The case against behavioral advertising is stacking up

techcrunch.com/2019/01/20/dont-be-creepy/

No one likes being stalked around the Internet by adverts. It's the uneasy joke you can't enjoy laughing at. Yet vast people-profiling ad businesses have made pots of money off of an unregulated Internet by putting surveillance at their core.

But what if creepy ads don't work as claimed? What if all the filthy lucre that's currently being sunk into the coffers of ad tech giants — and far less visible but no less privacy-trampling data brokers — is literally being sunk, and could both be more honestly and far better spent?

Case in point: This week Digiday reported that *the New York Times* managed to grow its ad revenue after it cut off ad exchanges in Europe. The newspaper did this in order to comply with the region's updated privacy framework, GDPR, which includes a regime of supersized maximum fines.

The newspaper business decided it simply didn't want to take the risk, so first blocked all open-exchange ad buying on its European pages and then nixed behavioral targeting. The result? A significant uptick in ad revenue, according to Digiday's report.

"NYT International focused on contextual and geographical targeting for programmatic guaranteed and private marketplace deals and has not seen ad revenues drop as a result, according to Jean-Christophe Demarta, SVP for global advertising at New York Times International," it writes.

“Currently, all the ads running on European pages are direct-sold. Although the publisher doesn’t break out exact revenues for Europe, Demarta said that digital advertising revenue has increased significantly since last May and that has continued into early 2019.”

It also quotes Demarta summing up the learnings: “The desirability of a brand may be stronger than the targeting capabilities. We have not been impacted from a revenue standpoint, and, on the contrary, our digital advertising business continues to grow nicely.”

So while (of course) not every publisher is the NYT, publishers that have or can build brand cachet, and pull in a community of engaged readers, must and should pause for thought — and ask who is the real winner from the notion that digitally served ads must creep on consumers to work?

The NYT’s experience puts fresh taint on long-running efforts by tech giants like Facebook to press publishers to give up more control and ownership of their audiences by serving and even producing content directly for the third party platforms. (Pivot to video anyone?)

Such efforts benefit platforms because they get to make media businesses dance to their tune. But the self-serving nature of pulling publishers away from their own distribution channels (and content convictions) looks to have an even more bass string to its bow — as a cynical means of weakening the link between publishers and their audiences, thereby risking making them falsely reliant on adtech intermediaries squatting in the middle of the value chain.

There are other signs behavioural advertising might be a gigantically self-serving con too.

Look at non-tracking search engine DuckDuckGo, for instance, which has been making a profit by serving keyword-based ads and not profiling users since 2014, all the while continuing to grow usage — and doing so in a market that’s dominated by search giant Google.

DDG recently took in $10M in VC funding from a pension fund that believes there’s an inflection point in the online privacy story. These investors are also displaying strong conviction in the soundness of the underlying (non-creepy) ad business, again despite the overbearing presence of Google.

Meanwhile, Internet users continue to express widespread fear and loathing of the ad tech industry’s bandwidth- and data-sucking practices by running into the arms of ad blockers. Figures for usage of ad blocking tools step up each year, with between a quarter and a third of U.S. connected device users’ estimated to be blocking ads as of 2018 (rates are higher among younger users).

Ad blocking firm Eyeo, maker of the popular AdBlock Plus product, has achieved such a position of leverage that it gets Google et al to pay it to have their ads whitelisted by default — under its self-styled ‘acceptable ads’ program. (Though no one will say how much they’re paying to circumvent default ad blocks.)

So the creepy ad tech industry is not above paying other third parties for continued — and, at this point, doubly grubby (given the ad blocking context) — access to eyeballs. Does that sound even *slightly* like a functional market?

In recent years expressions of disgust and displeasure have also been coming from the ad spending side too — triggered by brand-denting scandals attached to the hateful stuff algorithms have been serving shiny marketing messages alongside. You don’t even have to be worried about what this stuff might be doing to democracy to be a concerned advertiser.

