he Impact of Digital Technology Upon Democracy



Author Jillian C. York

By Jillian C. York

Introduction

In the nearly three decades since the invention of the World Wide Web by Sir Tim Berners-Lee, we have witnessed dramatic changes to democracy around the world, many of which were assisted by digital technologies. At the same time, the increasingly rapid innovation in Silicon Valley, China, and elsewhere has led us to a point in which governments and publics alike are struggling to keep up with the development of new technologies, leading to potential threats to the existing world order.

Digital technology — be it the Internet, digital assistants such as Alexa, or the artificial intelligence (AI) powering self-driving cars and other automated tools — has the potential to shape the way we view the world and interact with one another. It can facilitate freedom of expression and access to information, bring about revolution, and transform our economies — but as we've seen more recently, it can also enable the spread of populism and misinformation, and be used by state or non-state actors to manipulate publics.

There is a tendency amongst both experts and lay commentators alike to ascribe solely negative or positive attributes to digital technology, resulting in a false binary of "good" or "bad". Indeed, although most technology is not inherently neutral — that is, it can be imbued with the values and biases of those who create it — it can be used in ways that are detrimental or beneficial, sometimes by the same actors.

This paper will explore the ways in which digital technology — particularly the Internet — has influenced global society, and in particular, the impact that it is having on democracy and democratic participation.

The Internet & Elections

The Internet was initially developed to make communication between researchers and labs across disparate geographic areas more convenient. The invention of the World Wide Web enabled access to the network by 1991, and just four years later around 16 million people worldwide were online.

Web usage spread rapidly and by the year 2000 there were 400 million users globally, according to data from the International Telecommunications Union. The Internet as a tool for politics and democracy promotion was still nascent, but in 2004 US presidential candidate Howard Dean's campaign became the first to make

significant use of the web for fundraising and campaign promotion.

The keys to Dean's success were a digital-savvy, agile staff, and a core of passionate supporters, many of whom were bloggers. Although his main online presence, a group on Meetup.com, had only 3,000 members, a 2004 *WIRED* magazine editorial commented that "3,000 passionate supporters who are connected via the Internet are influential in a way that an equivalent crowd would never be if you had to gather it via direct mail or a telephone survey."

Dean lost the election, but his legacy as "the web's candidate" was secured — and his fundraising success ensured that the web would begin to play a major role in politics in the United States and elsewhere. At the same time, the potential that Dean's campaign exposed would alert less democratically-inclined governments to the threat the web posed to their survival.

A Game of Cat & Mouse

In 2004, the same year that Dean unearthed the potential of the web for political campaigns, the president of the Maldives, Maumoon Abdul Gayoom, was discovering its perils. When unplanned protests rocked the capital of Malé, with protestors demanding the release of political prisoners (including the dissident writers of an e-mail newsletter) and Gayoom's resignation, the president cut off the country's access to the Internet entirely, in order to prevent information about the protests from reaching the rest of the world.

Gayoom's decision would have lasting repercussions. Just three years later, unrest in Myanmar's capital of Yangon led to full-scale demonstrations that would later be referred to as the Saffron Revolution. In response to the growing protests, the government attempted to block access to any websites or services that could be used to publish information about the protests, but web-savvy activists were able to circumvent the blocks and began sharing images and videos of the situation on the ground. In the absence of international media, these images were the only ones to reach the rest of the world.

The government, following Gayoom's lead, cut off Internet access, resulting in a global outcry — and global online action. Bloggers and groups on social networks such as Facebook urged online and offline actions, including street demonstrations, in support of the country's protesters. "The marches," wrote Sarah Lai Stirland in an October 2007 piece for *WIRED*, "organized at a lightning pace by volunteers using Facebook, show the increasing power and reach of a social-



Citizens of Myanmar demonstrate against the government during the 2007 Saffron revolution.

networking site originally designed to help college students find drinking buddies."

In the Middle East, activists were connecting across borders through online platforms. Tunisian exiles connected with their counterparts back home, resulting in innovative tactics to expose the corruption of the ruling Ben Ali family. In one instance, activists exposed first lady Leila Trabulsi's use of the presidential airplane for private shopping trips in Paris by comparing the government's official travel schedule with photographs posted to websites tracking air travel.

Similarly, for Palestinians — separated by borders and identification documents — the Internet became a means of not only connecting families but also re-building national communities separated by occupation and war. As Miriyam Aouragh wrote in her 2011 book Palestine Online: Transnationalism, the Internet and the Construction of Identity, the result of Internet technology is that "the nation state is no longer a privileged space for the imagination of identity" and that the Internet enables a form of "long-distance nationalism".

Throughout the world, governments began cracking down on Internet usage, through the establishment of laws as well as through extralegal or extrajudicial blocking and filtering of online content. Their targets varied — Turkey, for example, was interested in preventing criticism of the government, while Pakistan's blocks were largely aimed at content deemed insulting to Islam, and China's captured wide swaths of information — but their methods were by and large the same.

