15 WHITEHALL, LONDON, SW1A 2DD. 020 3878 3955
hello@demos.co.uk, www.demos.co.uk

THE DEEPFAKE GAP: REGULATING FALSE STATEMENTS & AI TO SAFEGUARD ELECTIONS

A GUIDE TO THE LAW

Introduction

This briefing is designed to help UK lawmakers, policymakers, regulators, and policy experts consider how best the UK can safeguard its elections in the context of AI. It summarises the challenges the UK faces when it comes to addressing false and misleading claims about elections using existing UK law. We specifically focus on vulnerabilities associated with false statements, deepfakes, and related misleading AI-generated content about electoral candidates and MPs.

We explain what the current context is to this policy debate (Section 1), the law says (Section 2), what gaps and ambiguities there are (Section 3), the potential consequences of these issues (Section 4), and what can be done to overcome these challenges (Section 5).

We make five key asks to address the current gaps that leave our electoral systems vulnerable:

1. *For Government*: set out new legal guidance to clarify existing law
2. *For Ofcom and the Electoral Commission*: create new codes to address election risks
3. *For political parties*: establish shared principles on the use of AI in campaigning
4. *For Government & Parliament*: Introduce further legislation to address risks from AI
5. *For civil society & academia*: Conduct research to address the evidence gap

1. What is the context for the Representation of the People Bill, false statements, and deepfakes?

The UK Government introduced the Representation of the People Bill to Parliament on February 12th 2026. The Bill contains measures such as lowering the voting age to 16 and reforms to political donations. But, while the Government has previously acknowledged that "our own democracy is being threatened by misinformation", the Bill does not set out measures to address electoral mis- and disinformation, such as deepfakes of candidates and MPs. Nor does it address the role of digital platforms in spreading such content. This is a missed opportunity: the final Bill must go much further to safeguard our democratic processes from new and emergent threats. Moreover, the Bill's passage presents a window in which we can push forward on measures to build our democratic resilience.

By 'false statements', we specifically mean factual claims made about candidates running for elections which are provably incorrect. These statements could include, for example, false claims about the voting record of an MP standing for re-election or false allegations that a candidate has a criminal record. These claims are often defamatory in nature and may be intended to unfairly manipulate the result of an election. As we detail in this briefing, such false election-related statements are already addressed in various ways by UK law. This legislation sets a high threshold for claims to be identified as false statements, which generally involves proving that the person making the claim knew it to be false and shared it with the specific intent of affecting the outcome of an election.

We are not calling for restrictions to people's right to share political commentary and criticism about electoral candidates or MPs. The ability to make critical commentary about candidates is a fundamental part of the rights to freedom of expression and free elections, which are protected by the European Convention on Human Rights.

Meanwhile, there is no standardised definition of 'deepfakes'. For the purpose of this briefing, we use this term to refer to realistic AI-generated audiovisual content which reproduces a person's likeness. Deepfakes are typically created maliciously without the consent of the subject and often are made with the intent to deceive viewers into believing they are real. Deepfakes may be made to make it seem that a person said or did something they did not. In addition to deepfakes, we also discuss other false and misleading AI-generated audiovisual content that relates to candidates and MPs but which falls outside this definition. One example of this broader category of false AI content is AI-generated video which makes untrue claims about a candidate but which does not feature the candidate's likeness.

2. Which laws could protect MPs and candidates against the spread of false statements and deep fakes?

The UK already has legislation which in theory covers some situations where electoral candidates and MPs are targeted by false statements and deepfakes online. These laws primarily focus on the act of making, publishing, and sharing material which includes false claims about candidates and MPs. They may be interpreted as applying to false claims online, deepfakes and other false AI content about electoral candidates. But, as we discuss in Section 3, there are several gaps and ambiguities in these laws which have limited their application in practice.

The relevant laws are:

- Representation of the People Act (RPA) Section 106: Offence of false statements as to candidates.
- Elections Act (EA) Section 8: Offence of undue influence (amending RPA Section 114a)
- National Security Act (NSA) 2023 Section 13: Foreign Interference Offence
- Online Safety Act (OSA) Section 179: False communications offence.
- Online Safety Act (OSA) Schedules 5-7: Other relevant Priority Offences:
    - Non-consensual intimate image abuse
    - Hate speech
    - Harassment and abuse
    - Fraud

Next, we break down to what extent these laws relate to the following situations before explaining where we see gaps

- (1.1) False statements made about candidates and MPs
- (1.2) Deepfakes and AI generated content targeting candidates and MPs

2.1 What laws protect MPs and candidates against false statements?

There are several laws which feature criminal offences that could apply in situations where someone shares a false claim about a candidate or MP with the aim of interfering in an election: the Representation of the People Act (RPA), Elections Act (EA), the National Security Act (NSA), and the Online Safety Act (OSA).

