Fact, fiction and fake news—the involvement of data and analytics

28/04/2017

IP & IT analysis: Dr Felipe Romero-Moreno, lecturer at the University of Hertfordshire and member of the executive committee of the British and Irish Law, education and technology association, explains how data and analytics intersects with the current global problem of fake news. He outlines that although states are becoming more involved in the issue and more technologies—including Artificial Intelligence (AI) systems—are being developed to tackle its spread, the fundamental question of who should be allowed to determine what is and is not fake news remains a problem.

What kinds of issues does collecting and verifying data create in terms of producing reliable news stories and opinions? What regulatory issues can arise?

The kinds of issues that arise largely depend on the way the data is being collected and verified. Given the vast amount of new user-generated content that's produced daily worldwide, the ease with which it's generated, and its economic profitability in terms of advertising revenue, it is presumed that such data gathering and verification would have to be done through automatic means. A parallel could be drawn here with copyright. Currently, automated solutions are being used to combat online piracy due to the large volumes of new user-generated content being generated in breach of copyright law. For example, copyright holders are currently using software to:

- detect instances of online copyright infringement
- notify internet intermediaries of that infringement, and
- require such intermediaries either to takedown the infringing content (notice and takedown), or to ensure that this content is de-indexed and does not reappear again on the internet (notice and staydown)

However, while verifying data is important when trying to produce or check news stories, there are inherent problems with such automated processes. In terms of notice and takedown, for example, Google has recently reported that 99.95% of trusted takedown requests generated by automated systems under the US Digital Millennium Copyright Act 1998 were bogus.

Notice and stay down, meanwhile, would require installing content identification and filtering technology. It is worth noting that while the terms ‘content identification’, ‘filtering technology’ and ‘blocking technology’ are frequently used interchangeably—there is an important difference between them. Namely, that content identification and filtering entails the ‘real-time’ identification of infringing material (monitoring), while blocking prevents access to predetermined infringing material, for example, a URL ‘blacklist’ (please see: Perspectives on Policy Responses to Online Copyright Infringement).

Importantly, while blocking measures are legal under EU law (see the Court of Justice in UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and anor, Case C-314/12, [2014] All ER (D) 302 (Mar)), content identification and filtering measures would be incompatible with Article 15(1) of the E-Commerce Directive 2000/31/EC, which prohibits internet intermediaries, such as social networking sites, from carrying out general monitoring of the information stored. As flagged above, this is because content and filtering technology involves real-time monitoring of content.

Moreover, such a general monitoring obligation would contradict Article 3 of the Enforcement Directive 2004/48/EC, which states that measures adopted by internet intermediaries must be proportionate and fair and must not be unnecessarily expensive (see Court of Justice case decisions of Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10, [2011] ECR I-11959 at paras [35] and [36], Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV, Case C-360/10 at paras [33] and [34], and Tobias Mc Fadden v Sony Music Entertainment Germany GmbH, Case [2016] C-484/14, at para [87]).

What is the current legal framework for dealing with these sorts of issues?

As of March 2017, there is no legal framework for dealing with these kinds of issues in the UK. However, it should be noted that, on 30 January 2017, the culture, media and sport committee launched an inquiry into fake news more generally. The Committee defined this problem of fake news as the growing phenomenon of widespread distribution (via the internet and social media) and acceptance as fact of news with questionable accuracy or provenance.

Damian Collins MP, chair of the Committee, stated in Parliament on 30 January 2017 that:

‘The growing phenomenon of fake news is a threat to democracy and undermines confidence in the media in general. Just as major tech companies have accepted they have a social responsibility to combat piracy online and the illegal sharing of content, they also need to help address the spreading of fake news on social media platforms. Consumers should also be given new tools to help them assess the origin and likely veracity of news stories they read online. The Committee will be investigating these issues, as well as looking into the sources of fake news, what motivates people to spread it, and how it has been used around elections and other important political debates.’

