# IDENTIFY YOURSELF

**Stephen Ufford** *reveals how issues such as fake news and state-sponsored meddling in elections has made digital identity the key to the continued success of democracy*

**With the election season ramping up in the US, American citizens have been bombarded with warnings that the process might be hacked by adversaries from overseas or extremists at home. This follows a string of cases globally in which democratic electoral processes have been the subject of tampering and infiltration.**

The first major security issue involving Presidential election campaigns was in 2017, when French President Emmanuel Macron was targeted by a 'massive and coordinated' cyberattack. Late last year, the UK Labour Party was subject to two separate distributed denial of service (DDoS) attacks. Both were designed to flood a computer server with traffic to try to take it offline. The issue is now so apparent that it is being addressed head on. Speaking at a rally ahead of his campaign last month, Democratic Presidential hopeful Bernie Sanders condemned Russia for its reported attempts to help his campaign, telling it to: "Stay out of American elections".

ONLINE VERIFICATION CAN BE USED TO PREVENT THE CREATION OF SYNTHETIC ACCOUNTS OR BOTS

In the wake of such vociferous and frequent hacks and data leaks, it is only natural to wonder whether the fate of democracy is today more in the hands of the hackers than it is the people. Now, the question is: will democratic elections no longer be immune to cyberattacks?

The reality is that elections are becoming a target for interference and sabotage, from both state-led or state-sponsored actors and terrorist or criminal organisations and individuals. Around the world – from American elections to Brexit – foreign influencers, trolls and bots are doing their level best to interfere with and impact the results of political campaigns.

Nowhere is this influence more pervasive and dangerous than on social media platforms. As citizens increasingly turn to online sources for their news and content, we've seen firsthand these platforms become popular targets for disinformation campaigns orchestrated by bad actors seeking to influence elections across the world.

For instance, Donald Trump has flourished in the social media age. But he didn't do it alone. Project Alamo was an arm of Trump's 2016 Presidential election campaign, of which Cambridge Analytica's staff were a part. It used data on more than 200-million American citizens to target potential donors and voters, aiming to influence various universes – their term for groups of people. Project Alamo created a variety of adverts, each designed to appeal to a different universe, spending $85-million in the process. At the same time, this massive proliferation in volume of social content served as a veil for criminals and nefarious online activity to up the ante. The net result: it was extremely difficult for voters to distinguish between legitimate content and sources (including news and ads) on social media and the fake news being distributed by rogue agents.

With the future of democracy increasingly under threat, it's not surprising that this is having a profound impact on citizen's faith in political institutions and causing them to question the legitimacy of today's political leaders.

However, despite a widespread belief that more needs to be done to protect the integrity of democratic elections in a digital-first world, those stakeholders involved, including governments, electoral commissions and social media platforms, have a significant challenge on their hands. Put simply, there are two main threats to our democracy that have emerged as political campaigning and communication have shifted towards digital channels.

Firstly, there is clear evidence that bad actors are using social media platforms to share false information far and wide. With the advent of social media, many people assumed that a huge global increase in connectivity would be good for democracy. As these platforms have aged, however, optimism has faded and the list of known or suspected harms has grown. Unlike within mainstream media, organisations and individuals misusing social media will continue to take advantage of the anonymity they can maintain online. They have been able to take out paid advertising and disseminate messaging, often without any real analysis of its credibility and truth, and within hours distribute lies and unfounded claims that are not only seen but believed by millions of voters, leaving electoral bodies and government agencies playing catch up.

Secondly, and arguably even more worrying, is the evidence of foreign interference in domestic elections, where foreign governments or state-sponsored groups have created thousands of synthetic social media accounts to espouse a particular point of view, promoting one candidate or party and launching vitriolic attacks on the opposition. The most notorious example of this was the US Presidential election in 2016 when the Internet Research Agency, a 'troll farm' based in Saint Petersburg, distributed and promoted fabricated articles and disinformation from Russian Government-controlled media over a four-year period.