Name of law	Type of law	Section(s)	Summary
Representation of the People Act (1983)	Elections law	S. 106	Prohibits making false statements about electoral candidates' character or conduct.

Elections Act (2022)	Elections law	S. 8	Amends RPA 1983 to criminalise use of intimidation or threatening behaviour to influence someone's vote illegitimately.
National Security Act (2023)	Security law	S. 13	Criminalises act of interfering in a political process in the UK to the benefit of a foreign power.
Online Safety Act (2023)	Online safety law	S. 179	Criminalises the act of knowingly spreading false information with the intent of causing "non-trivial psychological or physical harm to a likely audience".
		Schedules 5-7 (Priority Offences)	Sets out various offences that platforms must address as a priority. Some of these may apply to deepfakes and non-consensual AI content of candidates, depending on the circumstances.

However, these laws all lack the specificity to be used effectively in addressing false statements, deepfakes and related AI content. The RPA and EA's provisions are specific to elections, but don't explicitly address digital communications or deepfakes, while the OSA's false communications offence is more general and applies to all situations where someone shares a false message with the intent to cause physical or psychological harm to an audience.

Representation of the People Act (RPA) 1983 Section 106: False statements about candidates

Section 106 of the RPA (1983) makes it illegal for a person to "mak[e] or publis[h] any false statement of fact in relation to [an election] candidate's personal character or conduct" if this takes place "before or during an election" with the intent to affect "the return of any candidate at the election". It therefore is specific to false statements about personal character or behaviour, not their political views or activities.

If a person is found guilty of this offence, they may receive a court order to prevent them from repeating the falsehood. This offence does not apply if the person making the statement can prove they had "reasonable grounds for believing, and did believe, that statement to be true."

Section 106 should, in theory, apply to malicious false statements made about candidates' personal character and conduct on social media or in other online spaces. The RPA's false statements offence counts as a 'relevant non-priority offence' under the OSA, meaning that it is treated as part of digital services' overall obligations to mitigate the risk of illegal content appearing on their platforms. We explain this in more detail later in the briefing, as part of our discussion of ambiguities surrounding non-priority offences in the OSA.

Elections Act 2022 Section 8: Offence of undue influence

The EA 2022 amended the RPA to add the offence of 'undue influence': using intimidation or threatening behaviour to change how another person will vote, to prevent them from voting at all, or to otherwise prevent someone from freely exercising their right to vote. Prohibited activities include:

- Using or threatening violence
- Damaging or destroying property, or threatening to do so
- Damaging or threatening to damage a person's reputation
- Causing or threatening to cause financial loss to a person

A person can also be found guilty if they carry out one of these prohibited activities with the assumption that they have changed how another person has voted or stopped them from voting.

This law is designed to prohibit voter intimidation and falls under the legal definition of 'corrupt practices' during elections (RPA Section 114). If convicted for undue influence, a person may face a prison sentence of up to one year, a fine, or both. They will also be barred from being elected to the House of Commons or from holding any elective office.

The offence of undue influence would, in theory, apply to cases where someone spreads reputationally damaging claims or threats of violence online to influence how others will vote in an election. It affects both candidates - who may be subject to online smear campaigns - and the rights of voters to participate in a free and fair election.

In theory, Section 8 of the EA would count as a relevant non-priority offence under the OSA in cases where there is an individual victim, such as a specific voter (see below).

National Security Act (NSA) 2023 Section 13: The Foreign Interference Offence

Section 13 of the NSA makes it a criminal offence for a person to engage in "prohibited conduct" in a manner which interferes in a political process in the UK to the benefit of a foreign power, such as a foreign state, whether knowingly or through reckless behaviour. Relevant political processes include elections, referendums, local authority proceedings, and the proceedings of registered UK political parties. For the purposes of the offence, prohibited conduct includes "making a misrepresentation of fact which contributes to the interference effect, such as a misrepresentation as to a person's identity or purpose" or "presenting information in a way which amounts to a misrepresentation. The foreign interference offence is listed as a Priority Offence in Schedule 7 of the OSA.