Fast moving consumer goods giants Unilever and Procter & Gamble are two big spenders which have expressed concerns. The former threatened to pull ad spend if social network giants didn't clean up their act and prevent their platforms algorithmically accelerating hateful and divisive content.

While the latter has been actively reevaluating its marketing spending — taking a closer look at what digital actually does for it. And last March Adweek reported it had slashed $200M from its digital ad budget yet had seen a boost in its reach of 10 per cent, reinvesting the money into areas with "'media reach' including television, audio and ecommerce".

The company's CMO, Marc Pritchard, declined to name which companies it had pulled ads from but in a speech at an industry conference he said it had reduced spending "with several big players" by 20 per cent to 50 per cent, and still its ad business grew.

So chalk up another tale of reduced reliance on targeted ads yielding unexpected business uplift.

At the same time, academics are digging into the opaquely shrouded question of who really benefits from behavioral advertising. And perhaps getting closer to an answer.

Last fall, at an FTC hearing on the economics of big data and personal information, Carnegie Mellon University professor of IT and public policy, Alessandro Acquisti, teased a piece of yet to be published research — working with a large U.S. publisher that provided the researchers with millions of transactions to study.

Acquisti said the research showed that behaviourally targeted advertising had increased the publisher's revenue but only marginally. At the same time they found that marketers were having to pay orders of magnitude more to buy these targeted ads, despite the minuscule additional revenue they generated for the publisher.

"What we found was that, yes, advertising with cookies — so targeted advertising — did increase revenues — but by a tiny amount. Four per cent. In absolute terms the increase in revenues was $0.000008 per advertisment," Acquisti told the hearing. "Simultaneously we were running a study, as merchants, buying ads with a different degree of targeting. And we found that for the merchants sometimes buying targeted ads over untargeted ads can be 500% times as expensive."

"How is it possible that for merchants the cost of targeting ads is so much higher whereas for publishers the return on increased revenues for targeted ads is just 4%," he wondered, posing a question that publishers should really be asking themselves — given, in this example, they're the ones doing the dirty work of snooping on (and selling out) their readers.

Acquisti also made the point that a lack of data protection creates economic winners and losers, arguing this is unavoidable — and thus qualifying the oft-parroted tech industry lobby line that privacy regulation is a bad idea because it would benefit an already dominant group of players. The rebuttal is that a lack of privacy rules also does that. And that's exactly where we are now.

"There is a sort of magical thinking happening when it comes to targeted advertising [that claims] everyone benefits from this," Acquisti continued. "Now at first glance this seems plausible. The problem is that upon further inspection you find there is very little empirical validation of these claims… What I'm saying is that we actually don't know very well to which these claims are true and false. And this is a pretty big problem because so many of these claims are accepted uncritically."

There's clearly far more research that needs to be done to robustly interrogate the effectiveness of targeted ads against platform claims and vs more vanilla types of advertising (i.e. which don't demand reams of personal data to function). But the fact that robust research hasn't been done is itself interesting.

Acquisti noted the difficulty of researching "opaque blackbox" ad exchanges that aren't at all incentivized to be transparent about what's going on. Also pointing out that Facebook has sometimes admitted to having made mistakes that significantly inflated its ad engagement metrics.

His wider point is that much current research into the effectiveness of digital ads is problematically narrow and so is exactly missing a broader picture of how consumers *might* engage with alternative types of less privacy-hostile marketing.

In a nutshell, then, the problem is the lack of transparency from ad platforms; and that lack serving the self same opaque giants.

But there's more. Critics of the current system point out it relies on mass scale exploitation of personal data to function, and many believe this simply won't fly under Europe's tough new GDPR framework.

They are applying legal pressure via a set of GDPR complaints, filed last fall, that challenge the legality of a fundamental piece of the (current) adtech industry's architecture: Real-time bidding (RTB); arguing the system is fundamentally incompatible with Europe's privacy rules.