The Internet Rises Up

By 2010, there were nearly 2 billion Internet users worldwide, and smartphones had entered the market, bringing the web to the pockets of many who could otherwise not afford a connected device. In Tunisia, which was among the first countries to offer public Internet access (in 1996), penetration was close to 40%, and Tunisians had found the web offered more access to information and freedom of expression than government-restricted traditional media.

In the preceding few years, Tunisia's government had increasingly begun to crack down on the web, blocking numerous news and political websites. In 2008, a brief ban on Facebook led to a lawsuit and street protests, and the government quickly reversed its decision at the request of President Zine El Abidine Ben Ali. Despite the knowledge of what their government was capable of, Tunisians took to the Internet to debate politics and engage in social activism. including a campaign against Internet censorship.

In late 2010, protests broke out in Sidi Bouzid and, owing in large part to the spread of information on Facebook and blogs, quickly spread to Tunis and other parts of the country, resulting eventually in the resignation of Ben Ali. In his final, televised speech, he promised various reforms, including the end to Internet censorship in the country.

The success of the Tunisian uprising led to a flurry of demonstrations throughout the Middle East and North Africa, most notably in Egypt, where protests called for on Facebook resulted in thousands taking to the streets and eventually overthrowing the long-time president, Hosni Mubarak. These initial victories, as well as more minor victories in Morocco (where the monarchy conceded reforms following protests organized online), led to the Internet being hailed as a force for democracy.

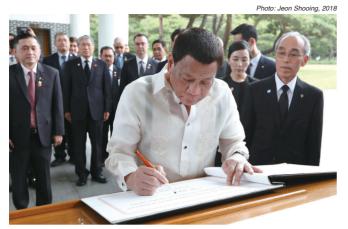
Despite these victories, or perhaps because of them, authoritarian governments in the Middle East and beyond — as well as, in several cases, democratic governments — were increasingly restricting freedom of expression and association online. In countries such as Saudi Arabia and China, the decision to censor was opaque and unexplained. In more democratic countries, however, censorship was often enacted under the guise of public or children's safety, or for economic reasons, as in the case of proposals to censor copyright violations or cut off Internet users who engaged in such acts, as was proposed in France.

By 2012, the OpenNet Initiative — a joint project of several academic institutions including Harvard University and the University of Toronto — estimated that 47% of the world's Internet users were viewing the Internet through a fractured lens; that is, they were experiencing Internet censorship.

The Social Media Era

Although social media most certainly played a role in the organization of the Arab uprisings, its role was exaggerated by media. Nevertheless, social media's place in the activist toolkit was secured, with movements from New York to Thailand becoming reliant on social networks for disseminating information and organizing protests.

Social media has undoubtedly enabled certain movements to



Rodrigo Duterte, president of the Philippines, visits the Seoul National Cemetery in South Korea.

thrive. The Egyptian uprising of 2011 was in some ways the result of years of strong ties amongst activists, but without Facebook — the platform on which the call to take to the streets on Jan. 25, 2011 was made — the demonstrations may not have gained the critical mass they needed to succeed. Similarly, in the US, the Black Lives Matter movement was the outcome of building frustration and organizing amongst African-American communities throughout the country, but social media enabled the movement to take advantage of a critical moment of national anger and, by using a hashtag on Twitter, garner widespread support and attention.

There is, however, also a risk to the increased utilization of closed, proprietary social networks by social movements. Although we often treat them as such, these platforms are not the town square; rather, they are like a shopping mall or company town, undemocratically governed and unaccountable to the public. Both of the aforementioned movements have experienced this firsthand: the page that eventually called for demonstrations in Cairo was taken offline just three months prior when its administrator ran afoul of Facebook's rules, while activists involved in the Black Lives Matter movement have complained of the platform removing images discussing racism.

More recently, events surrounding the US and Philippine elections have brought into sharp focus the question of whether social media is good for democracy. In a prepared testimony submitted to the US Senate judiciary committee, Facebook admitted that around 120 Russian-backed pages created 80,000 posts that were viewed directly by 29 million Americans during the 2016 presidential election campaign. The company has admitted to uncovering similar behavior in the run-up to the 2018 midterm elections as well.

In the Philippines, where Facebook is a leading provider of news and information and is often available for free to mobile subscribers. the platform is said to have been a key to the election of illiberal populist President Rodrigo Duterte. According to an article by journalist Davey Alba for Buzzfeed, doctored images and propaganda about Senator Leila de Lima, a fierce critic of Duterte, began

circulating on Facebook shortly after his ascension to the presidency. Duterte had publicly threatened to "destroy" de Lima, and the images became part of that campaign.

In a letter to *Buzzfeed*, de Lima wrote of Facebook: "We were seduced, we were lured, we were hooked, and then, when we became captive audiences, we were manipulated to see what other people — people with vested interests and evil motives of power and domination — wanted us to see. It was a slow takeover of our attention. We didn't notice it until it was already too late."

Propaganda disseminated on social media has not only influenced elections; in Myanmar, it may have contributed to the ongoing ethnic cleansing of the Muslim Rohingya population. UN human rights experts investigating a possible genocide in Myanmar have confirmed that Facebook played a role in spreading hate speech against the Rohingya minority.