The foreign interference offence would, in theory, apply where a person creates or shares a deepfake or similar AI-generated content which contains false information about an election candidate in a way which interferes with a UK election,but only where the foreign power condition is met. This requires proof that the false content was produced or shared with the intent of benefitting a foreign power, or where the defendant was reckless as to whether it would benefit one.

Online Safety Act (OSA) 2023 Section 179: The false communications offence.

The OSA makes it a criminal offence for a person to spread information they know is false with the intent of causing "non-trivial psychological or physical harm to a likely audience". This is known as the false communications offence.

The false communications offence has some overlaps with the RPA's prohibition on false statements about election candidates: both provisions cover situations where a person intentionally shares false information with the aim of harming another person. It may also overlap with the EA's undue influence offence in cases where someone intentionally tries to damage an election candidate's reputation. However, the false communications offence is not tailored to elections: it does not explicitly address the heightened risk that candidates and MPs face, nor does it address the impacts that election disinformation might have on democracy more broadly and the speed at which it would need to be tackled. And while it could cover them in theory, in practice the false communications offence is not tailored to addressing deepfakes or related AI content and was not designed for this specific purpose. Crucially, the False Communications Offence has not been applied in an elections context and its use for election-related deepfakes remains untested.[1]

2.2 What laws could protect MPs and candidates against deepfakes and AI generated content?

The laws we have discussed so far – the RPA's false statements offence, the EA's undue influence offence, the NSA's foreign interference offence, and the OSA's false communications offence – could also apply to cases where deepfakes or AI generated content about candidates and MPs are shared without their consent. Additionally, these situations may also be covered by other provisions in the OSA if they meet certain criteria.

Are deepfakes and AI content of candidates and MPs covered in the Online Safety Act?

[1] There were reports of several arrests under OSA S.179 in the summer of 2024 in relation to the Southport riots, which resulted in two convictions. These remain the most well-known instances of the False Communications Offence being applied.

Several of the OSA's Priority Offences apply to deepfakes and non-consensual AI content of candidates and MPs if these meet the offence's specific criteria, as set out in Schedules 5-7. Digital platforms are required to take pre-emptive steps to prevent these offences from taking place. These priority offences include:

- Non-consensual intimate image abuse
- Hate speech
- Harassment and abuse
- Fraud
- The foreign interference offence (derived from NSA Section 13)

The OSA is intended to be technologically neutral. This means that it should not matter whether a piece of content was generated by AI or produced manually: the key question is whether it meets the criteria to be considered harmful content.

For example, a deepfake video of an MP which involved racist or sexist abuse would be likely to count as hate speech. Similarly, if someone created and shared a sexually explicit deepfake or AI-generated video which involved an election candidate without their consent, this would count as non-consensual intimate image abuse (NCII). There have been real-world cases in neighbouring countries where politicians have been targeted with non-consensual, sexually explicit deepfakes. Based on the OSA's prohibition of NCII content, the UK government has announced a crackdown on sexually explicit deepfakes.

Meanwhile, sharing deepfakes or AI-generated content about candidates and MPs is illegal if it meets the criteria for the false communications offence. This means:

1) The content needs to state or imply a falsehood about a person, such as candidate or MP;
2) The person who shared has to be proven to be aware that the information was false;
3) The person who shared it has to intend to cause significant psychological or physical harm to the audience of the message or to the subject of the fake content.

During an election, the person or people harmed could be a candidate, MP, or a particular group of voters.

However, under the OSA, Ofcom does not have power to take down content itself. Responsibility for removing content that violates the OSA lies with platforms. Ofcom may conduct investigations and notify platforms of content violating the OSA that is in need of removal. This means that if content were to spread during an election which violated the OSA under the terms above, it is possible that it would not be taken down immediately, even if Ofcom was aware of it.

What about the RPA and EA?

As the Electoral Commission has noted, neither the RPA nor the EA address deepfakes or other AI content explicitly. Nor were they drafted with such content in mind. The RPA was originally enacted long before such technology existed.

3. What are the gaps, ambiguities, and challenges for applying these laws?

There are several gaps and areas of ambiguity which have made it difficult to identify when these laws apply or how they can be enforced. These problems involve:

- Gaps in the RPA, EA, and OSA
- The high bar set by requirements to prove intent and belief
- Ambiguities surrounding the status of relevant non-priority offences under the OSA

3.1 Challenges for applying the RPA Section 106

Both the Electoral Commission and the Director of Public Prosecutions have highlighted gaps in section 106 of the RPA. They recommend updating the provision to reflect digital campaigning and expressly cover deepfakes, to support consistent enforcement and improve understanding among campaigners. As the Electoral Commission writes, these changes are intended to "ensure that section 106 remains fit for purpose in the modern, digital era." In particular, they note that "while section 106 might be interpreted to cover the use of deepfakes (i.e. manipulated content) in an electoral context, this is not clear in the legislation." Police and prosecutors could be aided if it was made clear that "the scope of the offence does cover digitally manipulated false statements of fact about the personal character or conduct of a candidate."

