IMD
REAL LEARNING. REAL IMPACT

TOMORROW'S CHALLENGES

GDPR ISN'T ENOUGH TO PROTECT US IN AN AGE OF SMART ALGORITHMS

FACEBOOK AND GOOGLE ALREADY FACE A LEGAL COMPLAINT IN THE WAKE OF THE NEW DATA PROTECTION LAW, BUT THE MOST PRECIOUS DATA STILL ISN'T COVERED

By IMD Professor Howard Yu

IMD
Chemin de Bellerive 23
PO Box 915,
CH-1001 Lausanne
Switzerland

Tel: +41 21 618 01 11
Fax: +41 21 618 07 07
info@imd.org
www.imd.org

Europe's new privacy law comes with teeth. Within hours of the General Data Protection Law (GDPR) coming into effect, an Austrian privacy campaigner used the new EU legislation to file a legal complaint against Facebook and Google. It's too early to tell how the case will be resolved but companies that violate the law can be fined up to 4% of annual revenue. That means the two companies could be fined a total of €7.6 billion (£6.6 billion).

Yet, even as most internet users were dealing with a deluge of GDPR-related emails from companies trying to follow the law, it occurred to me that what is possibly the most strident attempt by lawmakers to protect people's privacy still won't be enough. Not even nearly. The problem is that the law doesn't protect the data that is most precious to tech firms, the inferred data produced by algorithms and used by advertisers.

The basic premise of GDPR is that consumers must give their consent before a company such as Facebook can start to collect personal data. The company must explain why data is collected and how it's used. The firm also isn't allowed to use the data for a different reason later on.

All these rules naturally translated into consent boxes that "popped up online or in applications, often combined with a threat, that the service can no longer be used if user(s) do not consent", observed Max Schrems, the campaigner who has filed the complaint against this "take it or leave it" approach.

Still, any new cases against Facebook and Google could go the way of the current enquiries into the Cambridge Analytica scandal. Addressing EU representatives during a parliamentary hearing, a suited-up Mark Zuckerberg was recently seen rehashing a familiar narrative, that he's sorry and hasn't "done enough to prevent harm". "Whether it's fake news, foreign interference in elections or developers misusing people's information, we didn't take a broad enough view of our responsibilities," he said.

In other words, a highly technical challenge concerning data security and consumer privacy has been reduced to a public spectacle of remorse and redemption. And when the resolution comes in, just as with GDPR, it will arrive in the shape of email consent forms full of incomprehensible fine print and terms and conditions. The greatest danger of this is that the public will be blinded from seeing what truly matters.

Where the social networking sites, search engines and big online retailers have truly succeeded so far is in defining the "personal data" that lawmakers say requires protection. The data that GDPR covers includes credit card numbers, travel records, religious affiliations, web search results, biometric data from wearable fitness monitors and internet (IP) addresses. But when targeting consumers, such personal data, though useful, is not paramount.

For example, if TV network HBO wants to advertise the new season of Game of Thrones to anyone reading an article about the show on the New York Times website, then all HBO needs is an algorithm that understands the behavioural correlation, not a demographic profile. And those all-knowing algorithms, the under-the-hood machine learning tools that power everything from Facebook's news feed to Google's self-driving cars, remains opaque and unchallenged. In fact they have their own protections in the form of intellectual property rights, making them trade secrets much like the Coca-Cola recipe.

But the difference between Coca-Cola and Facebook is, of course, in their business models. Facebook, Google, Snapchat and YouTube all generate revenue through advertising. Consumers pay for their Coca-Cola but they get their digital services for "free". And that seemingly free service has introduced what economists call the "principal-agent" problem, meaning tech firms may not act in consumers' best interest because they are the product not the customers. This is exactly why Sheryl Sandberg, Facebook's chief operating officer, has said Facebook users can't opt out of sharing their data with advertisers because that would require Facebook to be "a paid product".

GDPR could open the way for a solution

But this is not unsolvable. Tech companies could be required to nominate independent reviewers, computer scientists and academic researchers to conduct algorithm audits to ensure any automatic decisions are unbiased and ethical.

Data scientists working at tech companies could also be required to ensure that any smart algorithm follows the principle of "explainable artificial intelligence". This is the idea that machine learning systems should be able to explain their decisions and actions to human users and "convey an understanding of how they will behave in the future".

What is unique about the tech world today, and remains virtually incomprehensible to those who work outside the sector, is the minimal level of reassurance and regulation of the basics it has come to expect. Facebook's shares have already recovered since the Cambridge Analytica scandal.

This shows that the biggest potential payoff of GDPR is not so much immediate protection of consumers, but the chance to open up an arena for public debate. Imagine consumers could one day voice their grievances over unfair targeting, or challenge the logic of a proprietary algorithm at a public tribunal, staffed by independent computer scientists. It is this kind of built-in scrutiny that will make a fairer and more useful internet. GDPR is the first step in this direction.

Howard Yu is the LEGO professor of management and innovation at IMD and Director of the Advanced Management Program. His upcoming book is Leap: How to Thrive in a World Where Everything Can Be Copied.

This article was first published by The Conversation.