CASRO AND ESOMAR POSITION PAPER

submitted March 24, 2011 for the

W3C ONLINE TRACKING AND USER PRIVACY WORKSHOP

Introduction

The Council of American Survey Research Organizations, Inc. ("CASRO") and ESOMAR are pleased to submit this position paper and declare our interest in attending the W3C Workshop on Web Tracking and User Privacy.

As the foremost research trade association in the United States, CASRO has long championed the public's right to privacy. CASRO is a not-for-profit association representing nearly three 350 research companies engaged in opinion, social, and marketing research regarding a wide variety of public and private issues.

ESOMAR is the essential organization for encouraging, advancing and elevating market research worldwide. With more than 4,800 members from over 120 countries on both the provider and client side, as well as in public bodies and academic institutions, ESOMAR's aim is to promote the value of market and opinion research in illuminating real issues and bringing about effective decision-making. Together with other industry associations, ESOMAR is representing the sector to the European Commission and Council of Europe, and is working closely with CASRO which represents the sector to the FTC, taking into account the need for a harmonized global perspective relating to online regulation.

Both CASRO and ESOMAR actively advocate responsible and ethical conduct through self-regulation. The CASRO Code of Standards and Ethics for Survey Research and the ICC/ESOMAR International Code on Market and Social Research set forth principles that guide our professional activities, such as requiring researchers to respect and protect the privacy of individuals who participate, whether passively or actively, in social, opinion and marketing research. Core to such self-regulatory Codes is that personal data collected for research purposes must not be used for other purposes and consent must be obtained if further processing is intended at a later date.

Our position

We support do not track proposals to the extent that they allow consumers to opt-out of online behavioral advertising (OBA). The scope of do-not-track should be limited to this activity and tracking where there is criminal or malicious intent. Website analytics and tracking activities conducted by research organizations for legitimate research purposes should be excluded.

Accordingly, we support the HTTP header approach in browser-based do-not-track tools, which would signal to advertising networks that users do not want their online activities tracked across multiple websites for advertising and marketing purposes. We hope that advertisers and marketers honor these requests.

We also support browser do-not-track tools that allow users to better manage their cookies, both browser cookies and local shared objects. Reputable advertising networks offer opt-out cookies to help recognize users who choose not to receive behaviorally-targeted ads. When consumers use their browser privacy settings to remove all cookies, though, their desired opt-out cookies could also be deleted. Add-ons are available for browsers to permit users to persist opt-out cookies, which we support.

We are concerned, though, that another browser-based do-not-track approach, that of using filter lists to block content and tracking scripts, could extend beyond OBA to include legitimate website analytics and research activities. Filter lists that include research trackers could have unintended and undesirable consequences for online panel research firms that obtain explicit consent from individuals to monitor their online behaviors.

Worryingly for consumers, we think that filter lists also have the potential to cause them harm. Conceivably, consumers could download filter lists from a website that they believe is reputable and trustworthy, but this turns out not to be the case. It is possible that consumers could unwittingly download what they believe is a legitimate filter list from a trusted website, but which is in actual fact spyware from a spoofed website. Cybercriminals and identity thieves now have a new means by which to dupe and exploit consumers.

In another scenario, filter list users could visit a website where they currently receive valued content for free and be informed that in order to continue receiving free services, they must download the website operator's filter list. Conceivably, the site's filter list could be set to:

i) allow third-party scripts from an advertising network with which the site does business; and
ii) block third-party scripts from the advertising network's competitors.

Tracking lists could thus be used in unintended and unscrupulous ways that have little to do with protecting consumers' privacy. Indeed, harm could be caused to consumers and to the marketplace.

In addition, we anticipate that the filter list approach could result in an explosive growth in the number of domains involved in online tracking activities, as unscrupulous tracking companies seek to avoid detection by registering multiple domains. Filter lists could give rise to a "whack-a-mole" situation that could prove to be unwieldy. The laudable objective of giving consumers an effective means to filter and control OBA tracking would be severely tested.

Accordingly, we believe that the most effective way to protect consumers from harm and ensure that their do-not-track requests are respected is for the U.S. and other national governments to pass laws that would require companies to honor consumers' wishes not to have their online activities tracked by third parties for OBA purposes. We favor a header approach in which the defined scope is third-party tracking for OBA purposes and we support browser extensions that persist opt-out cookies.

If filter lists are used, though, we believe that regulatory oversight is necessary to define the scope of third-party tracking activities that should be covered in filter lists and which activities should be excluded.

We wish to note that the activities of reputable market, social and opinion researchers are different from marketing, selling and advertising activities. It is important to summarize the distinction.

Market, opinion and social research is distinct from marketing, selling and advertising

Opinion, social, and marketing research is distinct and separate from marketing, sales, and advertising activities and should not be subject to regulations aimed at those activities. While research is used by marketers to test their product or messages, it is not a promotional communication.

Market research, which includes social and opinion research, is the systematic gathering and interpretation of information about individuals or organizations using the statistical and analytical methods and techniques of the applied social sciences to gain insight or support decision making. Research elicits opinions and gathers information on behaviors, attitudes, characteristics, and possessions; it does not solicit money or invite purchases.