We covered these complaints last November but the basic argument is that bid requests essentially constitute systematic data breaches because personal data is broadcast widely to solicit potential ad buys and thereby poses an unacceptable security risk — rather than, as GDPR demands, people's data being handled in a way that "ensures appropriate security".

To spell it out, the contention is the entire behavioral advertising business is illegal because it's leaking personal data at such vast and systematic scale it cannot possibly comply with EU data protection law.

Regulators are considering the argument, and courts may follow. But it's clear adtech systems that have operated in opaque darkness for years, without no worry of major compliance fines, no longer have the luxury of being able to take their architecture as a given.

Greater legal risk might be catalyst enough to encourage a market shift towards less intrusive targeting; ads that aren't targeted based on profiles of people synthesized from heaps of personal data but, much like DuckDuckGo's contextual ads, are only linked to a real-time interest and a generic location. No creepy personal dossiers necessary.

If Acquisti's research is to be believed — and here's the kicker for Facebook et al — there's little reason to think such ads would be substantially less effective than the vampiric microtargeted variant that Facebook founder Mark Zuckerberg likes to describe as "relevant".

The 'relevant ads' badge is of course a self-serving concept which Facebook uses to justify creeping on users while also pushing the notion that its people-tracking business inherently generates major extra value for advertisers. But does it really do that? Or are advertisers buying into another puffed up fake?

Facebook isn't providing access to internal data that could be used to quantify whether its targeted ads are really worth all the extra conjoined cost and risk. While the company's habit of buying masses of additional data on users, via brokers and other third party sources, makes for a rather strange qualification. Suggesting things aren't quite what you might imagine behind Zuckerberg's drawn curtain.

Behavioral ad giants are facing growing legal risk on another front. The adtech market has long been referred to as a duopoly, on account of the proportion of digital ad spending that gets sucked up by just two people-profiling giants: Google and Facebook (the pair accounted for 58% of the market in 2018, according to eMarketer data) — and in Europe a number of competition regulators have been probing the duopoly.

Earlier this month the German Federal Cartel Office was reported to be on the brink of partially banning Facebook from harvesting personal data from third party providers (including but not limited to some other social services it owns). Though an official decision has yet to be handed down.

While, in March 2018, the French Competition Authority published a meaty opinion raising multiple concerns about the online advertising sector — and calling for an overhaul and a rebalancing of transparency obligations to address publisher concerns that dominant platforms aren't providing access to data about their own content.

The EC's competition commissioner, Margrethe Vestager, is also taking a closer look at whether data hoarding constitutes a monopoly. And has expressed a view that, rather than breaking companies up in order to control platform monopolies, the better way to go about it in the modern ICT era might be by limiting access to data — suggesting another potentially looming legal headwind for personal data-sucking platforms.

At the same time, the political risks of social surveillance architectures have become all too clear.

Whether microtargeted political propaganda works as intended or not is still a question mark. But few would support letting attempts to fiddle elections just go ahead and happen anyway.

Yet Facebook has rushed to normalize what are abnormally hostile uses of its tools; aka the weaponizing of disinformation to further divisive political ends — presenting 'election security' as just another day-to-day cost of being in the people farming business. When the 'cost' for democracies and societies is anything but normal.

Whether or not voters can be manipulated en masse via the medium of targeted ads, the act of targeting itself certainly has an impact — by fragmenting the shared public sphere which civilized societies rely on to drive consensus and compromise. Ergo, unregulated social media is inevitably an agent of antisocial change.

The solution to technology threatening democracy is far more transparency; so regulating platforms to understand how, why and where data is flowing, and thus get a proper handle on impacts in order to shape desired outcomes.

Greater transparency also offers a route to begin to address commercial concerns about how the modern adtech market functions.

And if and when ad giants are forced to come clean — about how they profile people; where data and value flows; and what their ads *actually* deliver — you have to wonder what if anything will be left unblemished.

People who know they're being watched alter their behavior. Similarly, platforms may find behavioral change enforced upon them, from above and below, when it becomes impossible for everyone else to ignore what they're doing.