Moreover, the Election Commission has noted that the specific wording of the law may create a challenge for enforcing the offence. Section 106 only applies to "false statement[s] of fact" about the "personal character or conduct" of a candidate. It therefore does not apply to false or misleading statements about a candidate's political views, conduct in office, or other significant subjects which may be the targets of election disinformation. The Commission has also noted that under Section 106, "misleading content about candidates is not considered an offence outside of the regulated [pre-election] period". Section 106 is "only enforceable during the regulated [pre-election] period", meaning that at present it cannot cover election-related cases such as the false deepfake of George Freeman MP. These gaps limit scope for which the offence can be used.

The Commission has recommended that the government should "conside[r] creating a clearer new overarching duty on platforms operating in the UK to cover a wider range of risks to elections, to ensure they take action to mitigate risks and protect legitimate political debate, particularly during critical election periods."

Meanwhile, the Director of Public Prosecution has highlighted barriers to prosecuting the offence, including the evidential challenges disproving the statutory defence that a person had "reasonable grounds for believing, and did believe, that statement to be true." During the 2024 General Election, UK police considered 90 alleged offences under section 106, but most cases led to no further action and no allegations resulted in a prosecution.

3.2 Challenges for applying the EA Section 8

There are similar challenges for applying the EA's undue influence in digital contexts. Like the RPA, Section 8 of the EA does not make it explicitly clear that it applies to manipulated content such as deepfakes and AI-generated material. Moreover, the undue influence offence applies only to cases where a voter or group of voters has faced intimidation or violence – not candidates and MPs.

3.3 Ambiguities surrounding non-priority offences in the OSA

Existing laws may count as 'relevant non-priority offences' under the OSA if they:

- Are not listed as priority offences in Schedules 5-7 of the OSA
- The offence's victim or intended victim is an individual or individuals
- The offence was created through the OSA, another Parliamentary Act, or another relevant statutory instrument.
- The offence does not concern intellectual property rights, the safety or quality of goods, or the performance of a service by an unqualified person.
- The offence is not an offence under the Consumer Protection from Unfair Trading Regulations 2008.

Based on the definition above, Section 108 of the RPA and Section 8 of the EA can be interpreted as being non-priority offences if it can be shown that there is an individual victim.

The OSA sets some requirements for platforms to address risks from harm from content that violates these non-priority offences. Platforms must assess the risk of harm from content which meets the criteria for a relevant non-priority offence if it appears on their service. While platforms do not need to assess the risk of every non-priority offence individually, Ofcom states that "if providers have evidence or reason to believe that other types of illegal harm that are not listed as priority offences in the Act are likely to occur on a service, then they will need to consider those in the risk assessment."

However, Ofcom has not given guidance on the RPA or EA offences in its Codes of Practice. The Codes are not intended to identify or address all relevant offences under the OSA. Ofcom has generally focused its guidance on the priority offences and has signalled that services should focus on these. The Codes also include general rules which apply to all offences, including non-priority ones.

Because there is no OSA guidance from Ofcom which addresses the RPA and EA specifically, platforms are less likely to take action on undue influence and false statements about candidates or MPs.This is because the OSA states that following Ofcom's Codes of Practice guidance is enough for a service to be considered to be compliant. As a result, platforms may do the legal bare minimum by only taking action on non-priority offences that are explicitly mentioned by Ofcom's Codes. Therefore, further guidance is needed from Ofcom or the government to push platforms to take action on undue influence and false statements.

3.4 Gaps in the OSA False Communications Offence

As identified in Demos' Epistemic Security report, there are several significant gaps in the OSA's false communications offence. Firstly, the offence is the OSA's primary mechanism for addressing the spread of disinformation, yet is focused on prosecuting individuals. The provision does not address the role of services' systems in incentivising or promoting false information and does not place proactive duties on platforms to mitigate the spread of false material. Moreover, the offence does not explicitly include deepfakes and other AI-generated content. Finally, the need to prove that a person intended to cause harm may set a high bar for proof - especially in cases where the communication is shared with a group or on a general feed on social media.

