Reframing the fake news debate: influence operations, targeting-and-convincing infrastructure and exploitation of personal data

Among the debates following the 2016 US presidential elections, the debate around fake news has been among the most intense - as well as perhaps the most poorly framed. Indeed, focusing on which news are fake and which aren’t has yielded solutions relying on cooperation between journalists and global platforms: the main outcome has been to enable users to flag content on Facebook as “disputed” so that other users know to exert healthy skepticism - an unsatisfactory answer at best to the issues at hand.

Indeed, this approach fails to consider three deeper reasons why fake news matter, that the international community should urgently begin addressing. First, fake news matter when we manage to show that they influence voting decisions. Second, targeting-and-convincing infrastructures\(^1\) can be used by foreign actors in influence operations. Third, the ability to collect, centralize and share personal data on an unprecedented scale vastly increases the efficiency of such operations.

Fake news matter not because they are fake but because they influence voting decisions
Fake news are not new: grassroots organizations or political campaigns have long used and spread rumours against their opponents. They only received such an emphasis after this election because some argued they tilted the election in favor of Donald Trump. In other words, what matters is not the fake news *per se*, but the influence - undue, in the minds of its critics - they had on people’s voting decisions.

A persistent narrative claims that a British company called Cambridge Analytica relied on personal data to craft personalized messages relying on psychometric data which would have made Trump’s campaign vastly more efficient\(^2\). While of course this causal link between psychometric data and voting decisions is not backed by evidence yet - more recent articles have debunked some of the original theories\(^3\) -, one does not need to think very hard to understand that more granular voter data (that Cambridge Analytica boasts being able to provide) leads to more elaborate and efficient campaigning.

Fake news matter therefore not because they exist, but because of the (alleged) influence operation that they belong to: that a company (Facebook, or Cambridge Analytica) or a foreign power (Russia, according to the intelligence community report released in January\(^4\)) would be able to tilt an election is a form of influence that we should not accept on democratic elections - in the same way we regulate media behavior during electoral periods to avoid undue influence. Academic research should therefore be directed to new questions questioning the actual extent of that influence, such as: what is the actual influence of fake news on voters’ decision-making processes? Should global platforms be regulated differently than traditional media in electoral processes on this basis? Can the US both protect its voters from undue influence from foreign organizations while promoting a global free flow of information?

Targeting-and-convincing infrastructures: new technical underpinnings of the digital public sphere

---

4. “Assessing Russian Activities and Intentions in Recent US Elections,” ODNI National Intelligence Council, Jan. 6, 2017
The underlying problem is that companies like Facebook and Twitter have built targeting-and-convincing infrastructures\(^5\) enabling foreign actors to wage influence operations.

The business model of global platforms relies on advertising. Online ads are more efficient than offline ones because of the increased ability to target your audience in a granular way. This system of incentives has led the adtech ecosystem to develop particularly efficient targeting-and-convincing infrastructures: infrastructures built to target the right people and deliver the right content at the right time - in other words, to increase the efficiency of an influence operation, for commercial purposes (e.g. marketing) or others.

The exploitation of such targeting-and-convincing infrastructures for non-commercial motives is becoming a security threat, not only because it might affect elections but also because of the threat of online radicalization. Indeed, the ability to ensure the integrity of an electoral process should be a matter of national security - in January, the Obama administration designated election systems as critical infrastructure\(^6\). Other scenarios could leverage such infrastructure against national security, for instance using Facebook to find those most likely to be convinced to wage terror attacks against their own country.

We should regulate targeting-and-convincing infrastructures - urgently, since Facebook announced it aimed to become a major technical underpinning of the digital public sphere\(^7\). Such regulation might include: separation of commercial advertising and political advertising at a technical level, or increased transparency and accountability to users on how algorithms personalize their feeds.

**Personal data matter because it further increases the efficiency of such influence operations**

Personal data is the fuel on which targeting-and-convincing infrastructures run. Targeting-and-convincing infrastructures rely on privately-held databases of personal information. More personal data seems to lead to increased ability to personalize the message and its delivery for optimal influence. Beyond its benefits in terms of privacy, data protection decreases the efficiency of targeting-and-convincing infrastructures and protects the integrity of citizens’ decision-making processes. We should start researching and advocating for global interoperable data protection mechanisms because from a data-centric perspective, privacy and security are mutually reinforcing. Indeed, data protection protects both privacy and security.

Furthermore, such infrastructures rely on the exploitation of personal data on a scale that is unprecedented in human history. On a more fundamental level, the incentive system in which these infrastructures have been created has been described as “surveillance capitalism:\(^8\)” a “systemic coherent new logic of accumulation”\(^9\) of personal data in the hands of a few global platforms. Addressing the security issues raised by targeting-and-convincing infrastructures requires States to start exploring ways in which they can change this incentive system. Possibilities include, again, comprehensive data protection frameworks, as well as taxes on the collection of personal data, seen as a form of “digital labor.”

---


\(^6\) “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector”, DHS, Jan. 6, 2017

\(^7\) “Building Global Community,” Mark Zuckerberg, Facebook, Feb. 16, 2017

\(^8\) “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” Shoshana Zuboff, SSRN, April 2015

\(^9\) ibid.