MISINFORMATION AND THE INTERNET

Richard Spearman QC – 39, Essex Chambers

Misinformation takes many forms, ranging from a single untruth about a particular individual or company at one extreme to "fake news" and propaganda which may affect governments, nations and international relations at the other. Somewhere in the middle is the kind of information which is typically likely to be of most concern to Chancery practitioners, such as that which may impact on financial transactions and, possibly, markets.

As with most things, one can say of misinformation that "There is nothing new under the sun". However, the impact of the Internet in this area has been profound: what are new on a practical level are matters such as the scale and effectiveness of distortions of the truth, and, in legal terms, when it comes to giving effect to the rights or interests which are adversely affected by misinformation, problems such as accountability and lack of effective remedies.

The problems in outline

The New Zealand Law Commission analysed the nature of the problems in *News Media Meets New Media: Rights, Responsibilities and Regulation in the Digital Age* in 2011.

With regard to the practical problems of "reach" and "spread", the Commission stated: "Before the advent of the web, the risk of causing harm to others through the exercise of free speech was most commonly a question that concerned the news media rather than ordinary citizens. However, now that everyone has the ability to publish, these risks – and potential liabilities – are much more widely shared … Then there is the difficulty of spread. Once published, a piece of information can "go viral"; it may be taken up and repeated by others."

With regard to the main legal problems of "uncertainty" and "enforcement", it stated: "The law imposes constraints on certain types of speech and in some circumstances provides remedies for those harmed by others' speech. However most of these laws were drafted in the pre-digital era and questions now arise as to how effective they remain … If an infringing publication has taken place, who can be held accountable, and against whom will criminal sanctions or civil remedies lie? Possible defendants are any media company responsible for the publication; the editor of the relevant publication (if there is one); the individual who wrote and/or uploaded the item in question; the host of the website on which the item has appeared; and (possibly) the internet service provider (ISP). The current law is complex and unclear. The answer may well be different for the purpose of different rules … Sometimes, even if the law clearly has been broken, there may be problems enforcing it. The fact that the internet has no geographical boundaries and that once published, information can be stored and accessed from a practically limitless number of places making it difficult, if not impossible, to remove, are among the challenges posed."

Traditionally, the mass communication of misinformation was beyond the capabilities of anyone other than political parties or large media organisations. The public were able to familiarise themselves with these sources of information and, over time, to assess their reliability. In the age of the Internet, it may be much more difficult to decide which sources are trustworthy and which are not. For example: there is in practical terms no limit on the number of sources of widely available information; it is relatively easy to imitate the news format; and skilful operators may be adroit at duping artificial intelligence and manipulating algorithms so as to give their reports a spurious appearance of credibility. Intermediaries such

as Google and Facebook are perceived, in general terms, as providers of beneficial services, and it is understandable that many users may find it hard to sort the wheat from the chaff.

Relevance to financial transactions

Misinformation involving the Internet may crop up as an electronic version of long-standing market manipulation ploys, such as the unethical "pump and dump" promotion of share prices, the propping up or inflation of stock values by false claims relating to company assets (for example, stories of medical or technological breakthroughs which do not, in truth, exist), or the unjustified denigration of competitors or takeover targets.

One manifestation occurs in online paid stock-promotion campaigns, which typically involve articles being published on investment websites without the appropriate disclosure of payment, in order to promote a company's stock and affect investor decisions: once the truth is uncovered, these stories ultimately lead to losses for investors.

The solutions in outline

The possible solutions to the problem are those considered by the New Zealand Law Commission in *Rights, Responsibilities and Regulation in the Digital Age*: voluntary action, criminal proceedings, substantive claims, amenability to injunctions; and, maybe, regulation.

Voluntary action

One difficulty about relying on voluntary action by intermediaries is that reducing or eliminating misinformation may be contrary to their commercial interests. Revenues and profits are influenced by content availability and traffic volumes, and there are costs associated with policing content or investigating and acting on complaints. In addition, identifying what is and what is not misinformation may be far from straightforward.

Intermediaries are capable of taking relevant measures: for example, in the run up to the general election in the UK on 8 June 2017, Facebook announced that it was taking measures which included use of its systems "to recognise …inauthentic accounts more easily by identifying patterns of activity – without accessing the content itself", that it had suspended 30,000 accounts in France before the first-round presidential election, and planned to remove tens of thousands of further accounts, and that "To help people spot false news we are showing tips to everyone on Facebook on how to identify if something they see is false".

However, an indication of how far intermediaries will go in resisting measures which threaten their revenues – typically under the banner of defending freedom of expression – can be gleaned from Google's opposition in the USA to the Stop Enabling Sex Traffickers Act, which will (for example) restrict backpage.com, reportedly a major child sex trafficking site.

Criminal proceedings

Criminal prosecutions may be effective against wrongdoers and, perhaps, have a chilling effect on others. But their deployment, whether against individual wrongdoers or even more so intermediaries, may be problematic. So far as concerns the UK, the Report of the Leveson Inquiry into the culture, practices and ethics of the British press states: "… the ability of the UK to exercise legal jurisdiction over content on Internet services is extremely limited and dependent on many things… which are rarely aligned. These include: the location of the service provider; the location of the servers on which material is held; and international agreements and treaties."

In the USA, the Securities and Exchange Commission announced on 10 April 2017 a crackdown on alleged stock promotion schemes, which led to charging 27 individuals and entities with misleading investors into believing they were reading "independent, unbiased analyses" on websites such as Seeking Alpha, Benzinga and Wall Street Cheat Sheet.

