

Do not track gathers momentum

Will market research be affected by the latest regulations on cookies and tracking technology?

Tracking cookies and other technologies are used by advertising networks to serve behaviourally targeted ads to consumers as they traverse the web. By collecting and examining a consumer's browsing history, advertising networks can present relevant ads that consumers are more likely to notice and value.

Legislators and regulators, however, have expressed concerns about online tracking. The Federal Trade Commission in the US endorses a Do Not Track (DNT) mechanism. In its December 2010 preliminary staff report on online privacy, the FTC stated that consumers should be presented with choices about the collection and sharing of their data at the time, and in the context, in which they are making decisions – not after having to read long, complicated disclosures that they often cannot find.

In Europe, EU legislation has required member countries to implement new cookie rules by May of this year. Only a handful of countries have met the deadline. Member states are interpreting the rules differently. The UK Information Commissioner's Office, for example, says that the new rules require website operators to obtain express consent to use cookies, unless they are "strictly necessary," such as when one clicks on an 'add to basket' or 'continue to checkout' button when shopping online. In addition, a user's browser settings cannot be relied upon to signify consent, especially if internet users do not make any changes to their browser's default settings. The UK deems most browsers not sophisticated enough for website operators to assume that visitors have given consent to receive cookies.

By contrast, the French Parliament recently published legislation that would consider consent given through browser settings to be valid even if users do not set or amend the controls. Finland also permits consent for cookies to be expressed through web browser settings or other applications.

A patchwork of different rules in Europe is nothing new, but it is nonetheless frustrating for website operators. Of concern for the research industry is the impact of DNT and stringent cookie rules on audience measurement, advertising effectiveness, website analytics, and panel-based online tracking in which panel members have explicitly agreed to receive tracking cookies for research purposes.

THE IMPACT ON RESEARCH

Last April, I had the pleasure of representing ESOMAR at a W3C Workshop on Web Tracking and User Privacy. As a condition of attending, participants had to submit a position paper, which I helped develop for ESOMAR and CASRO to submit jointly.

The ESOMAR-CASRO position paper expressed concerns about the scope of DNT, and argued that regulations should be limited to tracking for online behavioural advertising purposes and not legitimate research, which is distinct from advertising and marketing. Legislators around the world saw fit to exempt research from many national Do Not Call registries and anti-spam laws because research is not commercial speech. Further, we have an excellent track record in respecting individuals' privacy and de-identifying data, and we need access to the public to deliver high-quality data on which organisations in the private, public and not-for-profit sectors depend.

Our position paper also commented on DNT solutions that are available in the latest versions of browsers. Firefox offers users a checkbox to tell websites that they do not want to be tracked. Chrome offers a plug-in to allow users to retain desired opt-out cookies when all other cookies are deleted. Internet Explorer (IE) offers the header approach used by Firefox, as well as Tracking Protection Lists (TPLs). TPLs allow anyone to create a list of domains whose cookies and tracking



scripts are either blocked or allowed. To date, four organisations have prepared TPLs for IE users to download: Abine, EasyList, PrivacyChoice and TRUSTe.

BLOCKING PANEL MEMBERS

Unfortunately, a few research domains appear on the PrivacyChoice and EasyList TPLs. This means that panel members using the latest version of IE could download TPLs that block research domains' tracking scripts. Our position paper pointed out that panel companies use explicit consent to track their members' website visits or exposure to ads in return for financial or other rewards. Given that TPLs can have upwards of 4,000 or more blocked domains, we cannot expect panel members to review their filter lists carefully to see if a particular research domain is included.

Panel members, whether unintentionally or deliberately, could thus block research firms from reading the optional cookies that they agreed to receive. For their part, research firms would not know that their scripts were being blocked and could pay rewards to consumers who are not holding up their end of the bargain.

The opinions expressed over the two-day W3C workshop were far ranging. Internet companies, advertising networks and others wanted to limit the scope of DNT to the serving of behaviourally targeted ads. They argued that applying DNT to all forms of online data collection would undermine the internet economy and the security of online transactions. The collection of data is necessary for calculating ad impressions and determining associated display costs, as well as detecting and preventing advertising click fraud. In addition, web log files must be retained for some time so as to be able to conduct forensic investigations of illegal hacks and denial-of-service attacks.

Other participants, meanwhile, argued that DNT should apply to behaviourally targeted ads and most forms of online

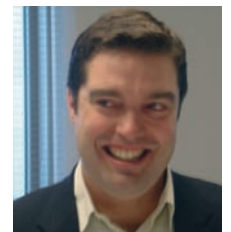
data collection, including website analytics and research. There was also debate regarding whether tracking should be allowed as the default unless individuals opt out via browser settings, or whether the default should be no tracking without an explicit opt-in.

In Europe, regulators appear to be treating tracking cookies used for website analytics or research purposes like tracking cookies used for interest-based advertising.

NEXT STEPS

We must continue to make our case to legislators about the role of research, our codes of conduct and guidelines, and we should communicate what we do to TPL operators. To this end, ESOMAR is surveying market research companies as input for a taxonomy distinguishing the different tracking techniques using cookies applied by research companies. At the same time, we must prepare for a world in which explicit consent is required to set cookies on users' machines.

ESOMAR is monitoring regulatory developments closely and has established a project team to focus on this fast-moving space. **RW**



David W. Stark

is GfK's vice president of compliance and privacy for the Americas, and is a member of ESOMAR's Professional Standards and Legal Committees.
