

NEW PRIVACY ISSUES ON DIGITAL MARKETING & MEASUREMENT

BY JASON CARMEL

“

Smart businesses are considering both privacy and relevance together as they forge their digital experiences online.

”

Online gaffes by top digital properties (Facebook, Google, Etsy, Zappos, etc.) in their attempts to drive targeted, relevant experiences to their customers have highlighted the need to take the issue of privacy much more seriously or risk considerable embarrassment, negative publicity, and a loss of market share. The launch of new privacy settings in Internet Explorer 9, as well as the European Union’s fast-approaching deadline for member states to draft restricting tracking legislation, are the first large scale examples where business and government are attempting to put privacy back in the hands of consumers. How successful are they?”

Increasingly, the tension between the notions of consumer privacy online and dynamically designed experiences based on known characteristics and past behavior are erroneously presented as a tug of war. But privacy is not a zero sum game between businesses and consumers, where comfort and control over the amount of information being collected and shared can only exist at the expense of meaningful, relevant digital marketing and product development.

Smart businesses are considering both privacy and relevance together as they forge their digital experiences online.

Not surprisingly, in the wake of the public outcry, businesses and governments have responded with a variety of proposals to put more control in the hands of consumers. In the last month, two specific executions have garnered significant buzz. The first is the release of in-browser privacy controls, most notably those included in the latest release of Internet Explorer 9. The second is the European Directive on Digital Privacy, scheduled to go into effect in May, which will significantly restrict how a business operating in the member states can drop cookies. These are two very different ways of addressing privacy online and will impact digital marketers and advertisers differently.

IE9 and Tracking Protection Lists

The big focus of the new IE9 tool is to limit the use of third party cookies tracking you from site to site. The controls are designed to limit access to cross-site browsing history rather than the measurement of, say, a how customers navigate a conversion funnel on one’s own site. Say, for example,

the travel site Expedia drops third party cookies from Doubleclick to take advantage of their display media capabilities. The Tracking Protection Lists on IE9, at a restrictive setting, would refuse to accept that Doubleclick cookie, though it would still allow an Expedia cookie to collect data. In that respect, media analytics and retargeting are clearly the most impacted here while site side measurement, optimization and targeting would remain relatively untouched.

Even with third party information sharing restricted, the true impact should not be devastating to digital media targeting and analytics- the Tracking feature is not set as a default for IE9, or for any other browser that is implementing something similar (e.g., Chrome, Firefox). The fact that consumers will have to opt-in to it will likely reduce the adoption rate to somewhere in the range of 8-14%. One could argue that an 8-14% drop in the retargeting pool would significantly hamstring media efforts, but the pool of people who will make use of the Tracking Protection Lists are likely not the people who will engage with display media, anyway (targeted or otherwise). In fact, one could argue that by allowing these privacy-focused consumers to opt-out of targeted media, conversion rates will actually inch up and cost per acquisition will drop.

The browser-based option provided by IE9 has the potential to be an effective tool for consumers concerned about data sharing across sites. Equally importantly, it is executed in a way that provides flexibility to consumers while still allowing business to collect vital information about how their digital properties are performing.

“

...with other privacy-related tools and browser updates on the horizon, it is clear that we are in the third inning of what is surely a long game.

”



ABOUT THE AUTHOR

Jason Carmel is the Director of Marketing Sciences at ZAAZ, a digital agency based in Seattle and part of the WPP/Wunderman network. With 10+ years of digital analytics and targeting experience, Jason manages a team of 50 digital analytics experts responsible for data collection, analysis and site-side optimization for clients such as Ford, Microsoft and Nokia. He has a JD from the Washington College of Law at the American University, and speaks and blogs frequently on behavioral targeting, digital marketing, and privacy.

The EU Privacy Directive

Whereas Microsoft took a proactive approach to allowing customers the flexibility to manage privacy settings, the European Union has opted for a much more heavy-handed approach through legislation.

The EU Privacy directive, approved in 2009 with a deadline for execution in May of this year, requires web sites operating in member states to ask for permission before collecting any data. This effectively requires an explicit opt-in for virtually every cookie, pixel or local object dropped on a site. The point of the Directive is unclear, as it seems to ignore technology already available to the end consumer (via browsers) and puts the burden squarely on every individual website to enact.

Perhaps more troubling is that the directive will be executed differently by separate laws within 27 member states, each of which could mandate a distinct or mutually exclusive mechanism to get consumer consent. European start-ups have been vocal in their outrage, concerned that non-EU competitors will have a competitive advantage.

Whether this is true or not (non-EU companies will still need to abide by the laws if they cater to EU consumers), this broad-brush mandate will have the impact of seriously derailing more than just cross-site information sharing. Under this Directive, simple measurement, optimization and targeted experiences within a business's site would be compromised. Exactly how severe the impact of this Directive is on the ability of businesses to build and maintain usable websites will only be known when all members of the EU have their local privacy laws crafted and available for review.

The Future

With talk from the White House about a need for a Consumer Bill of Rights on Privacy, and with other privacy-related tools and browser updates on the horizon, it is clear that we are in the third inning of what is surely a long game. Until more is known, here are some proactive steps to take:

- Forward the EU directive to your legal counsel and/or review it in detail yourself to understand the full implications. Know that everything about your current data collection process might be impacted—what is collected, where it is stored, and for how long.
- Review your own procedures regarding data collection and use to make sure that they are in line with customers' expectations and your public facing privacy policies.
- Investigate what a “cookie-less” experience would look like for your customers and invest in some usability strategy to determine how you might employ a meaningful “opt-in” interface to data collection on your site.
- Use first-party cookies for analytics wherever possible.
- Stay informed as each EU member enacts its privacy legislation