Research serves a critically-important function throughout our society to support decision making and to achieve that function, it must, and does, hold to the highest ethical standards of social science inquiry. It is utilized by universities, corporations, research institutes, litigants, politicians, and government agencies to develop behavioral and attitudinal data in support of technical, scientific, economic, health care, pharmaceutical, commercial, social and public policy issues. No other tool permits these constituencies to obtain comparable data or insights capable of serving as a barometer of public sentiment, behaviors, needs and aspirations. Without research, many issues affecting both public and private interests could not be addressed as intelligently or resolved as effectively.

It is important to note that the point of research is not to collect identifiable information for direct action, but rather to measure the behavior of small samples of a defined population in order to ascertain the views or behaviors of the whole population from which the sample was drawn. The risk of harm or adverse consequences for respondents where research is conducted in accordance with professional practices and under the oversight and enforcement of industry codes is infinitesimal.

U.S. federal law has supported the distinction between opinion, social and marketing research and marketing, sales and advertising activities. The Federal Trade Commission acknowledged the importance of research throughout its recent report, *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*. In addition, the FTC has previously written that research is "informational," has "social utility," and is "not commercial speech." It has recognized that distinction by excluding research from regulations that are intended to cover sales, marketing, and advertising activities, such as the Telephone Consumer Protection Act, the Telemarketing Sales Rule, the National Do-Not-Call Registry, and the CAN-SPAM Act.

Accordingly, we believe that browser-based do-not-track tools and any online do-not-track regulations should respect the trust and goodwill that researchers have earned with the public.

The research industry, including opinion, social, and marketing research, must have the ability to access respondents in order to collect and analyze their opinions and behaviors. Research depends on

statistical techniques to improve the quality of the sample and representativeness is a key characteristic for research to be robust for evidence-based policy making. Do-not-track tools that block researchers' ability to access Internet users and measure their online behaviors could degrade the quality of the statistical information and insights that we provide and on which decision-makers in the private, public and not-for-profit sectors depend to better understand consumers, customers and citizens for economic efficiency, innovation and progress.

Online tracking for research purposes

We wish to provide an example of how reputable online panel research firms implement behavioral tracking research among their panel members. From this example, it will be apparent that our industry stands to be adversely affected by do-not-track lists that include research domains.

Online research panels comprise individuals who have agreed to participate in online survey research. Prospective members join a panel by filling in an online form on the panel research firm's website. The form requests basic profile and demographic information and may include other data, such as hobbies and interests. The profile information is used by the panel research firm to select individuals who meet the eligibility criteria for a particular study, e.g. a government agency wishes to test an anti-smoking advertising campaign among young people, aged 18 to 25.

When prospective panel members submit their profile data online, they typically also agree to the terms of participation and the site's privacy policy. In exchange for receiving periodic survey opportunities by email, text message or via a mobile application, panel members receive points that can be redeemed for cash or merchandise when they complete online surveys.

Research firms use first-party cookies for site administration and survey quality control purposes and this is explained in the firms' privacy notices. Some panel research firms offer panel members *optional* cookies for tracking research purposes. If panel members elect to receive the optional cookies, it is with their full knowledge and consent, and they can opt-out at any time by logging into the panel website and indicating their preferences or by contacting the panel manager. Advertising or website content that a sponsoring company would like to measure contains a script that is designed to read the optional cookie that the panel member has explicitly agreed to receive.

Thus, if a research firm's domain is captured in tracking filter lists that are downloaded by panel members, the result is the firm's scripts embedded in ads or website content displayed on third party sites will be blocked. In many cases, the blocking will occur against the wishes of individuals who have agreed to participate in the research firm's optional behavioral tracking research program in exchange for additional survey opportunities (e.g. advertising recall research) that earn them rewards. Most consumers that download tracking filter lists are likely not going to take the time to read upwards of 4,000 or more domains to see if the research firm's domain is included.

From the research firm's perspective, fraud is another possibility. Some panel members could explicitly agree to participate in a research firm's behavioral tracking research program. They could then download a filter list that, with their full knowledge, blocks the research firm's domain.

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. Research firms could thus pay rewards to consumers who are not holding up their end of the bargain.

The integrity of behavioral tracking research conducted by panel research firms, which rely on explicit consent, is thus undermined by filter lists that capture research domains.

Conclusion

In our position paper, we have identified critical issues that need to be addressed and resolved in a timely manner, including:

- The scope of what should be covered in do-not-track browser-based requests;
- The need for do-not-track laws to define the scope;
- The need for careful consideration and regulatory oversight regarding the use of tracking filter lists so that they do not create unintended consequences and cause harm to consumers, fair competition, and the integrity of research;
- The need to recognize the value of research and the responsible conduct of market, opinion and social research organizations that follow established and recognized codes of conduct.

We look forward to the prospect of discussing these issues at the upcoming W3C Online Tracking and User Privacy Workshop.

Respectfully submitted on behalf of CASRO and ESOMAR,

Diane K. Bowers
President
CASRO

170 North Country Road, Suite 4
Port Jefferson, New York
Tel: +1 631-928-6954
Fax: +1 631-928-6041
casro@casro.org
www.casro.org

ESOMAR

Eurocenter 2, 11th floor, Barbara Strozzilaan 384
1083 HN Amsterdam, The Netherlands
Tel: +31 20 664 2141
Fax: +31 20 664 2922
public.affairs@esomar.org
www.esomar.org