EUROPEAN INTEGRATION 13.04.2018 | Jennifer Cobbe

Hot data

It's time to take back control of the information that surveillance corporations hold on us

Surveillance capitalism is the business model of the internet. Invented by Google and now used by most online services in some form – including Facebook, Amazon and LinkedIn – it involves the extensive surveillance and modification of human behaviour for profit. The apparatus of surveillance capitalism has enabled data-driven microtargeting by political organisations and hostile governments, and the complacency of its proponents has allowed disinformation and extremism to spread.

Surveillance corporations track us across the internet and throughout our day-to-day lives, watching and recording as much of what we do as possible. When we think of privacy online, we usually think in terms of other people and give comparatively little thought to the corporations to whom we provide troves of data. But this is the true price we pay to use their services: giving up our privacy allows corporations to compile extensive data profiles on each of us.

These don't just comprise the information that we give them about who we are. They also contain information inferred about us from their extensive knowledge of our interests and behaviour. These inferences, covering sensitive and even supposedly secret information, can be made with incredible accuracy. And these profiles contain the knowledge, gained through continual experimentation, of which adverts are most effective at exploiting known shortcuts in human decision-making – called heuristics – and persuading you to click. When you use the internet, you are likely the subject of dozens of experiments that seek to make it easier for corporations to get your money.

Access to this profile – and to the powerful behavioural modification tools that make use of it – is then sold on the advertising market for profit. In effect, surveillance corporations build up detailed models of our interests, our behaviours and our psychological weaknesses, then charge advertisers to use them against us for their benefit.

Where falsehoods run unchecked

Unsurprisingly, the ability to analyse people's behaviour, profile their interests and actions and target them with precisely crafted, empirically tested advertising is of interest to political campaigns. Using tools like Facebook's Custom Audiences and Lookalike Audiences, political organisations can reach large numbers of voters. And the personalised nature of this advertising means that no two voters are likely to see the same set of adverts. On the day of the third debate for the 2016 US Presidential election, for example, Donald Trump's campaign ran about 175,000 variations of its ads, targeting voters closely.

This moves politics and electoral campaigning away from the public sphere, in which ideas can be examined, contradictions challenged and inaccuracies corrected. Instead, campaigns take place in a more private arena, where contradictory arguments may be targeted to different groups without challenge, and where disinformation and outright falsehoods can run unchecked. And, of course, Facebook's lack of oversight has in the past allowed foreign governments to undertake disinformation and manipulation campaigns that seek to disrupt democratic elections.

Facebook carried out its own research on the impact of political messaging on its platform during the 2010 US midterm elections. It found that a single cleverly designed prompt was able to increase a user's likelihood of voting by 0.4 per cent. That's a small effect, of course, but on a national scale it translates to big numbers. Facebook estimates that in 2010 it managed to increase turnout by around 340,000 votes. Microtargeting clearly has the potential to have a major impact on close elections and referendums – in particular in countries such as the UK, where general elections are often decided by a relatively small number of marginal constituencies. Indeed, by one estimate, the Conservative Party missed out on an overall majority by just 401 votes in last year's general election.

Truth is secondary

And surveillance capitalism also contributes in other ways to a negative impact on the public sphere. Facebook's 'fake news' problem is, of course, much discussed, and the fundamental cause is clear. When your money comes from advertising and all that matters is engagement, things like truth, fairness, morals and even common sense are, at best, secondary considerations. As a result, there was little to be gained for Facebook in combating fake news and extremism until it became a matter of public outcry.

But the fake news problem isn't limited to Facebook. Google has faced its own issues, with disinformation and conspiracy theories placed front and centre in search results, in its news services and elsewhere. In the immediate aftermath of the mass shooting in Las Vegas in October 2017, for example, Google News promoted stories describing the shooter as a 'far-left loon' and other politicised disinformation about the event. Google has even been known to push adverts containing fake news on fact-checking websites.

And YouTube, one of Google's services, has repeatedly been shown to drive users to videos peddling extremism, disinformation and conspiracy theories. As a result, it's been described as the 21st century's most powerful radicalisation engine. Even Amazon, which uses a surveillance model to power its recommendation engine, has been at it. An investigation by Britain's Channel 4 News in 2017 found that the site recommended the ingredients for making bombs to shoppers who knew what to look for.

The forthcoming General Data Protection Regulation (GDPR), which strengthens data rights, is a positive step forward. To be introduced at the end of May, GDPR should put a brake on some of the more egregious practices of surveillance corporations and comes with the threat of heavy fines for non-compliance. And the European Union's proposed ePrivacy Regulation, which is strongly opposed by surveillance corporations, promises to strengthen protections for digital privacy. Between them, these two legal frameworks could make a big difference. And corporations themselves could make a positive contribution, by abandoning their surveillance-based business model and using contextual advertising instead.

The time is right

Governments and the EU have for too long taken a hands-off approach. Inaction has enabled corporations' irresponsibility. And proposals put forward by these corporations – which largely amount to giving them more power – are, generally speaking, simplistic and flawed. Regulation of some kind, taking power away from surveillance corporations and requiring them to clean up their act, is needed.

But legitimate concerns around extremism and disinformation must be balanced with freedom of expression and the need to allow even unpalatable ideas to be discussed. We should also be wary of the idea that artificial intelligence will cure these ills. After all, addressing many of these issues requires more human intervention, not less. Automation is not an unqualified good thing. So, while action is needed, governments

and the EU will need to think carefully.

As a society, we're finally waking up to the problems of surveillance capitalism. But it isn't too late for change. The time is right for a proper discussion about the role of these companies in the public sphere, and about what should be done to regulate them. Finding the right answers won't be easy, but it is necessary and it can be done. In the meantime, we should hold these companies to account for their failings and we should demand better. For too long the internet has served corporate interests above all else. But the online public sphere belongs to all of us. It's time to take it back.



Jennifer Cobbe
Cambridge

Jennifer Cobbe is a researcher in the Computer Laboratory at the University of Cambridge, and the coordinator of Cambridge's Trustworthy Technologies strategic research initiative.

-