In his statement, Mr Collins highlights the fact that internet intermediaries have a responsibility to combat fake news, just as they have in combating online piracy. However, it remains to be seen whether the British government itself will consider taking legislative action to address fake news more directly in the future, in the same way that it is current also tackling the issue of online piracy in its Digital Economy Bill 2016-17 (DEB). It is worth noting that the DEB, which is currently before the House of Lords, would allow English and Welsh courts to impose sanctions for online copyright infringement up to ten years in prison, for example. Although, this Bill has also raised issues about the powers it would give government has the power to share and collect the private information of citizens.

To what extent can and should unreliable data prevent publication of a news story?

In Joined Tele2 Sverige AB v Post- och telestyrelsenk, Cases C-203/15, [2016] All ER (D) 107 (Dec) and Secretary of State for the Home Department v Tom Watson, C-698/15, [2016] All ER (D) 107 (Dec) at para [94], the Court of Justice found that, under Article 52(1) of the EU Charter, any restriction upon the exercise of the rights and freedoms protected by the Charter (namely, the right to freedom of expression and information, ie EU Charter) must be provided for by law and must respect the essence of those rights and freedoms. The court explained that in order to assess whether the principle of proportionality had been infringed, restrictions might be imposed upon such rights and freedoms, only if they were necessary and genuinely met EU objectives of general interests or protected the rights and freedoms of others.

In order to ascertain the extent to which unreliable data could or should prevent the publication of misinformation would largely depend on the compatibility of said prevention or interference with the three-parts of the Court of Justice’s non-cumulative test. Under the EU Charter, any interference with the right to receive and impart information (Article 11 of the EU Charter), such as preventing the publication of a news story featuring unreliable data (fake news), must:

- be ‘provided for by law’
- genuinely meet objectives of general interest or protect the rights and freedoms of others, and
- be ‘necessary’ and ‘proportionate’

In terms of the test’s third prong, in its decision of Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU, C-275/06, [2008] All ER (EC) 809, the Court of Justice held that, where several fundamental rights and freedoms were at stake, it was for the domestic courts and authorities involved—in our case, the UK courts—to ensure that a fair balance was struck between all those rights (Productores de Musica de Espana v Telefonica de Espana, at paras[68] and [70]).

Ultimately, if the publication of fake news (based on unreliable data) were to be prevented, it must be compatible with the three-parts of the Court of Justice’s non-cumulative test. If this were not the case (for example, being incompatible with at least one prong of the three-parts of the Court of Justice’s non-cumulative test), such prevention would constitute a violation of the EU Charter, specifically the right to freedom of expression and information, under Article 11 of the EU Charter.
Can artificial intelligence help identify ‘fake news’ and what are the limitations of this approach?

Yes, it can. For example, Google has recently developed Perspective, a piece of software that utilises machine learning to flag up problematic comments. The technology has been developed by Jigsaw, the Google division that aims to tackle digital security threats, such as cyberbullying and extremism. It learns by looking at how thousands of posts have been moderated (namely, how human reviewers have previously assessed the content) and then keeps count of new posts by evaluating how ‘toxic’ they are and whether similar posts had resulted in other users leaving conversations. Every time the technology identifies new instances of possibly toxic language, or is given corrections from moderators, it can improve on scoring future posts.

This technology has already been tested by the New York Times, and it is expected that other news outlets, such as The Guardian and The Economist, as well as online sites like Wikipedia might use it in the future. It is also reasonable to assume that social media platforms such as Facebook and Twitter might consider using the software in the future. Perspective is, however, still in development mode, meaning that it is too early to assess its effectiveness.

However, relying on automated systems like Perspective to identify new instances of possibly toxic language can lead to over-blocking (ie a blockage of legal content), not to mention the mistaken identification of information in the process of the software trying to learn and improve on scoring future comments. It is, therefore, arguable that such systems should always be accompanied by several layers of human review.

Moreover, as Google itself has stressed, the main issue here is who should be allowed to decide what does and does not count as fake news. Should it be the internet service providers, search engines, hosting services, social media platforms, users, or the state, for example? There is no easy answer currently, which is why, as the BBC reported in February 2017, it does not seem that Google will be using its own artificial intelligence solution in the near future.

