Second reading briefing – Representation of the People Bill
Establish stronger rules to deal with political deepfakes

The government's policy paper for electoral reform recognised that our democracy *"is being threatened by misinformation"*. The Prime Minister has said he is *"very worried about the potential for misinformation in future elections in this country."* However, the Representation of the People Bill does not address this serious and growing threat, and risks being a missed opportunity to safeguard UK democracy and restore public trust.

Advances in AI now allow realistic, cheap, false and digitally manipulated videos and audio (deepfakes) to be created quickly and shared at scale online. The Bill does not currently address this emerging risk.

The threat of political deepfakes

Deepfakes can misrepresent politicians, mislead voters and distort public debate. This increases the risk that voters make decisions based on fabricated material, particularly in the final days of a campaign when corrections may not reach the same audience or travel as far.

As deepfakes proliferate, many people report difficulty distinguishing synthetic from real content. In a 2024 survey by Ofcom, 56% of people expressed concern about the impact of deepfakes on the general election, while 46% were unsure whether they had seen one. The combination of concern and uncertainty risks eroding confidence not only in individual pieces of content, but in the integrity of political information.

In 2025, George Freeman MP reported to the police a deepfake purporting to show his defection to Reform UK. The video was widely shared on social media, illustrating how quickly synthetic material can circulate. However, the deepfake reportedly did not meet the test for a criminal offence. This incident is one of a growing number of examples internationally of misleading AI-generated political content spreading.

Gaps in the law and regulatory framework

Section 106 of the Representation of the People Act 1983 criminalises false statements about a candidate's character or conduct to affect their return at an election. It was drafted in an era of printed leaflets and does not explicitly address synthetic audio or video, cloned voices or manipulated material.

Both the Electoral Commission and the Speaker's Conference on the security of MPs, candidates and elections have called for the offence to be updated to expressly cover digitally manipulated false statements. It is currently unclear whether a deepfake would be treated as a false statement for the purposes of the offence.

This ambiguity weakens deterrence and risks inconsistent enforcement during an election campaign. Without legislative clarity, police, prosecutors, regulators and platforms may interpret the law inconsistently during an election period. Legal uncertainty increases the risk that harmful deepfakes will continue to circulate.

There is also no statutory requirement for parties and candidates to label AI-manipulated political content. The Electoral Commission suggested that social media platforms should require labelling of AI-modified content during election periods to *"complement existing digital imprint rules, helping voters understand who is paying for and promoting campaign content as well as whether this content has been altered using AI."*

Recommendations

(1) Clarify legal coverage of AI-generated content

The government should issue formal guidance clarifying whether key electoral offences – including false statements about candidates and undue influence – apply to AI-generated or digitally manipulated content. If they do not apply, the Bill should amend those offences to explicitly include synthetic audio, video and imagery.

Any amendment should be carefully drafted to protect satire, parody and legitimate political expression.

(2) Require transparency markers

The Bill should require campaigners to include a clear transparency marker on any campaign material that manipulates the voice, image or video of a political figure. The marker should clearly state:

- the name of the promoter;
- the person and party on whose behalf it is published; and
- that the content has been digitally altered.

Failure to comply should attract proportionate civil sanctions to deter non-compliance.

Conclusion

Parliament has an opportunity to ensure electoral law keeps pace with rapidly advancing technology before the next general election. These measures would provide legal clarity around key electoral offences, deter the creation and dissemination of harmful political deepfakes, and enable voters to identify manipulated content quickly. Failing to act would leave a known vulnerability in the UK's framework for democratic resilience.

This is one in a series of briefings by Full Fact on measures to strengthen the Bill:

1. Upgrade the Online Safety Act to safeguard the UK's democracy.
2. Create stronger rules to deal with political deepfakes.
3. Establish a comprehensive public library of political adverts.
4. Regulate to prevent misinformation and disinformation in political campaigns.
5. Create a transparent system for dealing with electoral information incidents.
6. Increase the investigative powers of the Electoral Commission.
7. Give platforms a statutory duty to support effective media and political literacy.

For more information, please see our policy paper. To discuss the issues raised in this briefing, please contact George Havenhand, Policy Manager at Full Fact, on george.havenhand@fullfact.org.