"Complexity is Fraud": Why We Must Drop Micro-Targeted Ads to Help Publishers and to Protect Online Privacy

Glyn Moody

November 4th, 2021

It has been clear for years that the widespread use of micro-targeted advertising and real-time bidding represents a huge threat to online privacy. Fortunately, an alternative approach is already to hand. Using contextual advertising, where ads are placed according to the editorial material, rather than based on who is viewing it, would allow the entire surveillance advertising edifice to be dismantled. But there are major forces ranged against the idea. The Internet giants Google and Facebook derive most of their income from privacy-harmful advertising. A huge adtech industry has sprung up to service that approach. The publishers that display many of these micro-targeted ads claim they need them to survive. Many of these players have well-oiled lobbying machines that push these arguments to politicians in order to prevent new legislation from restricting or even banning micro-targeted ads.

Against those massively well-financed and well-connected groups, the fight to rein in micro-targeted advertising might seem hopeless. Nonetheless, there are efforts to counter those powers. Privacy News Online wrote about one of them back in July. The Tracking-Free Ads Coalition is "a coalition of political leaders, civil society organisations and companies from across the EU that are committed to put an end to the pervasive tracking advertising industry that dominates the internet today." It includes 24 Members of the European Parliament from a range of parties. Recently, they took the unusual step of writing to leading businesses that use targeted advertising:

Among civil society there is a growing consensus that the current digital advertising system is posing a burgeoning threat to privacy, societal cohesion and democracy around the world. With this letter, we want to call upon you as corporate leader to stop contributing to the highly opaque and toxic ecosystem of tracking advertising. We call on you to switch to less harmful and still, even more effective, alternatives which are already available.

Another group active in this area is the Irish Council for Civil Liberties (ICCL), not least thanks to the work of Johnny Ryan. He's just written a review of "sustainable publishing and tracking-

based advertising" for the ICCL. It builds on his work last year that explored the privacy risks of real-time bidding. Back then, Ryan claimed that over 100 trillion pieces of personal data were sent out over the Internet as part of the RTB system in a year. His new report seeks to rebut the main arguments of those in favor of surveillance advertising.

For example, Ryan cites three examples where removing tracking has increased publisher revenue. Advertising increased by 149% when Dutch publisher NPO Group replaced micro-targeted ads with contextual ads. Similarly, Web sites operated by a Norwegian news publishing group saw advertisers pay an average of 391% more for contextual ads than for traditional surveillance-based ones. And another Norwegian site found that contextual ads achieved a price that was 210% higher than competing micro-targeted ads. This is a very small sample, so it would be hard to draw any firm conclusions from the figures. But at least it shows that contextual advertising can produce markedly higher revenue in real-world applications.

Ryan points out that tracking-based advertising turns a publisher's audiences into a re-usable commodity for Google and Facebook. In 2004, 51% of Google's ad revenue came from displaying advertisements on publishers' sites. Today, 85% of its ad revenue comes from displaying advertisements on its own Web sites and apps. In other words, Google has used the personal data it gleans from micro-targeted advertising to divert revenue to itself.

There are two other significant ways in which traditional, micro-targeted advertising is bad for publishers – despite their claims to the contrary. For example, Ryan points out that the tracking-based adtech industry is dominated by intermediary companies, not publishers. These adtech companies connect advertisers to publishers, and take large cuts of the fees in the process. The report suggests that these fees can represent 35% to 70% of the money spent by an advertiser. Back in 2016, the Guardian bought some micro-targeted ads on its own site in order to compare how much it was paying with how much it received. In some instances it only earned 30% of the fees it paid.

Unless publishers go to the trouble of carrying out this kind of research, they are unlikely to be aware of just how much revenue goes to the intermediaries because of the complexity and opacity of the ad-buying process. For example, real-time bidding takes place so quickly it has to be completely automated. It is impossible to audit why ads were placed on the chosen sites, and for what price. An excellent report cited by Ryan explains the huge cost of this complexity because of the fraud that it enables:

This year [2020], the losses from digital advertising fraud ($35 billion) have swiftly overtaken global annual credit card fraud ($27 billion). Despite the relatively insignificant digital advertising sector annual spend ($333 billion) compared to the $3.32 trillion credit card sector. The fraud rate in digital advertising is more than six-times higher than the insurance sector, 1.8 times higher than in health care and 13 times higher than the credit card industry.

This again is a factor of complexity and opacity which acts as a breeding ground for fraud, and digital advertising in particular.

The ICCL report quotes PJ O'Rourke, H. L. Mencken Research Fellow at the libertarian Cato Institute, who sums up the situation as follows: "There is a simple rule here, a rule of legislation, a rule of business, a rule of life: beyond a certain point, complexity is fraud." This is a compelling reason why micro-targeted ads based on opaque, algorithmic processes like real-time bidding should be replaced by simpler ones that use contextual advertising. Doing so would reduce large-scale fraud, boost publishers' revenue significantly, and help protect privacy.