Trans Atlantic Consumer Dialogue

DOC No. INFOSOC 45-11 DATE ISSUED: JUNE 2011

Resolution on Behavioral advertising

Introduction

New forms of advertising are emerging online and they are overtaking traditional media as a consequence of the digital shift. With the advent of the Internet and the growth in computer processing and storage capacity, advertisers have the tools to collect and analyse unprecedented loads of data to help target their ads. When surfing the Internet, consumers' data are being collected at different layers, by Internet Service Providers, web browsers, email scanning, publishers, affiliation companies, social network platforms, ad-serving agencies and data aggregator companies. All these layers are increasingly interconnected, thus raising concerns as regards consumers' privacy and protection of their personal data.

Recommendations

TACD resolves that EU and US governments should:

1. Investigate and take regulatory action as needed to address new threats to consumer privacy from the growth of real-time tracking and sales of information about individuals' online activities on ad exchanges and other similar platforms.

2. Commit to developing a global common standard for protecting privacy and consumer welfare in the digital marketplace that reflects the highest possible standards for human rights.

3. Ensure a coherent implementation and proper enforcement of existing personal data protection and privacy legislation rules, including the principles of data minimisation, necessity, purpose limitation, limitation of storage period and data security.

4. Address the constantly evolving techniques used by advertisers for the profiling of online users and adopt measures that go beyond the standard third party cookies that have been the focus of regulators to date.

5. Clarify the rules on informed, specific, revocable and limited consent required to lawfully store information or to gain access to information stored in the user's terminal equipment. There should be specific and rigorous rules on the consent for the processing of sensitive personal data.

6. Carry out a legal gap analysis to assess how the current legislation and regulations on unfair and misleading or deceptive commercial practices applies to profiling and behavioural advertising and adapt new measures if needed.

7. Consider clarifying that matching identifiers and contact data fall under the scope of personal data. Matching identifiers may allow for the cross matching of data from

different sources, while contact data are increasingly being used to send location-specific advertisements to mobile phones' users.

8. Adopt privacy by default as a regulatory principle to ensure that any technology developed is designed with the highest privacy and security requirements and consider the development and implementation of browser control tools to give consumers more control over their data.

9. Improve transparency and fairness of privacy notices though several means including prominent ad tracking disclosure, development of standard and multi-layered privacy notices, use of privacy seals and use of Transparency Enhancing Technologies.

10. Ban the use of Deep Packet Inspection and email scanning technology for the purpose of collecting user information to deliver targeted ads.

11. Develop solutions to enable consumers to receive information about the companies that have had access to his data and to exercise this right to access his personal data.

12. Encourage the development of international standards for behavioural advertising through cooperation within the Organisation for Economic Cooperation and Development (OECD).

13. Adopt specific rules for the protection of children and young people. Online marketing practices that have a negative impact on children and young people's cognitive and emotional development should be prohibited.

14. Monitor closely the merger of online advertising networks and the blurring of boundaries between content and advertising providers and carefully assess the impact on competition and on consumer welfare.

15. Ensure that self-regulation and voluntary codes of conduct fully comply with the principles of independent governance, added value for consumers, effective monitoring, robust sanctions, effective redress and significant market coverage.

16. Set up joint and multi-layered liability rules to ensure that users can claim compensation for any damage suffered from any of the parties involved in the processing of their personal data.

17. Improve the enforcement of existing legislation by Data Protection Authorities and consider the adoption of an instrument of judicial collective redress that would provide for compensation of the damages suffered, together with specific guidelines of the quantification of the damages suffered, which are often moral and of low value.

18. Investigate the emergence of ad exchanges, demand side plaforms, data trading desks that buy and sell individual users in real-time, where they are online—including mobile devices.

Background

Introduction

Profiling has expanded enormously since the arrival of Web 2.0. A number of new business models have emerged that are based on harvesting data from data subjects, and subsequently converting these massive streams of data into profiles. These profiles can then be used to make suggestions or recommendations to users, to improve services, to learn more about customers, or to generate personalised advertising on the Internet. Today, companies are able, via the enhanced possibilities of profiling consumers, to discriminate against consumers i.e. by offering the same products at different prices based on individual users' online profile. Such practices already happen on the Internet.Interactive advertising techniques incorporate some of the latest developments in such fields as semantics, artificial intelligence, auction theory, social network analysis, data mining, and neuroscience.

Consumers and many policymakers are largely unaware about how online advertising operates, let alone its impact. This data collection and targeting apparatus has already been purposely migrated into the core business models shaping social media, mobile devices, gaming platforms, virtual worlds, and online video. Advanced techniques for the buying and selling of individuals online for targeted advertising are found in EU countries, the US, and many other countries.

Targeting and profiling techniques are not as such harmful for consumers; they can even bring forward consumer benefits, if adequately designed. However, many existing practices lack the necessary transparency and accountability.

Consumers should not be expected to understand the privacy dimensions of a "custom targeting" system that uses wide-ranging data sets to determine "the absolute value of each impression" for an advertiser. And even if they did, it is currently impossible for consumers to exercise control over how their data is collected and used. The global growth of real-time digital ad exchanges depends on the ability of advertisers to seamlessly access both online and offline consumer information. To better serve the 21st century digital marketing industry, behavioral targeting warehouses and "co-ops" have been formed. Such services are a kind of data-mining "one-stop-shopping" for online targeting. Across the world, both established companies and new entrants are now part of a consumer data outsourcing supply chain. So-called "third parties" collect and sell information that can be used by ad networks, audience buying platforms, and other data buyers.