Just as social media allows social movements to take advantage of attention and quickly build up their networks, so too does it allow bad actors to disseminate propaganda and misinformation which, once released, can be nearly impossible to counter with truth. The deleterious effect this has on democratic participation, though difficult to quantify, is clear.

The "echo chamber", a media phenomenon by which individuals are exposed only to information from like-minded individuals, has been exacerbated by what Internet activist and commentator Eli Pariser calls the "filter bubble", a state of isolation (again, often with only like-minded individuals) that occurs as a result of algorithms selectively offering up content based on a user's searches, "likes" and other online activity. Legal scholar Cass Sunstein has referred to echo chambers as "the enemy of democracy", citing diverse debate and freedom of speech as fundamental elements of a democratic society.

Indeed, the ways in which algorithms have segmented elements of society into their own "filter bubbles" has resulted in a scenario where the very essence of truth is now in question. Furthermore, the information collected about us could be used to nudge us toward particular voting systems. In the most recent US presidential election, Facebook allowed presidential campaigns to upload their email lists and voter files containing real names, political habits, and contact information to the company's advertising network, enabling candidates to micro-target voters with ads that suit their personal preferences and lifestyles. This practice, assisted by machinelearning algorithms, has put Facebook at the forefront for campaign spending in the US.

Pervasive Surveillance

In the past few years, the term "surveillance" has become part of our lexicon in the wake of revelations that the US — often in partnership with other countries, namely the so-called "Five Eyes" has been collecting massive amounts of metadata on its own citizens and foreign citizens alike. This method of surveillance — often called

"dragnet" or "mass" surveillance — has been widely condemned by civil society groups as being both unnecessary and disproportionate in the fight against terrorism.

The knowledge, or even the perception, of being surveilled can have a chilling effect on the joint freedom of expression and association. An industry survey conducted by the World Economic Forum in 2012 — a year before Edward Snowden leaked information about the National Security Agency's programs — found that in countries with high Internet penetration, a majority of respondents (50.2%) believe that their government "monitors what people do on the Internet". Simultaneously, 50% believe that the Internet is a safe place for expressing their opinions.

But government-conducted mass surveillance is only one way in which data and metadata are being constantly captured about us. We regularly give up data about ourselves voluntary to the same companies from which we seek out news and information, enabling them to tailor their algorithms to give us exactly what we want to see. The pervasiveness of new digital technologies like virtual assistants such as Alexa or Siri raises questions about what, precisely is being collected about us.

Furthermore, there is data *involuntarily* being collected about us as we move throughout cities. A number of cities throughout the world have begun to pilot facial recognition programs in public spaces aimed at matching the faces of individuals with images contained in criminal databases or, in some cases, identifying emotions — such as nervousness — through the use of sentiment analysis technology. Many of these programs have been undertaken without appropriate oversight to ensure the security of the data, and to ensure the consideration of human rights.

Conclusion

The next few years promise even more intense development of new digital technologies, from self-driving cars assisted by AI to the spread of digital cryptocurrencies and blockchain technology. We will also see new technologies applied to existing practices as old as our very democracies, such as voting.

Take Estonia, for example. In a country where modern citizens increasingly interact with their government through digital means, an e-voting system linked to the national ID card promised secure voting, until a set of Finnish and American researchers found flaws in the security of the system. While e-voting systems are intended to bring greater ease to electoral practices, security flaws threaten society's confidence in the integrity of elections, jeopardizing the very underpinnings of democracy.

And in India, a controversial identity database that has begun enrolling the country's more than 1 billion citizens has been found to contain serious security flaws: a software patch, easily obtained for around 2,500 rupees (\$35), allows anyone to generate new identity numbers, creating a threat to national security.

Many new digital technologies pose unique threats to democratic



Estonia's e-voting system allows citizens to vote from home using their ID card.

norms, as advances in new wave technologies increasingly put humans secondary to machines. Matthew Stender, a technology ethicist and researcher who sits on several working groups of the Institute of Electrical and Electronics Engineers (IEEE), told me that "[p]erhaps the greatest risk that AI poses to democracy is not found in the technology itself, but in the rush for policy makers to embrace an unproven and biased technology with little regard to its long-term impact. In an effort to avoid uncomfortable decision making, democratic representatives and civil servants alike are laying the groundwork to take humans evermore out of the loop."

Nevertheless, new digital technologies have the potential to change the very nature of governance. It is thus imperative that governments and corporations involved in the development of machine learning and AI technologies ensure that a diverse constituency of humans are involved in every step of the process. from design to launch. We must also ensure the security and integrity of new technologies applied to existing systems, and not sacrifice safety for convenience.

The ability of campaigns, governments, and other actors to manipulate trusted systems and platforms (such as, but not limited to, Facebook) poses a very real threat to democracy that we are only beginning to fully understand. At the same time, the ever-increasing level of control exerted by some governments over technology, and the Internet, creates a hindrance to progress, including progress of our democratic systems. As we progress toward the future, we mustn't forget the lessons of the past. Democracy is ultimately a system of checks and balances, and we as members of society must use that to hold technological development accountable just as we would our elected representatives. JS

Jillian C. York, a writer and activist based in Berlin, is director for International Freedom of Expression at the Electronic Frontier Foundation.