Are there any areas where this technology is already making headway (ie in combating ‘spear phishing’ and what lessons can be learnt from their deployment?)

AI and other technologies are currently being used to tackle the spread of digital misinformation—in particular, the detection of malevolent phishing emails. ‘Spear phishing’ is a similar, but more problematic area (it is a more refined and dangerous process that often targets specific and often vulnerable people) that this technology is also trying to tackle. However, the current use of automated solutions in tackling online copyright infringement is one of the most notable examples of where these technologies are making headway. Namely, relying on notice and takedown and content identification and filtering (ie notice and staydown) approaches.

However, there are two potential problems related to the deployment of these systems. The first is the previously mentioned risk of over-blocking, that is to say, the blocking of content that is legal and does not need to be blocked. Google recently flagged numerous examples of such over-blocking activity, such as a film studio sending a takedown request for a ‘neutral network’ test relating to Blade Runner, which was clearly fair use. (The content that was reported as online copyright infringement was not part of the Blade Runner film, but an AI encoding project trying to reconstruct Philip K Dick’s movie.) This problem is highlighted by the rulings of Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) and Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV at para [50]), where the Court of Justice held that since technical measures did not differentiate adequately between illegal and legal information, their introduction could lead to the blocking of legitimate content.

The second possible problem is the risk of mistaken identification. As noted earlier, Google reported that 99.95% of recent notice and takedown requests generated by bot software under the US Digital Millennium Copyright Act 1998 were erroneous. In fact, in L’Oréal SA and others v eBay International AG and others, Case C-324/09, [2012] All ER (EC) 501, the Court of Justice confirmed that when using automated solutions one needs to be particularly careful because ‘notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated’ at para [122].

For this reason, before these technologies are actually put into use, a case can be made that they should be checked and authorised by either state authorities, such as the UK Information Commissioner’s Office (ICO), or the courts. After this stage has been cleared, it should additionally be supplemented by human review.
How can data and information literacy and education be used to combat the dissemination of fake news?

The first way to tackle the dissemination of fake news is by giving the reader of the news the tools to act like a fact checker and detect misinformation. Wineberg and McGrew of Stanford University consider that a possible answer to the fake news problem is to educate users so that they can check facts in order to verify and assess the validity of news sources for themselves. A framework could be developed to help consumers follow links to other sources of information in order to find out more about the topic before reading it—this would enable them to assess the content and to compare it with other sources and content.

Another potential solution would be to use a referencing system to check the accuracy of information. Over time, peer checking (like the system used for Wikipedia) can result in more trustworthy news and less partisan publications. Readers can create, polish, and fact-check materials with neutrality, verifiability, and no original research. Copy-edits, for example, can be looked at behind the page. In fact, these days, Wikipedia is often portrayed as being as rigorous as the Encyclopaedia Britannica. If an approach such as this is eventually adopted—perhaps one with a kind of ‘value mark’ indicating that the content has been authenticated—then it could be possible to verify and assess the validity of information at the source (See BILETA Response to the Culture, Media and Sport Committee’s ‘fake news’ inquiry at page 7).

Is the law keeping apace with the latest developments and what should lawyers advising in this area be aware of?

As is generally the case with situations such as these, it would be reasonable to suggest that the law is lagging behind the rapid pace of technological change. For example, at the same time that the UK government is inquiring into the fake news phenomenon, new technology such as Google’s Perspective has already been developed to help auto-moderate the publication of online comments. Therefore, there are several important things that lawyers should keep in mind when advising in this area.

Firstly, while it is possible to require internet intermediaries, such as ISPs, search engines, and social media platforms to take technical measures to combat fake news, this solution is not desirable. This is due to the costs and burdens it places on service providers, the potential for censorship (giving rise to freedom of speech issues) and manipulation of the content, not to mention the human rights issues involved. This ‘solution’ also raises the fundamental policy question of who should be allowed to decide what constitutes misinformation: internet intermediaries, users or the state (See BILETA Response to the Culture, Media and Sport Committee’s fake news inquiry at pages 6–7).

