The DSA fails to reign in the most harmful digital platform businesses – but it is still useful

Sebastian Becker Castellaro 2022-11-08T09:40:32

The Digital Services Act (DSA) adopted by the European Parliament on 5 July 2022 was lauded by some as creating a "constitution for the internet" and a European response to the "digital wild west" created by Silicon Valley.

Together with many other civil society organisations, European Digital Rights (EDRi) has been working extensively with the EU's institutions to ensure that the new regulation not only fulfils this promise but, by doing so, protects the fundamental rights of people and reaffirms the open internet as a public good. To some extent we have succeeded. But the DSA is far from perfect and much will depend on how well the new regulation is going to be implemented and enforced.

This essay argues that while the DSA has just been crafted carefully enough to avoid major damage to digital rights in the EU, it has focussed so much on who must delete what kind of content within which time frame, that it missed the bigger picture: no content moderation policy in the world will protect us from harmful online content as long as we do not address the dominant, yet incredibly damaging surveillance business model of most large tech firms.

This essay builds its legal and policy observations on EDRi's DSA research and advocacy work of the past three years.

Freedom of expression online and the role of online platforms

One of the main pillars of the DSA is the new content moderation framework for online platforms such as Facebook, YouTube and Twitter. This framework consists of a conditional liability regime that follows the logic of the EU's Electronic Commerce Directive (ECD) and the jurisprudence of the Court of Justice of the European Union. Just as under the ECD, online platforms can only be held liable for user-generated content if they have "actual knowledge" of the illegality of that content, and – just as under the ECD – the DSA continues to prohibit EU Member States to impose any obligation for platforms to generally monitor user content.

These principles aim to protect freedom of expression by ensuring that online platforms are not incentivised to over-police people's online speech. Therefore, the EU's decision to uphold the conditional liability regime and combine it with a mandatory 'notice-and-action' system that should enable users to flag illegal content and complain about the platforms' inaction are considered by many civil society

organisations to be welcome steps in the right direction. This is particularly true when compared to the various dangerous proposals that were put forward by some EU member states and Members of the European Parliament: from 24-hour removal deadlines from the moment of flagging to mandatory and generalised content surveillance by platform companies. Many of those dangerous proposals would have almost entirely dismantled free expression rights of all platform users.

However, the DSA's strong focus on the comprehensive regulation of user-generated online content has also somewhat obstructed the view on the bigger questions: Why does harmful or illegal content spread so expansively on social media in the first place? What responsibility do online platforms' algorithms play in the distribution and promotion of online content? And what are the commercial incentives that guide the development of those algorithms?

These questions motivated EDRi's digital rights advocacy early on, aimed at understanding the commercial interests of large online platform providers and at highlighting their role in actively distributing and amplifying different kinds of online content, including through and funded by surveillance-based online advertising.

Big Tech is broken by design and by default

When online platforms moderate and recommend online content, they can do so based on various rules and factors. This includes their own terms and conditions, applicable law in the country where a given piece of content was posted from, as well as what kind of content maximises the platform's profits. The larger the profits, the stronger the incentive to let them guide content moderation and recommendation practices.

EDRi and many other organisations and researchers have shed light on how companies such as YouTube's Alphabet Inc (US$ 76 billion net income in 2021) and Facebook's Meta Inc (US$ 39 billion in 2021) continuously optimise their content recommendation algorithms in view of maximising their profits.

But it is not only the company's size that matters.

The business models of most of the largest tech firms are built around what we call "surveillance-based advertising" – digital ads that target people based on personal, often very sensitive data that those firms extract from us all. It is "extracted" because while this data is sometimes explicitly provided by users, it is most often information inferred from our observed behaviour online: every website we visit, every article we read, apps we install, product we buy, our likes, our comments, connections, and many more sources of metadata are being combined into the largest commercial collection of individual profiles that humankind has ever seen.

All of this just to enable companies to fill our screens with advertising micro-targeted at us, trying to convince us to buy more stuff.

