Fake news, disinformation, manipulation and online tactics to undermine democracy

Susan Morgan

Routledge
Taylor & Francis Group

INTERVIEW

Check for updates

Fake news, disinformation, manipulation and online tactics to undermine democracy

The supporting infrastructure of a healthy public sphere is under strain. There are fundamental challenges facing journalism as it seeks a sustainable financial model. Evidence is growing of the sophisticated manipulation of technology platforms. Novel ways to use citizen data are exposing widening gaps between the practices around elections and the current regulations that underpin them. Questions of foreign meddling abound. Classic tactics of disinformation seen in authoritarian regimes are emerging in Western states, and the economic insecurity of millions of people is fuelling a growing disaffection with politics.

There is an urgent need to find ways to enable democracy to defend itself, and to bring into the open the intentional tactics being used to undermine public discourse and democracy. Susan Morgan, Senior Program Officer at the Open Society Foundations, speaks with Journal Editor Emily Taylor about the fragility of the online public sphere, the ways in which technology is being manipulated for political purposes, and suggested responses for civil society and government regulators to create resilience in the digital world.

Do you think democracy is in crisis? Can you describe some of the current challenges facing the digital information ecosystem and a healthy online public sphere?

What is happening to the online public sphere is complex. First of all, disinformation and fake news are widespread, and those seeking to manipulate the online public sphere can capitalise on declining levels of trust in institutions and experts. There are different motivations for the types of propaganda and 'fake news' we are seeing. Sometimes, it is a deliberate attempt to spread false information or sow doubt in people's minds as in Russian *disinformatzya* tactics. At other times, the motivation is purely financial, as in the case of Macedonian teenagers who were targeting Trump supporters in the 2016 US presidential election for the advertising revenue they received. And at this time when established sources and institutions have lost credibility and people struggle to accurately identify when news is false, these factors contribute to potentially fertile ground for those wishing to manipulate opinion in a particular direction.

Secondly, there is a tremendous concentration of power and money held by internet platforms. Currently, major internet platforms are not regulated as media companies (despite in many instances curating content) or as public utilities. The intermediary liability protections internet companies have enjoyed in much of the world in recent years facilitated a flourishing of free expression online. Opportunities for free speech crept into relatively closed societies via the internet. But there is now an extraordinary concentration of market power in a very few US-based technology companies, raising serious questions in a world where artificial intelligence and technology have the potential to transform whole sectors of the economy in the way we have seen in recent years with news.

Thirdly, we are living with a radically altered media landscape where tech platforms are now receiving the bulk of advertising revenues which used to go to traditional news publishers including local newspapers. The growth of what Tim Wu from Columbia Law School has described as the attention economy: 'the resale of human attention – that is, gathering eyeballs or access to the public's mind and selling it to advertisers.' raises profound questions about the news people access (do clicks matter above all else?) and whether citizens understand this new landscape where misinformation and disinformation proliferate online alongside traditional journalism.

You mentioned that there are different motivations for spreading the kinds of propaganda and fake news we have been hearing about in the media over the past year. Who exactly is spreading propaganda and can you describe some of the different kinds of tools and techniques that are used to manipulate public opinion?

There are many different actors involved and we're learning much more about the different tactics that are being used to manipulate the online public sphere, particularly around elections. There are numerous examples of hacking, leaking and the insertion of fake information into troves of dumped documents online. The US alt-right, along with bots, played a role in amplifying the #Macronleaks that took place just 48 hours before the second round of the French presidential elections. After Macron's emails were hacked, fake documents were inserted into them suggesting Macron had connections to offshore financial accounts. What is interesting to see here, is not only the coordination involved in both the leaking of fake and genuine documents and then the spreading of this information on Twitter, but also the role of foreign actors, including the US alt-right in a French election. This suggests that efforts at manipulation across geographic boundaries are occurring now not only in state-sponsored efforts, but also through motivated individuals and groups wishing to promote a particular world view.

The US presidential election in 2016 saw the behavioural targeting of voters and using this data to suppress voter turnout. The US presidential election in 2016 provided several examples of this tactic. For instance, in the days before the election, messages circulated on social media that Hillary Clinton had died. And in some key battlegrounds, messages were targeted at Democrat voters claiming that the date of the election had changed. Politics and political campaigns increasingly look like classic consumer marketing, with political parties taking advantage of sophisticated data capture, segmentation and micro-targeting techniques. At the same time, there is currently little serious public discourse on the potentially serious ethical and philosophical implications for democracy and open societies.

Another trending tool is the use of automated accounts or bots to shape the news agenda. These kinds of accounts play an important role in the amplification of false information and fake news. Co-ordinated activity by fake accounts can increase the likelihood of something trending on Twitter, or can reduce the chance of legitimate news being found by internet users. A study conducted by Jonathan Albright at Elon University, examining the 2016 US presidential election, showed strong evidence that partially automated accounts were flooding Twitter hashtags, such as #podestaemails. Researchers at the Computational Propaganda Project at the Oxford Internet Institute researchers have

concluded that the most powerful computational propaganda efforts are those with bots and trolls (so, automation and human curation) working together.

