

# Action Plan: Defend Democracy from Digital Threats

## Find out more

To develop an Action Plan,  
contact us: Ben Scott  
[bscott@luminategroup.com](mailto:bscott@luminategroup.com)

The Digital Democracy Charter is a starting point to align public, private and civic sector stakeholders around shared principles of reform. But that will only matter if we translate it into actions that make change. Because every country faces its own unique combination of challenges with technology and democracy, we must focus on national action plans to craft and implement new policies that harness the power of technology to democratic goals. Plans, insights, and learnings can be coordinated across borders in an “agile multilateralism” even as nations forge ahead with domestic reform agendas.

There are no single-solutions that can meaningfully address digital threats to democracy. Only a combination of policies – all of which are necessary and none of which are sufficient by themselves – will begin to show results over time. We can start immediately with a first phase of actions by treating the worst of the symptoms. That means increasing cyber-security against foreign interference, increasing transparency in political advertising, and combating online hate speech and fraud. Dealing with these urgent issues will lead us to a second phase – addressing root causes. These are the structural tensions between technology and democracy at the center of the data economy and the digital information marketplace. We must establish a data “bill of rights”, modernize competition policy, and make long term investments in digital literacy and public service journalism.

## Rapid Response: Digital disinformation in our democracy manipulates political viewpoint, divides our society, weakens the integrity of public debate, normalizes extremism and distorts electoral outcomes.

The top priority of the Action Plan is to address immediate symptoms of the exploitation of information markets. First, it is a national security priority to shut down organized disinformation operations that come from foreign agents. Second, it is a clear matter of democratic integrity to mandate transparency for all paid political advertising. And third, it is imperative of public safety and consumer protection to give citizens confidence that illegal activity online will not be tolerated – from cyber-attacks and data breaches to hate speech, harassment, and fraud.

### Security

We will protect the integrity of our elections from the cyber-attacks and disinformation campaigns of foreign actors and criminal enterprise.

- **Cyber-security for Democracy:** Electoral institutions – such as parties, campaigns and election administration – will meet the same standard of cyber-security protection that we use for critical infrastructure like the electricity grid and the water system.
- **Research:** Universities, security firms, and government agencies should collaborate in a transparent program to monitor, track and expose organized disinformation operations.
- **Market Regulation:** Companies will be required to take all reasonable measures to protect sensitive data and prevent the abuse of digital media by foreign actors.

### Transparency

We will protect the right of citizens to know who is trying to influence their political views and how they are doing it. New regulations will curb the amplification of false narratives through the opaque channels of targeted digital advertising, organized political spam, and automated networks of social media accounts.

- **Political Ad Disclosure:** All online political ads must be made available in a searchable database and all political advertisers must be verified as legal. Each ad must disclose in real time to the consumer the source of the ad, the true source of the funding behind it, and all of the targeting criteria that brought the ad to a specific individual.

- **Countering Political Spam:** All digital media accounts that exhibit behaviors of automation or high-frequency spam should be clearly labelled as a default setting.

### Consumer protection

We will protect the public from illegal content. We will apply adaptive, transparent regulations to remove types of content that are already illegal in our democracy – such as hate speech and incitement to violence. We will develop new systems that leverage corporate technologies to find and remove illegal content with the supervision of regular judicial review and a transparent process, including a fast-track appeals process. Because of the risk of infringements on legitimate speech, this practice will be strictly limited.

## At the root of the digital democracy crisis is the powerful business model of platform monopolies.

First, they leverage the vast quantity of behavioral data they collect through surveillance of billions of Internet users to rent advertisers access to the attention of highly targeted audiences. Then they use sophisticated artificial intelligence (AI) to customize content on digital media to maximize the amount of time people are online and available to see ads. Of course, in exchange for watching ads, they offer people popular products and services that have contributed great value to social life. But they have been blind to the fact that this business model serves as an ideal vector for manipulative publishers and advertisers (including covert agents of foreign powers) to find audiences for every type of prejudice. Fragmentation, polarization, propaganda, and manipulation in the news media are accelerated by the logic of modern information markets. So too is the decline of traditional newsrooms and the erosion of credible public service journalism.

We now stand at an inflection point. We must design an ambitious public policy response to steer technological development back towards serving the wellbeing of democratic society. We cannot allow our society to be held hostage to a marketplace that undermines the integrity of our democracy. We must address the root causes with a structural policy agenda that focuses on data rights, competition, education, and public service.

### Data rights

We will establish and enforce rules that give individuals control over how data about them is collected, used, and monetized. The rules must be flexible to adapt to technology change and directly address the connection between data profiling, content targeting, and polarizing media audiences. These targeted data policies that address disinformation fit within a broader agenda of data rights that are foundational for the modern economy.

- **Restrictions on Sensitive Data:** To constrain the profiling of political viewpoint, users should be provided additional protections (collection and use restrictions) for any sensitive data, including that which may be used to reveal a political preference or to manipulate a political viewpoint.
- **Consent and Control:** To prevent all-or-nothing privacy policies that deny service to any user that declines to opt-in to certain types of data collection or use, platforms should be prohibited from discriminating against users that choose privacy. For those that do consent, these consequences of these agreements must be meaningful and understandable to any user.
- **Child Online Safety:** Additional restrictions in data collection, data use, and certain forms of targeted communications should be applied for vulnerable user groups, especially children under the age of 18.
- **Data Portability & Interoperability:** In a market that offers limited consumer choice and high barriers to competitive entry, we need policies enabling portability and interoperability of data across services.

### Competition

We will protect the public against the exploitation of concentrated market power. Especially in information markets that sustain our democracy, consumers should have meaningful choices to find, send and receive information over digital media.

- **Modernization of Antitrust:** We need new forms of antitrust oversight for the digital economy that look not just at price increases to judge market power but also at control over data, constraints on innovation, and reduction in consumer welfare.
- **Concentration Restrictions:** The rapid concentration of power in the digital market is driven by mergers between large companies and acquisitions of upstart competitors. Oversight of commercial mergers should consider not only horizontal market power but also the acquisition of data and patents that enable competitive advantage.

### Algorithmic accountability

We will develop new forms of public oversight that apply a duty of care and regular auditing to the technologies that control information markets. The algorithms that mine large data sets, target advertising, and curate digital media feeds are increasingly forms of AI. These technologies have the potential for enormous social impact – positive and negative – and should be subject to government oversight, including a review of training data, design bias and discriminatory outcomes. These audits should mirror health and safety inspections of traditional industries.

### Public service journalism

We will restore and strengthen public service journalism as a cornerstone of democracy. The rise of disinformation as a disruptive phenomenon coincides with the decline in commercial viability for public service journalism in the Internet age. The accumulation of market power over content aggregation and digital advertising in search and social media has hastened these changes. But even as the number of professional journalists drops, the public's need for their services has surged. What the market fails to provide, society must build for itself with public policies. These might include support for the modernization of public media channels, wage-tax credits for professional journalists that are technology and viewpoint neutral, investments in student journalism to build a career pipeline, or a program of citizen vouchers to put the power to restore journalism in the hands of the people.

### Education

We will support and strengthen digital media literacy. The fight against disinformation in democracies will be won by changing public attitudes and the ways people consume digital media. The rise of digital media giants has weakened traditional markers of source credibility by compressing every news headline into a single stream and eroding a shared public narrative of facts in pursuit of greater ad sales. As a society, we need to establish digital media literacy skills in our educational curricula. We will begin by working with civil society groups to generate broad public awareness about the problem of disinformation. And we will fund programs to deliver digital literacy in our schools to the next generation of voters.