The combination of all this data used for real-time targeting should be a central focus for the privacy policy debate. Given the consolidation within the online marketing industry, advances in advertising technologies, the growth of new online ad markets and the dizzying data-chain of partnerships and alliances, it is vital for regulators to develop appropriate rules that reflect today's challenges to privacy.

Many of the same consumer data collection techniques that have raised privacy concerns on the Internet have also been brought into the mobile marketplace. Mobile devices, which know users' locations, are being turned into portable behavioral tracking and real time tracking tools. Consumers are increasingly tracked "across platforms," including when on the Web, using mobile devices, playing online games, or soon when watching television.

The commercial digital media system is largely designed to promote data collection through "360-degree" online marketing strategies. Advertisers are now able to track, buy, and sell an individual in real time, through what's known as digital ad exchanges. In just milliseconds,

a user is subject to an invisible auction process, where advertisers—armed with copious amounts of information on that person—compete in a bidding process for the ability to serve them an ad. Real-time bidding is available for consumer targeting whether they are visiting a website, watching an online video, or using their mobile phone. A complex array of data is used for consumer profiling, tracking, and targeting on these "exchange" and "demand-side" platforms. Data collected on an individual, including via behavioral tracking, "intent" data warehouses, and outside databases, are used to determine the value of an individual targeting "impression."

Online marketers, including Google, Microsoft, and Facebook, have proposed that the U.S. engage in negotiations with the EU on consumer privacy that will lead to a revamped "safe harbor" regime. What U.S. online marketers hope to achieve is a new treaty that creates a "separate, but equal" privacy regime, enabling them to conduct business in the EU as unfettered as possible by rules on data controllers. This approach argues that if the U.S. enacts a federal privacy law—even a weak one relying on self-regulation—it should be treated as the equivalent of the civil liberties-based EU system.

Research evidence

Consumer organisations in the EU and the US have carried out significant qualitative and quantitative research which clearly demonstrates that awareness of online behavioural advertising is low while a significant proportion of consumers currently feel uncomfortable with the idea of being tracked online.

- Research by Which? in the UK found that over 74% of over a thousand respondents had not heard of the term online behavioural advertising and only 50% claimed to understand what cookies are.
- The results of an omnibus study by Consumer Focus (February 2010) have shown that overall 47% of respondents were unsure/did not know/never heard of cookies
- These figures are confirmed by a recent scientific report "Young People and Emerging Digital Services (2009), according to which 82% of young people are concerned that personal information is used without their knowledge, 75% that their identity is reconstructed using personal data from various sources and 69% that their views and behaviours may be misinterpreted based on their online behaviour.

The privacy policies include complex and legal terms which fail to comply with the principles of transparency and fairness, aiming exclusively at complying with legal requirements rather than informing consumers. They are often obscure on issues where clear explanations matter the most, as for instance the question of whether data is shared with or sold to third parties, who these third parties are and what they intend to do with the data, the use of cookies and other data collecting technologies and data retention limits. As a result, consumers rarely read and even more rarely understand privacy notices.

- According to the Eurobarometer survey, 64% of users feel that information on the processing of their data is not yet satisfactory.
- According to a study by the Norwegian Consumer Council, 73% of users aged 15-30 years seldom read Terms of Service,
- The research carried out by Which? in March 2010 found that only 6% adults aged 16+ with internet access questioned have read the privacy policies of websites.

These surveys demonstrate that although consumers are concerned about their privacy, they do not view the privacy policy as a suitable way to understand and answer their privacy concerns

Consumer organisations are also concerned with recent efforts by the advertising industry to develop self-regulatory proposals. These proposals, despite their value in terms of information disclosure about profiling practices, fail to meet the higher standards of governance, independent monitoring, effective sanction, redress and significant market coverage that are needed for self-regulatory schemes to be effective.

- The recent icon-based proposal by the European Advertising Standards Alliance is unlikely to enhance consumers'' empowerment. A recent TRUSTe study in the US of a comparable icon showed that out of approximately 20 million consumers, it was accessed 56,000 times with 44,000 unique views. If calculations are just made on the unique visitors and unique views, this means that only 0.6% of consumers clicked through to the ad info page. This, in no way, signifies informed consent.
- It is also highly questionable whether all industry players will adhere to such self-regulation. The recent example in the UK, where the Code of Conduct by IAB is only applied by 9 out of the 540 members is clear example of the low take-up. Similarly, ad networks do not have to comply with the code if the web publisher is within the same corporate group.
- Even if consumers click on the icon and got to the control page to opt-out, they will only stop receiving ads based on tracking, but their data will continue to be tracked.
- Research conducted by consumer groups in the U.S., including World Privacy Fourm, documents the failure of online ad industry self-regulation.
- The Center for Digital Democracy and U.S.PIRG have documented the failure of the new icon-based self-regulatory system, and also demonsrated that sensitive data—including on a consumer's finances and health interests—is a risk.