Deception as a service

In theory, under the EU's General Data Protection Regulation (GDPR), this type of data collection for marketing purposes is only legal with people's consent. Yet, many companies deploy deceptive designs in their user interfaces. Those include, for example, consent pop-ups that do not offer users meaningful ways to reject tracking, that trick users into clicking "accept", or do not provide the necessary information about how personal data would be used for advertising.

These deceptive designs (or dark patterns) are currently deployed on 97% of the 75 most popular websites and apps according to a 2022 study. Hence, they continue to play a central role in the surveillance-driven advertising business. Companies are of course fully aware of what they are doing: in its 2018 annual report, Facebook stated that the regulation of deceptive design "could adversely affect [their] financial results". Both Meta and Google have joined other tech firms in firmly opposing any deceptive design regulation in the DSA.

Not least thanks to civil society's advocacy, the final DSA does recognise the negative impact that deceptive interface designs have on users' privacy rights, but heavy corporate lobbying has led it to contain only very limited restrictions: While Article 25 prohibits interface designs that "deceive or manipulate the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions", this prohibition only applies to online platforms (such as Facebook, TikTok, YouTube, or Twitter), not to websites that embed, say, Google ads. More crucially, the prohibition does not apply to practices covered by GDPR and the Unfair Commercial Practices Directive (UCPD) – a limitation that will exclude all consent pop-ups for personal data collection.

Tracking-free ads instead?

Knowing that the DSA was unlikely to solve these problems, more than 20 Members of the European Parliament, 50+ civil society organisations, and many ethical tech firms banded together in the Tracking-Free Ads Coalition (EDRi is a supporter), to achieve more substantive change: an end to surveillance-based advertising altogether.

This attempt sparked a colossal counter-lobbying campaign that included full-page newspaper ads from Facebook, social media ads micro-targeted at MEPs, as well as Brussels' billboards and other ad spaces covered all with a single message: European SMEs need surveillance-based online advertising to reach customers. Without them, the EU economy basically falls apart.

As a result, the DSA addresses surveillance-based ads only with half-baked restrictions in Article 26. It prohibits providers of online platforms to "present advertisements to recipients of the service based on profiling" as defined by GDPR, as well as to use "special categories of personal data referred to in Article 9(1)" of the GDPR.

Just as with deceptive interface designs, those restrictions only apply to online platforms as defined in the DSA, but not to websites, apps or other intermediary services that embed Google ads, for example. Worse, the DSA limits the prohibition to ads shown by platforms *to their own users*. Providers are therefore free to micro-target such ads to anywhere else on the web, if they offer this kind of service. This does not respond to the actual and current ad tech ecosystem. In practice, the prohibition in the DSA will not cover things like cookies and tracking banners that appear as advertisements on most webpages thanks to Google ads services.

Even worse still, Article 26 does not address the use of proxy data for sensitive characteristics. While a platform will not be allowed to target ads based on the sensitive category “race”, they can simply replace it with a generic proxy “interested in African-American culture” or “K-pop”. While targeting based on health data, for example based on pregnancy, won’t be allowed anymore, a platform can simply use a category based around “interest in baby toys”. As long as those proxies cannot be construed as “revealing” sensitive data (which would be prohibited again), anything goes. As a result, this DSA provision is unlikely to protect people from the discrimination and abuse of personal data that the ad industry enables.

A semi-positive conclusion

Despite all the shortcomings touched upon above, EDRi holds that the DSA is a positive step forward. That is because, while not ambitious enough, it has — maybe for the first time in Europe — enabled politicians and the public to debate and understand the harms inflicted by the data-driven advertising models that many of the largest tech firms would rather keep hidden from public view.

Now it is known that Google is not a search engine provider and Facebook never was a social media company. They are global commercial surveillance corporations.

The biggest contribution of all debates around the DSA is that next time around, lawmakers and the public are already aware.