3.5 Consequences for a timely response to election information incidents

In today's information environment, false claims and deepfakes about election candidates can spread online near-instantaneously. For example, a deepfake of Irish Presidential candidate Catherine Connolly was published just days before voters were due to go to the polls and went viral immediately. In the UK, pre-election periods can vary, but are typically relatively short – taking between 15 and 25 days. This means that time is of the essence for any action on deepfakes or widespread false claims about candidates.

Addressing the gaps and ambiguities we have identified in legislation may help to ensure that timely action is taken on legal proceedings, such as the application of an injunction to prevent further false claims being circulated. But, given the nuance and complexity of cases involving allegations of false claims about candidates, it may be that these changes do not speed up the legal process to the extent that they are completed within the pre-election period.

Therefore, in addition to legal avenues, the Government should consider other non-judicial mechanisms which can be used to help address information incidents in a timely manner during election windows. These measures could help to mitigate the spread of false and misleading claims about candidates and MPs in the immediate period that they spread, alongside legal proceedings that may take longer to come to fruition. As we detail in our briefing on the Elections Bill, these measures could include the Government triggering a publicly-available election crisis response procedure and regulatory requirements for digital services to implement election-specific crisis protocols. More systemic mitigations could include regulations which require platforms to label AI generated content as such and tighter rules for social media recommendation algorithms.

4. How are false statements different from legitimate criticism of MPs and candidates?

The provisions described above for false statements and deep fakes are not intended to prevent citizens from sharing legitimate political commentary and criticism about electoral candidates or MPs. The ability to make critical commentary about candidates is a fundamental part of the rights to freedom of expression and free elections, which are protected by Article 10 of the European Convention on Human Rights (ECHR). Under the ECHR, the right to freedom of expression does not extend to false statements made dishonestly.

The RPA and EA specifically target cases where people intentionally spread claims which they know are probably false with the express aim of harming an election candidate or manipulating voters. This means that these laws are narrowly defined so as to avoid infringing on the right of voters and candidates to freely participate in elections. Where the RPA and EA are applied in contexts that involve a restriction on free speech rights, this use must be shown to be proportionate and justified under human rights law. Courts must weigh the accused's right to freedom of expression under Article 10 of the ECHR against the candidate's right to the protection of their reputation under Article 8 (the right to private and family life). As the Electoral Commission has noted, the RPA's false statements offence is not intended to silence legitimate complaints or criticism about a candidate's political views.

Additionally, the Crown Prosecution Service applies a 'public interest test' to determine whether to pursue election offence cases. This requires prosecutors to establish whether that offence was not committed as a result of a genuine mistake and had a material influence on the result of the election process, among other considerations. The public interest test sets a further requirement to ensure that legitimate political activity is not wrongly prosecuted.

We are not advocating for restrictions on legitimate political speech or criticism of electoral candidates during elections. Instead, we are calling for clarity about how these existing laws apply to digital contexts and AI-generated content.

5. What can be done?

In addition to the recommendations for the Elections Bill that we set out in the Information Crisis Coalition's Elections Bill briefing, we have identified five critical measures to help address these challenges and safeguard the integrity of our elections. These recommendations are primarily non-legislative and are directed towards the Government, Ofcom, the Electoral Commission, political parties, academia, and civil society.

Our five recommendations are:

1. *For Government*: set out new legal guidance to clarify existing law
2. *For Ofcom and the Electoral Commission*: create new codes to address election risks
3. *For political parties*: establish shared principles on the use of AI in campaigning
4. *For Government & Parliament*: Introduce further legislation to address risks from AI
5. *For civil society & academia*: Conduct research to address the evidence gap

5.1 New guidance

The Government should produce new legal guidance to clarify the status of the RPA and EA when it comes to online disinformation, deepfakes, and AI-generated content of candidates and MPs. This guidance should specify how this existing legislation applies to false and manipulated online content that targets election candidates and MPs, as well as deepfakes and other synthetic media.

New guidance will help encourage more consistency in how the law is applied and reduce the risk of misinterpretations. It is vital for there to be more fairness and consistency in how these offences are interpreted and prosecuted. By identifying how these laws relate to digital services, new guidance may also be a useful way of ensuring that platforms take appropriate action. We have set out what this guidance should look like in detail in our briefing on the Elections Bill.

5.2 New Codes from Ofcom and the Electoral Commission

There are additional steps that Ofcom and the Electoral Commission should take to promote action and best practices.

