IPS

GLOBAL CORPORATIONS AND NATION STATES 20.09.2017 | Jennifer Baker

Big tech has become the world's policeman

Who's deciding our future?

We should not allow private companies to take over our law and order. To say this seems self-evident. For-profit companies are interested in making money first and foremost. It is not their job to safeguard human rights, protect the innocent or uphold society's values. And yet this is increasingly what big tech is being asked to do.

It is widely accepted that Facebook and Google are the de facto gatekeepers of the internet. But in fact they are in danger of becoming much more than that. They are not neutral portals through which internet access is granted. That is something closer to what telcos provide. Rather they have become the arbiters of what is and is not acceptable – legal, even – online.

It is a shocking failure of imagination, and possible dereliction of duty, for lawmakers and regulators to abdicate responsibility for digital rights. Yes, it's difficult, and no, regulation doesn't always get it right first time – but to opt instead for an unenforceable 'gentleman's agreement' of self-regulation is lazy, shortsighted and potentially dangerous for democracy.

It is a shocking failure of imagination, and possible dereliction of duty, for lawmakers and regulators to abdicate responsibility for digital rights.

But let's look more closely at what sort of rights we're talking about when we talk about digital rights. 'Online' is not some niche, obscure technical detail to be ironed out. What we are really talking about includes freedom of speech and expression, the right to privacy, and the right to information. Freedoms are also about the rights to be free *from* certain things as well as free to do certain things. Do you really want a company that is beholden to no one but its shareholders to decide whether you should

be free from harassment? What about free from exploitation and manipulation by fake news – particularly when those same companies are fed by the use and data generated by that same fake news?

Censorship by any other name?

In December 2015, the European Commission teamed up with Google, Twitter, Facebook and Microsoft to create the EU Internet Forum to tackle online radicalisation – a worthy aspiration. By signing a voluntary code of conduct, the IT companies committed to 'reviewing the majority of valid notifications of illegal hate speech in less than 24 hours and to removing or disabling access to such content.' In agreeing to this self-regulation, the companies managed to avoid any of that pesky real regulation – the sort that comes with big fines for getting it wrong.

To its credit, the code also 'underlined the need to further discuss how to promote transparency and encourage counter and alternative narratives.' But, although a nice idea, this is not in any way enforceable.

The code is very much focussed on the speed of getting content taken down, which will obviously be at the expense of accuracy. Jillian York, director for international freedom of expression at Electronic Frontier Foundation pointed out recently that Google's anti-bullying AI mistakes civility for decency, and we all know that Facebook's checkers mistake breastfeeding for pornography, so this emphasis on doing more, faster, could have dramatically poor results, taxing an already substandard system.

Algorithm accountability

Unfortunately it's not just the public-facing big tech firms that have become the policemen of the modern world. As pointed out above, it's the algorithms behind them that we need to worry about. Of course Google *et al* want to avoid rules that limit what they can do with all the information they collect, and of course they reserve the right to do whatever they want with their platforms to make the most money possible, but I don't believe they're intentionally setting out to destroy democracy one app at a time. However, the secrecy around algorithms and the decision-making process is worrying.

Look at Google's transparency report on the Right to be Forgotten and you will see bland examples of decisions made, but no real indication

about how decisions are arrived at in trickier cases.

In the US, a recent American Civil Liberties Union report pointed out algorithms are everywhere: 'They can decide whether you get a job interview, how much credit you access, and what news you see. And, increasingly, it's not just private companies that use algorithms. The government, too, is turning to proprietary algorithms to make profound decisions about your life, from what level of health benefits you receive to whether or not you get charged with a crime.' Predictive policing is just the thin edge of the wedge in this regard.

Algorithms are everywhere: 'They can decide whether you get a job interview, how much credit you access, and what news you see.'

Earlier this year MEPs called for the European Commission to take 'any possible measures to minimise algorithmic discrimination, including price discrimination, where consumers are given different prices of a product based on data collected from their previous internet behaviour, or unlawful discrimination and targeting of certain groups or persons defined by their race, colour, ethnic or social origin, religion or political view or being refused social benefits'.

While there is clearly a need for greater accountability and transparency of algorithms, that is an uphill battle as companies will cry 'trade secret' if asked to hand over anything but the most basic information.

What can be better controlled – and to give credit where it's due, the EU's General Data Protection Regulation is a big step in the right direction – is what personal information these companies are gathering about us in order to make their godlike decisions.

According to Eddie Copeland, director of government innovation at Nesta: 'Without a radical rethink about the future internet we want, we risk sleepwalking into a world in which a few online platforms have total dominance of our online lives. That is bad for privacy, bad for trust, and bad for innovation. The key to building a fairer internet is to give people a real choice in how their personal data is used.'

A new report from DECODE, a major EU Horizon 2020 project, concludes that 'citizens have unwittingly surrendered their online identities to a handful of big digital platforms, with little transparency about how their information is used for profit or influence'. Equally, because of this, a multitude of social and economic opportunities are

being missed.

The DECODE paper imagines six personas from the year 2035 that are broadly optimistic, including: Florence who shares information about her long-term health condition with researchers of her choice via an opt-in data commons; and Sarah, an ethically-minded entrepreneur, who minimises the amount of personal data she gathers and uses anonymous customer analytic data for business development.

This is the rosy view of the future. Without hard thinking and hard work it won't happen. Instead we'll have Jill who is investigated by social services for posting an image of bathing her child, or Fred who is detained by police for clicking 'like' on a dubiously worded post; along with millions of others who won't be able to tell if they are being offered a product or if they are the product since by then 'consumer laws' will have given way to self-regulation.

Jennifer Baker
Brussels

Jennifer Baker has been a journalist in print, radio, and television for nearly 20 years, the last eight specialising in EU policy and legislation especially in the tech/digital sector. Her aim is to translate EU policy-speak and tech jargon into understandable English. She likes good books and bad films.