Substantive claims

The traditional tortious remedies for economic loss and claims based on reliance on online material may be capable of providing an effective response. In the case of online paid stock-promotion campaigns, and depending always on the particular facts, there is no reason, in principle, why an investor should not have legal remedies not only against the false information provider, but also against the operator of the investment website, and, it may be, the company itself if it knew about the fake news or failed to police it. In an appropriate case, a claim for conspiracy may be available. This requires (1) a combination of two or more persons; (2) to take action which is unlawful in itself; (3) with the intention of causing damage to a third party; (4) who suffers the damage (see *Kuwait Oil Tanker v Al Bader* [2002] 2 All ER (Comm) 271, Nourse LJ at [108] and [110]), and liability has been extended on the facts of some cases to those who only join in at a late stage or play only a minor role.

In *Taberna Europe CDO II Plc v Selskabet AF1 (formerly Roskilde Bank A/S (In Bankruptcy))* [2016] EWCA Civ 1262, the claimant purchased from a third party subordinated loan notes issued by the defendant bank, having regard to an "investor presentation" on the defendant's website. When no payments were made on the loan notes, the claimant claimed damages from the defendant on the basis that it had been induced to purchase the loan notes by misrepresentations made by the defendant in that "investor presentation". The defendant succeeded on appeal on the ground, among others, that, in answer to the claimant's claim, it was entitled to rely on disclaimers in the "investor presentation" to the effect that no representation was made as to any information therein. On different facts, a claim against the operator of a website based on reliance on misinformation made available on that website might well succeed.

Where misinformation involves defamation, in principle a claim will be available against the author(s) of the defamatory words. However, they may be hard to identify or locate, and, even if they can be served with proceedings, they may lack the resources to provide appropriate compensation. More effective protection for the victims of libel would be available if intermediaries such as search engines were treated as publishers for the purposes of the law of libel (just as search engines are treated as data controllers for the purposes of the law of the protection of the personal data of data subjects: see *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez* Case C-131/12). However, to date that is not the approach that has been taken by the English law of libel (see, for example, *Tamiz v Google Inc* [2013] EWCA Civ 68).

Injunctions and their limits

The need to face up to the argument that, at least in some circumstances, injunctions have no sensible place in the age of the Internet was recognised in *PJS v News Group Newspapers Ltd* [2016] UKSC 26. In that case, the Court of Appeal discharged an interim injunction which it had granted at an earlier hearing to protect private information, because, in the intervening period, the story, including the names of those involved, had been published in the USA, Canada and Scotland, on Internet websites and on social media. On the second occasion, the reasoning of Jackson LJ involved an acceptance that "the Internet and social networking have a life of their own". The claimant appealed to the Supreme Court, which, by a majority,

allowed the appeal and ordered the continuation of the interim injunction until trial or further order. Lord Mance said at [45]: "At the end of the day, the only consideration militating in favour of discharging the injunction is the incongruity of the parallel - and in probability significantly uncontrollable - world of the internet and social media, which may make further inroads into the protection intended by the injunction".

In the area of copyright law, however, the Information Society Directive recognises that the services of intermediaries "may increasingly be used by third parties for infringing activities" and that "In many cases such intermediaries are best placed to bring such infringing activities to an end" (see Recital (59)), and Article 8(3) of that Directive has been transposed into domestic law by s97A of the Copyright Designs and Patents Act 1988. This provides that the High Court "shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright". Since the original test case of *Twentieth Century Fox Film Corpn & Ors v British Telecommunications plc* [2011] EWHC 1981 (Ch), the Court has granted injunctions pursuant to s97A on many occasions. Further, in *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2016] EWCA Civ 658 (Ch), the Court of Appeal upheld the decision of Arnold J that the High Court has power to grant a comparable injunction in a trade mark case in spite of the fact that no specific step comparable to s97A has been taken to implement the equivalent provision in the Enforcement Directive (Article 11). If the like reasoning could be relied upon in cases of misinformation, that might provide a real remedy.

Regulation as a solution

In Germany, and in spite of strenuous arguments to the contrary about the threat to freedom of expression and the dangers of turning intermediaries into policemen and censors who may feel impelled to err on the side of caution in denying access to statements of doubtful reliability, the view has been taken that strong measures are required. Against the background that research in Germany showed that Facebook and Twitter were not complying with a code of conduct that they signed in 2015 concerning the deletion of hate speech, the German government resolved to extend to at least some forms of false news the proposal to, in effect, convert that code into a law covering hate speech, defamation, threats and incitement. In outline, under the Network Enforcement Act social networks have 24 hours to delete or block criminal content and 7 days to deal with less clear-cut cases, as well as an obligation to report back to the person making the complaint as to how the complaint was handled. The regime provides for fines of up to €50m for a company and up to an additional €5m for its chief representative in Germany, and Germany would like it to become Europe-wide.

That would be in keeping with the protection afforded by European legislation in other areas. The Recitals to the General Data Protection Regulation, which comes into effect on 25 May 2018, state that technological developments and globalisation "require a strong and more coherent data protection framework in the Union, backed by strong enforcement", and the sanctions which may be imposed under it include fines of up to the higher of 2% of worldwide turnover and €10m in respect of some breaches and up to double those figures in respect of others.

Conclusion

The harmful consequences of misinformation involving the Internet are clear and serious. Intermediaries seem best placed to bring harmful actions to an end, but also appear unwilling to shoulder their responsibilities voluntarily. Regulation could be the only effective answer.