For Ofcom: set out an Elections Code of Practice

Ofcom should set out an OSA Code of Practice describing measures for platforms to reduce harms against candidates and MPs. In collaboration with Demos and other partners, the OSA Network has published a draft Code for Ofcom to adopt. The draft Code includes requirements for platforms to provide high-quality support lines to candidates, more tools for candidates to block and report harmful content, and adjustments to platforms' terms of service to reflect election harms.

For the Electoral Commission: create a new Elections Code of Conduct

The Electoral Commission should establish an Elections Code of Conduct to set standards for campaigning, as recommended by the Speaker's Conference on the security of candidates, MPs and election. This should include a prohibition on the use of deepfakes for campaigning.

5.3. Principles on the use of generative AI for political campaigning

Major political parties should agree on a set of principles for the use of generative AI during election campaigns. As Demos and partners advocated for ahead of the 2024 election, this agreement should include requirements to:

1. Not use generative AI tools to produce misleading audio or visual content, such as deepfakes of candidates and MPs;
2. Clearly label where generative AI is used to produce audio or visual content in a non-trivial way;
3. Not amplify misleading AI-generated content;
4. If misleading AI-generated content poses a significant risk, act responsibly by calling out such content in such a way that does not contribute toward further amplifying it;
5. Ensure party staff, members, volunteers and supporters are given clear guidelines for the use of generative AI in election campaigning.

5.4. Broader regulation to address AI risks

There are additional regulatory steps which could help to address risks that deepfakes and false or misleading AI content pose to our information environments. As Demos identified in our report on epistemic security for crisis resilience, the societal risks of audiovisual AI content include threats to election integrity but extend far beyond them. Broader measures to address broader AI risks to information integrity would therefore be useful for addressing epistemic threats both during and outside election contexts.

Yet, outside of the specific contexts addressed by the OSA that we have discussed in this briefing, AI systems remain under-regulated. It is therefore necessary to introduce new AI-specific legislation and regulations. These should include:

- Regulation which requires AI services to watermark AI-generated content.
- Broader regulation of AI content generation tools, such as regulation on likeness rights.

5.5 Address the evidence gap

While there have been several highly-alarming incidents, such as the deepfake of George Freeman MP that emerged in October 2025, there remains an evidence gap.

Specifically, new research is needed to identify:

- The number of candidates and MPs affected by false statements online, deepfakes, and related AI content.
- The types of false and misleading content being shared.
- The number of people engaging with such content i.e. viewing it, commenting on it and resharing it.
- How such content was treated by digital platforms' moderation systems i.e. if it was removed or de-ranked, and/ or boosted.
- The effects of such content on candidates, MPs and their staff
- The effects of such content on citizens and their voter behaviour i.e. electoral outcomes.

This evidence is needed to demonstrate the scale of the challenge represented by false statements and deep fakes during an election period and to help pinpoint solutions. Without further evidence, it may be difficult to build momentum for legislation and to gain buy-in for mitigation measures.

Such research could be conducted by civil society and academia. It would benefit greatly from enhanced access to digital platforms' data on their services. Elsewhere, we have called on the Government and Ofcom to use powers set out in the Data Use and Access Bill (2025) and the Online Safety Act to compel platforms to provide public interest researchers with access to such data.

To help address this evidence gap, Demos is gathering testimonies from MPs and electoral candidates about their experiences. We will use this to shape our policy recommendations and advocacy ahead of the passage of the Elections Bill. If you are an MP, candidate or a member of their team, and have an example of a false statement or deep fake about an MP or electoral candidate, please do share this with us confidentially to: deepfakes@demos.co.uk.

Further reading

Through the Epistemic Security Network (ESN), Demos is undertaking research and convening leading thinkers to tackle threats to the UK's *epistemic security*: the resilience of the UK's information supply chains that our democracy depends on. Within the ESN, Demos convenes the Information Crisis Coalition to work on strengthening resilience to information crises, including during election periods.

This briefing is meant to be read alongside the Information Crisis Coalition's Elections Bill briefing, which sets out our overall recommendations for what should be added to the Representation of the People Bill.

Demos' other publications on Epistemic Security include:

- Epistemic Security 2029 (Feb 2025) - Fortifying the UK's information supply chain to tackle the democratic emergency
- Epistemic Security for Crisis Resilience (Jan 2026) - An analysis of information threats, vulnerabilities, and priority interventions for the maintenance of effective crisis response capacity in democratic societies
- Epistemic Security: Our BBC (Jan 2026) - A blueprint for a more independent and future-proofed BBC