In the United States and the United Kingdom, there have been a number of investigations into the role of foreign states in meddling with elections. Do states typically target other states with computational propaganda and fake news?

Foreign meddling in elections and the affairs of other countries more broadly is both far from new and incredibly topical. Recent years have seen Russia significantly expand its news coverage in other countries, which is often used as a proxy for influence by organisations which analyse foreign influence. Evidence of their specific intervention on particular topics such as French identity and immigration around the time of the French elections suggests an interest in moving the discourse in a particular way. In the French example, there was evidence of Russian influence on both the right and left of the political spectrum online.

On what kinds of platforms does this happen? Is it just Twitter and Facebook? Or are other online platforms used to disseminate misinformation?

Many messaging boards are important for political manipulation. In the alignment of politically-motivated actors with an agenda and geeks messing with the system for the lulz, messaging boards such as 4chan, 8chan and Discord have played an important role in the developing and testing of messaging, and served as a useful staging post prior to the wider distribution of messages or leaked documents through social media. Prior to the US election, some stories that started on 4chan (for example, Hilary Clinton's health) found themselves eventually in the mainstream media, with the help of bots and the pressure on the mainstream media to feed the 24/7 news cycle.

What is industry doing to address this problem and do you think these steps are enough to solve some of the challenges of misinformation in the digital age?

As concern and public awareness has grown over the ability of far-right and other interest groups to deploy sophisticated tactics to manipulate news and opinion, tech companies have announced a raft of initiatives. Shortly after the US presidential election, Facebook said it would make flagging false stories a key element in its attempts to tackle fake news. Facebook is now working with fact-checking institutions such as Fact-check.org, ABC and Associated Press, referring stories reported by users to these institutions for verification. False stories are now flagged on Facebook. It is still too early to tell whether this effort will have tangible results or will instead spur greater attempts by people to spread false stories.

As tech companies are increasingly receiving advertising revenues which previously went to news organisations, those platforms have begun programmes and initiatives to help support journalism. However, company initiatives to date do not address the more fundamental issues created by their dependence on eyeballs and clicks, and their stance on regulation seeks to preserve by and large the current hands-off approach. Whether it's going to be possible to address the challenges of retaining a healthy public sphere without changes being made at a more fundamental level is difficult to say, but this must remain an active area for further consideration.

What are governments doing to regulate some of the challenges that platforms may themselves not be able to fix?

Governments are becoming increasingly concerned about fake news, misinformation and the way the public sphere can be manipulated. Several governments have announced enquiries, are establishing units to debunk fake news and are proposing legislation and regulation. Egypt and the Gambia have long had legislation aimed at combatting fake news, which has been criticised by free speech advocates. The German parliament recently passed a law to fine social media companies with more than two million users for failing to remove certain content (such as fake news and hate speech) within 24 hours. In Italy, the anti-trust chief Giovanni Pitruzzella has called for the EU to establish agencies which can fine companies for spreading false information.

Some countries are at an early stage in tackling issues related to fake news and misinformation. For others, misinformation has already been a long struggle and the digital aspect merely brings a new dimension. There has long been tension between the desire to allow free speech to flourish and, even in a Western democratic context outside the US, a desire to curb the most undesirable forms of speech around terrorism and hatred. The momentum for governments to act to tackle fake news and misinformation is now translating into practical actions, many of which could legitimise the actions of non-democratic nations and harm free speech.

What interventions would you recommend that government regulators and industry representatives to make, and what are some of the broader challenges that incentivise the spread of misinformation?

In recent elections we've seen various tools, tactics and actors exposed. However, the research to date is too often sporadic work, or lacking the necessary infrastructure for it to happen in a systematic, coordinated way. There needs to be increased international collaboration and the sharing of methodologies and results.

There should also be a commitment from political parties in democracies to greater transparency on how they are using citizen data. There are enormous opportunities now for political parties and campaigns to very specifically target voters around elections and referenda. Current regulation of this activity is lacking and will need to be addressed. But for the moment this leaves democracies vulnerable and citizens in the dark as to what is happening. Political parties have an ethical choice to make on what methods they use and how transparent they are about it.

We also need to create incentives for tech companies to open useful data sources. The large tech players hold vast troves of data that could be an invaluable resource in helping those trying to minimise or counter the manipulation of the online public sphere. They also profit financially from the activities of political parties around elections. As a part of their contribution to tackling the issues, and reflecting the critical role they play in this ecosystem, these companies could open those data points to external experts who are working to find solutions.

A fourth recommendation would be to require companies to take more action to tackle bots.

Bots account for a tremendous amount of traffic on social media, particularly Twitter. If companies fail to step up to this challenge voluntarily, governments should initially put in place incentives for companies to act through self-regulatory mechanisms.

Finally, we need long-term policies to help citizens become more informed about how the online public sphere is shaped. Individuals in society need to understand much more about how the online public sphere works, in order to build resilience into the democratic system. It is reasonable to assume that we won't be returning to a media landscape where there are only a few arbiters of truth, and this shift is to be welcomed. However, this places responsibility on each and every one of us to understand more about what is happening as other actors work to address the systemic vulnerabilities that are being uncovered.

Susan Morgan
Open Society Foundations