Chapell & Associates, 236 West 10th Street, New York NY 10014 212 675 1270

Chapell & Associates

Why did DidTheyReadIt Become so Controversial?

Originally published in the DMNEWS on August 9, 2004

I was at a privacy conference down in DC a couple of weeks ago. I like to go to the big privacy conferences just as much as I like to attend the big direct and interactive marketing events, as the business of Privacy-Marketing incorporates ideas from within each industry. (Just as an aside, I'd strongly recommend to people programming direct marketing conferences to continue to include segments with members of the privacy community – each group could stand to learn a great deal from the other.)

Anyway, at the conference, someone expressed concern about a new software product called DidTheyReadIt, which allows people to track the emails they send, and lets them know when a recipient opened their message. A lively discussion ensued, where terms such as 'web beacons', 'cookies', and 'IP addresses' were tossed around. I was surprised that the subject had received this much attention – and equally surprised that so many privacy experts didn't really understand how these products work. More than one conference attendee suggested that email monitoring should be banned altogether. In response, attendee Dave Fowler from email-marketing service provider (ESP) @Once stood up and announced that most, if not all, of the ESP's track open rates on behalf of their customers. He added that most ESP's ability to deliver personalized, relevant content to subscribers would be limited if they could not monitor open and click behavior.

As many of you know, tracking opens and clicks has gone on for as long as the email marketing industry has been in existence. Frankly, I was under the impression that this was a widely known and generally accepted industry practice. Which begs the question – why is DidTheyReadIt garnering all this negative attention?

The Company

I had the pleasure of speaking with Alastair Rampell, the founder of Rampell Software, and developer of DidTheyReadIt. Mr. Rampell's original conception was for DidTheyReadIt to be a tool to combat deliverability issues – a certified email of sorts. The premise is that an online retailer such as Brooks Brothers could already tell whether a customer has opened one of their emails, while a single person had no way of knowing if their email had been opened. For example, if I'm applying for a job, I want to know that the company has received the resume I emailed to them. Clearly, the product was not intended to be creepy. So why did it turn out that way?

Seems like at least some of the trouble began as a result of the initial PR campaign for DidTheyReadIt. The company emailed a press release to several journalists requesting that they conduct an interview with Mr. Rampell. That email was followed up by a

second email providing details of when the journalists opened the first email. The PR campaign was conceived as a neat way to show the press how the product worked.

Although many journalists responded favorably to DidTheyReadIt's PR email, some of them were less than enthusiastic. Walt Mossberg, the tech reporter for the Wall Street Journal, sent back an email saying that the product should be illegal. I certainly wouldn't agree with Mr. Mossberg on that, but it illustrates some of the challenges of introducing a new technology product into the marketplace. Even if 90% of the journalists loved the product, (according to Rampell, a few of them even purchased it) there was a good chance that some of the journalists would be taken aback by the PR campaign. And it seems like more than a few were, judging from the number of articles and Blog posts that criticized DidTheyReadIt.

If you subscribe to the motto that there's no such thing as bad press, then maybe this isn't so bad. The PR campaign certainly generated some attention, and some of that attention translated into sales. Over 25,000 people have already taken a look at DidTheyReadIt. And if, as the company claims, 10% of them purchased the software, that's $150,000 in revenue in just over a month. However, the negative press may have tainted RampellSoft, and its founder's reputation in the marketplace. The next product they introduce will likely receive enhanced scrutiny by the privacy police. According to Mr. Rampell, the company was considering developing some privacy enhancing products, but have for the time being at least, shelved those plans due in part to the furor over DidTheyReadIt.

Can we learn something from this?
My philosophy is that technology companies should articulate a clear value proposition when marketing privacy sensitive technologies. It's not simply about doing the right thing anymore. Consumers need to understand what privacy they are giving up, and what value they are getting in exchange. Successful marketers will generate buzz by providing colorful examples of why a product is "useful", "valuable" and "fun." Moreover, they'll de-emphasize the privacy rights they are asking consumers to give up, creating the perception that the positives outweigh the negatives.

I realize that this is to a certain extent an exercise in Monday morning quarterbacking, but I believe that we can all learn from RampellSoft's experience launching DidTheyReadIt. I also realize that there are some people who would have found DidTheyReadIt to be creepy no matter how it was positioned. In this business, there are no guarantees – only the ability to increase your chances of marketplace acceptance. So with that in mind, here's the Chapell view positioning privacy sensitive products.

1. **Gauge consumer perceptions** – I think it's a good idea to run a consumer survey prior to launching any technology product with potential privacy implications. The survey can help develop an understanding of how consumers will react to your product, and uncover potential issues prior to the product launch. Also, it comes in really handy to have objective research stats to sprinkle into your marketing materials.

2. **Always lead with the positive** – The most important thing when positioning a technology sensitive product is to clearly demonstrate why someone would want it. Provide the marketplace with one or more examples of someone getting value from your product. Judging by their press release, DidTheyReadIt did a pretty good job here. For example, the Company described how a customer of DidTheyReadIt was able to determine that an HR department received her resume.

3. **De-emphasize the negative** –It's extremely important for companies to be equally proactive in addressing those concerns. Here's where DidTheyReadIt might have done things differently. They could have emphasized how the technology used by DidTheyReadIt has been used for years by many of the brands that consumers already know and trust.

4. **Notice and Choice** – One of the best ways to reduce privacy concerns is to provide consumers with notice and choice. If the recipients know that they are being tracked, and can decide for themselves whether they want to be tracked in the future, some of the perceived intrusiveness could have been mitigated. Here, the company could have added a disclaimer at the bottom of emails. And the disclaimer could have included opt-out or other disabling instructions so that consumers could choose whether they wanted their emails tracked. According to Mr. Rampell, the Company considered adding a disclaimer, but ultimately decided against it. They were concerned that paying customers might not want a branded message to appear at the bottom of their emails.

In today's environment, many consumer facing technology products have the potential to create privacy concerns. Companies that learn to navigate these challenges will be in a much better position to receive marketplace acceptance.

Alan Chapell is president of Chapell & Associates, a consultancy focusing on privacy, marketing and consumer perceptions. He is the New York chapter co-chair of the International Association of Privacy Professionals, publishes a daily blog on issues of consumer privacy, and will be teaching a class on privacy and marketing at NYU this summer. His e-mail address is achapell@chapellassociates.com.