PHYS.ORG

Social media doesn't need new regulations to make the internet safer – General Data Protection Regulation can do the job

February 14 2019, by Eerke Boiten

Credit: AI-generated image (disclaimer)

From concerns about data sharing to the hosting of harmful content, every week seems to bring more clamour for new laws to regulate the technology giants and make the internet "safer". But what if our existing data protection laws, at least in Europe, could achieve most of the job?

Germany has already started introducing new legislation, enacting a law in 2018 that forces social media firms to remove hateful content. In the UK, the government has proposed a code of practice for social media companies to tackle "abusive content". And health secretary Matt Hancock has now demanded laws regulating the removal of such content. Meanwhile, deputy opposition leader Tom Watson has suggested a legal duty of care for technology companies, in line with recent proposals by Carnegie UK Trust.

What's notable about many of these proposals is how much they reference and recall the EU's new General Data Protection Regulation (GDPR). Hancock, who led the UK's introduction of this legislation (though he has also been accused of a limited understanding of it) referred to the control it gives people over the use of their data. Watson recalled the level of fines imposed by GDPR, hinting that similar penalties might apply for those who breach his proposed duty of care.

The Carnegie proposals, developed by former civil servant William Perrin and academic Lorna Woods, were inspired by GDPR's approach of working out what protective measures are needed on an case-by-case basis. When a process involving data is likely to pose a high risk to people's rights and freedoms, whoever's in charge of the process must carry out what's known as a data protection impact assessment (DPIA). This involves assessing the risks and working out what can be done to mitigate them.

The important thing to note here is that, while earlier data protection laws largely focused on people's privacy, GDPR is concerned with their broader rights and freedoms. This includes things related to "social protection, public health and humanitarian purposes". It also applies to anyone whose rights are threatened, not just the people whose data is being processed.

Existing rights and freedoms

Many of the problems we are worried about social media causing can be seen as infringements of rights and freedoms. And that means social media firms could arguably be forced to address these issues by completing data protection impact assessments under the existing GDPR legislation. This includes taking measures to mitigate the risks, such as making the data more secure.

For example, there is evidence that social media may increase the risk of suicide among vulnerable people, and that means social media may pose a risk to those people's right to life, the first right protected by the European Convention of Human Rights (ECHR). If social networks use personal data to show people content that could increase this risk to their lives then, under GDPR, the network should reconsider its impact assessment and take appropriate steps to mitigate the risk.

The Cambridge Analytica scandal, where Facebook was found to have failed to protect data that was later used to target users in political campaigns, can also be viewed in terms of risk to rights. For example, Protocol 1, Article 3 of the ECHR protects the right to "free elections".

As part of its investigation into the scandal, the UK's Information Commissioner's Office has asked political parties to carry out impact assessments, based on the concern that profiling people by their political views could violate their rights. But given Facebook's role in processing the data involved, the company could arguably be asked to do the same to see what risks to free elections its practices pose.

Think about what you might break

From Facebook's ongoing history of surprise and apology, you might think that the adverse effects of any new feature in social media are entirely unpredictable. But given that the firm's motto was once "move fast and break things", it doesn't seem too much of a stretch to ask Facebook and the other tech giants to try to anticipate the problems their attempts to break things might cause.

Asking "what could possibly go wrong?" should prompt serious answers instead of being a flippant expression of optimism. It should involve looking not just at how technology is intended to work, but also how it could be abused, how it could go too far, and what might happen if it falls victim to a security breach. This is exactly what the social media companies have been doing too little of.

I would argue that the existing provisions of GDPR, if properly enforced, should be enough to compel tech firms to take action to address much of what's wrong with the current situation. Using the existing, carefully planned and highly praised legislation is better and more efficient than trying to design, enact and enforce new laws that are likely to have their own problems or create the potential for abuse.

Applying impact assessments in this way would share the risk-based approach of enshrining technology firms with a duty of care. And in practice, it may not be too different but without some of the potential problems, which are many and complex. Using the law in this way would send a clear message: social media companies should own the internet safety risks they help create, and manage them in coordination with regulators.

Provided by The Conversation

Citation: Social media doesn't need new regulations to make the internet safer – General Data Protection Regulation can do the job (2019, February 14) retrieved 24 April 2024 from https://phys.org/news/2019-02-social-media-doesnt-internet-safer.html