:privacy@computerworld.com).*