**The future of digital identity will require some kind of identity custodian that maintains a verified connection between a physical and digital self**

The extent of the impact that a so-called 'bot army' can have on the results of an election is still to be determined, but there can be little doubt that they have a direct influence on voter behaviour at the ballot box.

In order to avoid the controversies that have plagued so many recent elections across the world, we are now seeing a concerted and coordinated effort from all of the stakeholders involved. This is a global challenge that requires a global response. Indeed, there is a recognition across the board that the most effective way to tackle this attack on democratic values is to reduce the level of anonymity that individuals and organisations are currently afforded online. This anonymity extends from paying for high-profile advertising campaigns online through to leaving provocative comments at the bottom of articles on online news sites.

Reducing anonymity essentially means putting identity at the heart of all digital and social media activity and engagement, so every single social media account that is created can be linked back to a web carbon version of an individual or organisation. The technology is available nowadays to verify the identity of online users and advertisers, wherever they are in the world, and this verification can prevent the creation of synthetic accounts or bots, which are capable of causing so much harm to our political processes and our faith in democracy. In fact, it's now possible to deprive trolls of their anonymity.

▶

Picture credit: Getty

Fortunately, it would appear that social media platforms are finally starting to take their role and responsibilities within political campaigning seriously and are making huge progress in this regard. Some are already making identity central to their political advertising strategies and policies going forward, and this is having a profoundly positive impact on the authenticity and validity of political messaging on these platforms. Other social networks are set to follow.

> BAD ACTORS ARE USING SOCIAL MEDIA TO SHARE FALSE INFORMATION AND FAKE NEWS FAR AND WIDE

Additionally, there is increasing pressure to ensure that those directly involved in campaign processes are undertaking tighter scrutiny and monitoring of political advertising online. In the same way that advertising is regulated on traditional channels such as TV and print media, with a focus on facts and evidence to support campaign messaging, there are now moves to replicate this regulation across social media advertising. These initiatives will help to root out and expose fake news and to identify those responsible so that they are properly penalised and unable to advertise in the future.

The future of digital identity will require some kind of identity custodian that maintains a verified connection between a physical and digital self, ensures that no data is used without consent, monitors malicious behaviour and provides user support in case of a lost key. Nonetheless, this is far from an easy solution and should be provided by a regulated entity.

## TAKING BACK CONTROL

While some may argue that this type of regulation goes against the whole ethos of the world wide web being a place of freedom and accessibility, social media platforms and governments must ensure that there are formulated strategies to counter fake news and bot armies. Fortunately, they now have at their disposal sophisticated technology and identity verification platforms that can protect free speech while at the same time make elections safer.

There is too much at stake when it comes to our digital identities to ignore what is going on, as shown numerous times through both data breaches where our personal data is compromised and manipulation of public opinion through social media. No matter which technology or appointed custodian we deploy to solve this, our identities should belong to us, the people, rather than one corporation or consortium of corporations that seek to exploit data for profit.

Ultimately though, the current trend line of fake news and misused information has to stop. Today's digital citizens doubt the validity of the information and data they are being fed online, therefore becoming increasingly sceptical about the integrity of elections as a whole. Social media platforms and governments should continue to collaborate and innovate to reverse this issue, using identity verification and technology as a means to create safer, more transparent and ultimately more engaged democracies ●

**Stephen Ufford** CEO and Founder of Trulioo has launched and successfully sold several data-focused startups during his career. In 2011, he launched his fourth startup, Trulioo, to help build a layer of trust and safety online, and with the mission to provide access to financial services to the billions of unbanked individuals around the globe.

Cambridge Analytica
The Power of Big Data and Psychographics in the Electoral Process
CONCORDIA

**CEO of Cambridge Analytica Alexander Nix reveals how big data can be used to influence elections**

Picture credit: Getty