However, adopting a ‘follow the money’ approach (such as squeezing the advertising revenue of rogue sites) could be of help. The rationale behind such a strategy is that by restricting the ad revenue of infringing websites or by cutting the payment processor activities enabled on such sites, the owners of pirate websites are unable to make money from them, thus making them commercially absurd or unworkable as a result. For example, in the UK, as part of the Operation Creative partnership with online advertising companies, the City of London Police Intellectual Property Crime Unit (PIPCU) replaces ads on alleged copyright infringing websites with police warnings.

In my view, however, the most appropriate and effective way to solve this issue may be user education from childhood to adulthood, as well as the development of specific targeted skills, such as critical reading and critical thinking. For example, BBC Newsround (aimed at young users) has recently published some useful guidance and techniques about how to respond to fake news. Education initiatives such as these, in particular those aimed at young people, are to be commended and encouraged.

Are there any other trends or developments in this area which are worthy of mention?

Globally there are numerous trends in the area of fake news.

China

The problem of fake news is nothing new in China. State censorship in the region means that a significant amount of web content (in particular matters related to dissenting groups) is labelled as ‘fake’ in one form or other.
In fact, at the 2016 World Internet Conference held in Wuzhen, as a result of the recent fake news stories stemming from the US presidential election, coupled with the threat of terrorism, the internet was branded as uncontrollable and dangerous by the Chinese Government. There has been a subsequent rise in China suppressing and controlling more information.

Ren Xialing of the Cyberspace Administration of China, meanwhile, has proposed the identification of those who are publishing misinformation and falsehoods so as to give rise to criminal liability.

Germany

Chancellor Angela Merkel has supported a proposal to make the posting of fabricated stories a criminal offence, particularly those that are widely disseminated through social media. This would also require internet intermediaries (social media platforms, for example) to expeditiously remove this content. Since there is a growing concern that fake news could affect the upcoming elections, it is thought that this legislation is likely to pass.

The German Government has also stated that Facebook will be subject to fines for the publication of misinformation.

Iran

The Government of Iran has announced that it is determined to regulate fake news. One such measure they are pursuing is introducing legislation to target public news channels on the instant messaging service, Telegram. Given the popularity of the service, it’s assumed that a significant proportion of the Iranian population must trust the news released on Telegram’s channels. It has therefore been decided that channels with an excess of 5,000 subscribers will be required to hold a licence. Iran’s Minister of Information and Communications Technology, Mahmoud Vaezi, noted that the publication of false information poses a particularly serious problem for the countries less developed and rural regions.

Italy

Giovanni Pitruzzella, the head of Italy’s competition body (Autorità Garante della Concorrenza e del Mercato), has argued that the fake news phenomenon should be tackled by independent authorities with the support of the state. He recommended that such a scheme should be handled in a similar manner to the way they deal with EU competition law. Namely, that an independent authority would be able to initiate legal proceedings against publishers of fake news, in the same way the Commission can launch proceedings against corporations for violations of competition legislation.

United States

One solution, suggested by US Congresswoman Marsha Blackburn, is the involvement of ISPs in the regulation of fake news. However, there are those—like American journalist, Ari Melber—who suggest that the spread of misinformation should be regulated by the Federal Trade Commission (FTC) in the same way the organisation tackles fraud. It has been proposed that the FTC could cooperate with Congress in tackling the fake news problem, or build a dedicated framework to tackle it independently. The problem remains, however, as to whether this would give such a body (with unelected officials) the power to determine what real news is (see BILETA Response to the Culture, Media and Sport Committee’s ‘fake news’ inquiry at pages 8–9).

Interviewed by Giverny Tattersfield.

This article was first published on Lexis®Library IP & IT 28 April 2017. Click for a free trial of Lexis®PSL. The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor