# EMERGING TECHNOLOGY

## Civic Space Future Trend Report

BY POONAM JOSHI

Resource paper for the
International Center for Not-for-Profit Law
Civic Space 2040 Initiative
Published March 2020

ICNL
INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW
WWW.ICNL.ORG

# FUTURE TREND: EMERGING TECHNOLOGY

*Over the next two decades, environmental, technological, and demographic trends will dramatically change how we live our lives. A vibrant civic space is essential to ensure everyone can fully participate in shaping this future. ICNL launched "Civic Space 2040" — a futurist initiative to craft a positive vision for civic space and map strategies to make it a reality. The initiative explores trends that will radically transform the future and discusses ways in which these trends will affect civic space. This briefing is one in a series commissioned by ICNL to help inform civic space advocates about the opportunities and challenges ahead.*

The potential impacts of emerging digital technology[1] on civil society are widely discussed, but much more could be done to prepare civil society for a digital world. Whether digital technology will have a positive or negative impact on civic space and philanthropy will depend on a range of factors:

- The feasibility of reforming the practices and business models of the technology companies;
- The governance of the internet and the degree to which states instrumentalize technology for their own geopolitical and domestic goals;
- Whether the efforts of technologists to re-invent and decentralize the infrastructure of the internet gains traction; and
- The capacity of civil society — beyond a small group of digital rights experts — to integrate a focus on digital technology into every aspect of their work.

This briefing explores the trends in emerging digital technology most likely to shape civic space, and opportunities for civil society advocates to mitigate and capitalize on the changes ahead.

## POLICY AND GOVERNANCE OF DIGITAL TECHNOLOGY AND THE INTERNET

Digital technology has delivered a huge range of benefits and challenges to businesses, citizens, and wider society. The internet has fundamentally changed how people access and receive information. It has allowed civic actors to flourish and compete in the so-called 'marketplace of ideas,' but it has also created the conditions for malign actors to interfere in elections, fuel polarization and spread hatred.

[1] For the purposes of this paper, emerging digital technology refers to hardware and software built using information and communication technology and/or the internet, such as artificial intelligence applications, facial recognition tools, online social networks etc.

## BUSINESS MODELS

The threats digital technology poses to civic space and democracy are rooted in the business model of the most successful technology companies and the governance of the internet eco-system to date.

The digital economy is predicated on the accumulation, analysis, and sale of vast amounts of data by a handful of largely US-based platforms: Facebook, Amazon, Alphabet (the parent company of Google), and Apple. This data — based on the browsing habits, social media profiles, online purchases, and Google searches of users — can be used to send targeted messages to influence the behavior of increasingly specific groups of social media users for private profit, public good, or malign purposes.

The next generation of digital technologies will enable companies to extract data not just from online spaces, but from the built environment. The Internet of Things[2] will enable companies to gather personal data from cameras, smartwatches, fitness trackers, toys, and automated travel. Facial recognition technologies and sensors in Smart Cities[3] will also allow the harvesting of data from users in public spaces.

While this data could be used to improve fitness, health care, transport, or energy efficiency, without regulation or oversight, it could equally aid manipulation or surveillance by malign states, companies, or other non-state actors on an unprecedented scale.

## REGULATING THE INTERNET

Whether current or emerging technologies will be harnessed for the public good or in ways that threaten civic space will be determined by who governs the internet. Built and operated by the private sector, the technical governance of the internet from inception has been global and consensus-based, rather than state-based or backed by law.

In the absence of an overarching legal or regulatory framework, governance of the internet has largely remained in the hands of the US tech platforms. Resistant to regulation, the platforms have largely failed to take responsibility for the social and political impact of their systems and operations, or offered anything beyond ameliorative measures.[4]

[2] In the broadest sense, the term Internet of Things (IoT) encompasses everything connected to the internet, but it is increasingly being used to define devices that "talk" to each other, from simple sensors to smartphones and wearables. Through combining these connected devices it is possible to gather information, analyze it and create an action that improves the experience for the user.

[3] A Smart city is an urban area that uses different types of electronic IoT sensors to collect data and then use insights gained from that data to manage assets, resources and services efficiently. This includes data collected from citizens, devices, and assets that is processed and analyzed to monitor and manage traffic and transportation systems, power plants, utilities, water supply networks, waste management, crime detection, information systems, schools, libraries, hospitals, and other community services.

[4] Ameliorative actions taken by the tech platforms are documented in Governance Innovation for a Connected World, edited by Eileen Donohoe and Fen Osler Hampson, Centre for International Governance Innovation, 2018.

Set to dominate the artificial intelligence (AI)[5] sector, the tech giants will be responsible for the evolution of the technologies likely to transform civic space unless states take steps to regulate the sector or reform the underlying business model in partnership with civil society.

However, effective regulation of the internet, AI, and future digital technology will only be possible with the cooperation of multiple government agencies and the private sector companies, a challenging outcome to achieve given the divergent values and agendas of Western democracies and authoritarian states on this issue.

The battle for who governs the internet reflects a broader geopolitical struggle for values and influence between authoritarian states and Western democracies. China, Russia, and Iran, in particular, have raised concerns about the decentralized governance of the internet, partly as a reaction to the internet being driven by the US and other Western democracies. A decentralized internet runs counter to the desire of these states to manage information and communications centrally.

One country where the US tech platforms have very little power and influence is in China, which has protected its domestic internet market from foreign competitors and built its own set of social networks, including the Twitter—like Sina Weibo and WeChat/Weixin, which is similar to WhatsApp. Censorship is baked into these platforms, as platform operators must monitor online content and remove offending posts or risk losing their operating licenses.

Internationally, China is aggressively advocating for cyber sovereignty[6] and exporting its model of extensive censorship and automated surveillance systems to a significant cohort of countries. Freedom on the Net reported that last year China hosted media officials from 36 countries for seminars on its system of

> “Whether technology will be harnessed for the public good or in ways that threaten civic space will be determined by who governs the internet.”

[5] Artificial intelligence (AI) refers to a constellation of technologies, including machine learning, perception, reasoning, and natural language processing. See: The Social and Economic Implications of Artificial Intelligence: Technologies in the Near-Term, AI Now, July 7, 2016.

[6] Cyber sovereignty is the assertion of the right of each state to control the internet within its borders. States justify this concept by arguing they should be allowed to assert control over information and communication technology and enhance their capacity for surveillance to guarantee a peaceful, safe, relevant or appropriate information space.

censorship and surveillance, including several with poor track records on civic freedoms, such as Egypt, Libya, Saudi Arabia, and the Philippines.

Western democracies — although ostensibly committed to civic freedoms — have also struggled to develop coherent policy positions on governance and regulation. Concerns about privacy, election interference, and the dissemination of violent, extreme, and harmful content online have led several states, including the UK, France, and Germany, to propose laws that permit censorship and content removal in ways that inadvertently limit freedom of expression. For example, in April 2019, the British government proposed sweeping new powers to remove "harmful" content from the internet, which could easily be used as a pretext to censor speech.

At the same time, the US, Israel, and several European countries have a record of exporting surveillance technologies to governments with poor human rights records, leaving them in a weak position to challenge China's actions. In June 2018, a number of European Union member states — including the UK, Poland, Sweden and Ireland — attempted to block curbs on the export of surveillance equipment to abusive regimes.

In contrast, the European Union has been at the vanguard of safeguarding privacy through the introduction of data protection laws in 2018, challenging the monopoly of US tech giants.[7] The EU is also seeking to set global standards on the ethical and legal framework of AI, particularly where it is adopted by public authorities and used in healthcare, policing, and transport.

## OPPORTUNITIES FOR ACTION

### REGULATORY INNOVATION

Civil society has a critical role to play in informing government efforts to articulate law and policy in the field of AI that speaks

## Advocating for New Legal protections

### IMPROVING DATA PROTECTION

Comprehensive data protection laws, which should apply to both the government and private sector, could address many of the human rights risks posed by AI. One model is the European Union's General Data Protection Regulation (GDPR), one of the strongest and most comprehensive attempts to regulate the collection and use of personal data by both governments and the private sector. The GDPR limits data processing to permissible purposes, with protections for sensitive data. It also requires opt-in consent, which limits the use of personal data for training AI systems. Rights provided for by the GDPR, and similar laws, offer a framework to prevent against unaccountable uses of AI that impact individual rights while ensuring a level of control of personal data and accountability for the use of AI and machine learning systems.[8]

### COMBATING DISINFORMATION

Digital rights experts are calling for laws that mandate that all automated accounts are clearly labeled to show the source of an ad, the funding behind it, and the scope of its reach. This could disrupt targeted digital political advertising and the amplification of bot networks.[9]

[7] The European Union has launched several actions, including challenging Google's alleged monopoly and demanding that Apple pay the Irish government 13 billion euros in back taxes.

[8] See: Human Rights in the Age of Artificial Intelligence, Access Now, November 2018, p 30-31. GDPR was enacted in 2016 by the European Union, and went into effect May 25, 2018, across the EU's 28 Member States.

[9] See: https://luminategroup.com/storage/275/Digital-Democracy-Charter.pdf

to both public and private sector applications. However, the internet policy field is relatively young, and much more needs to be done to build the capacity of a wider range of civil society actors to safeguard civic freedoms within digital environments through policy and advocacy.

Civil society groups would benefit from training and tools to enable them to defend civic space at the national level vis-à-vis governmental tech initiatives, such as national AI strategies or laws on surveillance, as well as in the dozen multi-stakeholder fora where global policy is discussed.[10] A recent collaboration between ICNL and Stanford's Global Digital Policy Incubator to conduct the first Tech Camp for Civic Space Defenders serves as an example. Particular support is required to enable civil society representation from repressive governments, especially China and Russia, in stakeholder forums.

Issues of privacy, data protection, and combating disinformation could be tackled by civil society through demands for new legal frameworks.

### CIVIL SOCIETY INVOLVEMENT IN THE DESIGN OF TECHNOLOGY

Human rights experts have also called for much greater civic engagement in the design of AI to ensure human rights safeguards are built-in from inception to implementation.

> **HUMAN RIGHTS IN AI DESIGN**
>
> The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, and Access Now recommend that civil society be consulted during human rights impact assessments to be conducted throughout the AI lifecycle, from conception to implementation.[11] Those consulted should include human rights defenders and representatives of marginalized or underrepresented end users. The results of human rights impact assessments and public consultations should be made public.

### ALTERNATIVE TECHNOLOGICAL AND BUSINESS MODELS

Finally, there is a growing movement of digital rights activists who argue that the only way to address the harmful impacts of digital technology and harness its power for the public good, is to transfer power over data from centralized platforms back to their users. Although there is a growing focus on the concept of technology serving public interests, the approaches being suggested are diverse.

[10] Policy is debated in multilateral bodies like the International Telecommunication Union, engineering groups like the Internet Engineering Task Force, the human rights system of the UN, normative bodies like the Internet Governance Forum or the OECD, domain name organizations like Internet Corporation for Assigned Names and Numbers (ICANN) or regional registries.

[11] See: https://undocs.org/A/73/348 29 August 2018, pp 20-21 and Human Rights in the Age of Artificial Intelligence, Access Now, November 2018, p 32.

### DATA, DIGITAL INFRASTRUCTURE, AND SERVICES FOR THE PUBLIC GOOD

Tim Berners-Lee, the inventor of the World Wide Web, is experimenting with a new architecture called Solid, in which user data remains under a user's control and is shared with applications when they need it, rather than being owned by those platforms.

The British think tank, the Institute for Public Policy Research (IPPR), is one of many think tanks calling for reforms that organize data and digital infrastructure as a public good. IPPR recommends moving from conditions of "monopolistic data enclosure" to a "digital commonwealth," where the vast potential of socially generated data helps develop the wealth, creativity, and capacity of all society. IPPR proposes several measures, including: (1) Strengthening competition law; (2) Regulating platform giants as public utilities; and (3) Creating a digital national public service that drives the curation and productive use of public data and oversees the creation of a national data portal.

In The Case for Digital Public Infrastructure, media scholar and digital rights activist Ethan Zuckerman makes a case for tackling the issues created by the current platforms and their business model, through technological innovation rather than regulation. He calls upon governments and philanthropies to fund rigorous research about the effects of social media on individual health and on our broader civic health, which can then be used to foster direct experimentation or set policy. For example, if research finds that radicalization stems from interactions in video comments, experimentation in moderating conversations around videos might be more effective than regulation.

# THREATS TO CIVIC SPACE ONLINE

## PRESSURE ON FREE EXPRESSION, ASSEMBLY, AND ASSOCIATION

This section examines the impact of digital technology on civic space in more depth, as well as emerging responses from civil society and technologists.

The 2018 report, Malicious Use of AI, predicts that AI will figure prominently in the security landscape of the future and that more can and should be done as a matter of urgency to prevent the use of AI by malign actors. Some commentators[12] argue that policymakers have yet to seriously grapple with AI's repressive implications, particularly with expression and assembly in the context of rising authoritarianism and democratic backsliding.

[12] Steven Feldstein reports that from 1989 onwards, popular revolts and electoral defeats have become the most common causes of departure for dictators, compared to coups in the period 1946-1988. He argues that as the gravest threats to authoritarian survival are from discontented publics on the streets or at the ballot box, autocrats are embracing digital tactics for monitoring, surveilling and harassing civil society movements, and for distorting elections as strategies that are both cost effective and carry less political risk. He also notes that democratic governments may have an incentive to use AI to monitor the activities of political opponents and civil society and take pre-emptive action against potential challenges to their authority. Finally, governments that depend on Chinese technology to control their populations will feel increasing pressure to align their policies with China's strategic interests. See: Feldstein, Steven. The Road to Digital Unfreedom: How Artificial Repression is Reshaping Repression, Journal of Democracy, January 2019.

### INCREASING CENSORSHIP

Demands by states to companies to address terrorist content, hate speech, and fake news are increasing, but there are no clear definitions for what the issues encompass or standards on how to address them. Filtering out hate speech could create a massive backlash in authoritarian contexts where governments direct or are complicit in hate speech towards certain groups.

Content moderation might also be used to censor marginalized groups and appease illiberal or authoritarian governments. Content intended to be controversial, hyperbolic, satirical, or ironic may also be wrongly censored by human or automated monitors seeking to target offensive content.

### UNPRECEDENTED STATE SURVEILLANCE

Machine learning systems can already infer or predict highly sensitive information from non-sensitive data. Looking ahead, authorities could aggregate the data we produce online, through our phones and other devices, and facial recognition technology in public spaces to monitor, identify, or locate certain individuals or groups. This could be used for positive goals — improving public transportation — but also for targeted and mass surveillance. According to Access Now, 50% of adults in the US are already in law enforcement facial recognition databases, and China could be the first country to develop a fully centralized facial recognition system.[13]

### AI-ENABLED RESTRICTIONS PROTEST

AI-enabled censorship could be used to remove content that facilitates the organization of in-person gatherings and collaboration. Through data from satellite imagery, including heat maps,[14] facial recognition powered cameras, and cell phone location, AI could also be used to provide detailed information to predict and disrupt gatherings. Facial recognition technology in public spaces could also have a chilling effect on assembly, as many people rely on the anonymity provided by mass protests to gather in public and express their views.

> “Facial recognition technology in public spaces could have a chilling effect on assembly, as many people rely on the anonymity provided by mass protests.”

[13] See: Human Rights in the Age of Artificial Intelligence, Access Now, November 2018, p 21

[14] Heat mapping involves the detection and strength of signals sent out from mobile devices to create a “heat map” that indicates where protesters are gathering.

The problem of predictive policing and sentencing and racial bias in the criminal justice system has already been well documented. This issue is likely to be replicated for minority and marginalized groups engaging in dissent and protest. The surveillance of the Black Lives Matter movement and the recent use of facial recognition technology against protesters in India challenging anti-Muslim legislation illustrates that intersection.

### RISE OF MISINFORMATION

We are now in an era of information warfare where repressive states are realizing that manipulation via digital platforms could be a much more powerful tool than suppression or surveillance to achieve their goals.  A growing number of states are advancing their goals by using various tools to spread misinformation, including AI-powered bots,[15] deepfakes,[16] and manipulating social media algorithms to interfere in elections[17] and erode public trust in fact-based evidence.

If platforms do not successfully curb these methods of spreading misinformation, public trust in the legitimacy of elections, as well as traditional media and civil society, may decline further. The devaluation of notions of truth and fact poses significant challenges for civil society, as their ability to advocate for social change relies on the legitimacy of their evidence. Looking ahead, there are concerns that deepfakes could be used to incite discrimination, violence, and conflict, or discredit activists and leaders — particularly women — through the creation of compromising images.

### PLATFORMS CURATING ACCESS TO INFORMATION[18]

Tech platforms will continue to play the role of gatekeepers to information on civil society through curation, the ranking of information based on user interest and data sets, and content moderation. There has been little examination of how curation impacts freedom of association, including how systems determine which civil society groups and issues are given prominence online. The growing use of non-traditional interfaces, such as Amazon's digital assistant Alexa, could heighten this effect as the interfaces present users with information about issues and organizations based on existing preferences. As a result, civil society organizations may find it harder to engage with potential supporters.

[15] A chatbot, or chat bot, is a machine that has a conversation with humans via text or audio. An AI powered chatbot is a smarter version, which uses natural language processing (NLP) and machine learning (ML) to better understand the intent of the human and provide more natural, near human-level communication.

[16] Deepfakes are images or videos that are altered using neural networks and machine learning, making them both realistic and difficult to detect.

[17] Strategies include using bot-driven, large-scale information-generation attacks to swamp information channels with false or merely distracting information, making it more difficult to acquire real information.

[18] CAF's 2018 report, Machine made goods: Charities, Philanthropy & Artificial Intelligence provides a comprehensive guide to the practical and ethical implications of technology for philanthropy.

## OPPORTUNITIES FOR ACTION

### COMBATING SURVEILLANCE

Until recently, activity on the issue of surveillance was limited to the investigation and exposure of the European, American, and Israeli tech companies that supplied spyware to repressive regimes.

Holding companies to account had proved difficult until October last year, when WhatsApp launched an unprecedented lawsuit against Israeli cyberweapons firm, the NSO group, accusing it of being behind secret attacks on more than 100 human rights activists, lawyers, journalists, and academics in a two-week period last year. The lawsuit — mounted with the support of Citizen Lab — marks a major positive step forward for human rights protections online and could set a precedent.

Looking ahead, the issue of surveillance and privacy in public and private spaces requires much greater attention from civil society. Examples of emerging thinking on this issue include the Digital Freedom Fund's program on Future Proofing Digital Rights, which explores how to protect data collected by children's toys and devices and how to prevent states from introducing hacking powers over connected household devices.

With regards to practical security, international organizations including Frontline Defenders and The Engine Room, offer digital security training to human rights organizations, but massive gaps remain in providing protection against digital surveillance for communities or movements. Pioneering work in the US with racial justice activists illustrates what is possible.

### RESTORING TRUST IN MEDIA AND FACTS

The role of digital technology in eroding trust in media and democracy has received considerable attention from states, media organizations, and civil society, although the problem continues to outstrip the scale of the response.

There has been investment in media literacy initiatives, in particular fact-checking websites and tools such as PolitiFact.com, FullFact.org, and BBC Reality check. While useful, it is questionable how effective these initiatives are, as they operate at the level of evidence rather than feelings or mood, which is the forte of propaganda.

### Community-level Strategies for Countering Surveillance

MediaJustice in Oakland exposes the application of surveillance against people of color and the Black Lives Matter movement. Its national campaign, Defend Our Movements, seeks to protect activists working on racial and economic justice in a digital age. Support offered includes a web-based clearinghouse offering activists the most up-to-date and useful information about protecting devices and data.

Crypto-Harlem provides free public workshops on privacy, anti-surveillance, and digital security for people in New York City.

Greater transparency from media outlets on how they collect, report and disseminate news, disclosure of who pays for advertising, regulating political advertising, and investment in independent and investigative media could be more effective ways to build or re-build trust in media and democracy.

### CREATING A PUBLIC DISCOURSE AROUND THE IMPACTS OF TECHNOLOGY

Civil liberties and digital rights groups have traditionally struggled to secure public support regarding the issues of data and privacy due to disinterest or the complexity of the issues involved. However, public concerns over election interference and, more recently the use of facial recognition technologies provide an unprecedented opportunity to engage the public on the abuse of AI.

The 2019 Netflix documentary, The Great Hack, which focuses on manipulation of voters' data and interference in the 2016 US Presidential elections and the success of the book, The Age of Surveillance Capitalism[19] by US academic Shoshana Zuboff demonstrates it is possible to engage public interest on complex issues such as AI, surveillance and the digital economy.

## POSITIVE TRENDS AND INITIATIVES

Over the next two decades, all civic actors will need to learn how to operate in a digital world. In her 2020 forecast on digital civil society, Lucy Bernholz notes that "Effective organizations will be those that manage and govern all of their resources—time, money, staff, data, and digital systems—toward mission." Digital technology offers civic actors the power to transform their impact, increase transparency and trust, improve communications, and find new sources of funding.

As the community of engineers and entrepreneurs thinking about digital tools that meet civic needs remains relatively small, we don't yet have a full sense of what AI and digital technology could do to improve civic space. However, new ideas and tools are emerging that could improve the impact and reach of civil society and benefit society more broadly.

### Using AI to Provide Real-time Assistance to Protesters

OVD-Info is an independent Russian human rights project which collects information about arrests at public protests and other forms of political repression. In 2017 OVD-Info developed a special Telegram bot that allows users to voluntarily report their arrests and any other interaction with law enforcement and to receive immediate advice on their legal rights. Over 8,000 people registered to receive information through the bot. When Russians took to the streets to protest proposed pension reforms on September 9, 2018, an estimated 1,200 people were arrested in 38 cities, of which 184 reported their arrests to OVD-Info.

[19] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019

### INNOVATION TO ADVANCE MISSION AND GOALS

AI could be utilized by charities and civil society organizations to help them further their mission and goals. Work underway falls largely into three categories:

1. Improving accessibility to info and services for users facing challenges to access due to disability, visual impairment or language – e.g., Tailored Chatbots that provide advice or service;
2. Analysis of data at an unprecedented speed and scale to advance breakthroughs in medical treatment and research, and predict extreme weather events to assist with climate adaptation, and
3. Using novel applications and machine learning to uphold civic freedoms and human rights – from platforms to improve access to legal advice for protesters, to investigative journalists using machine learning to mine huge volumes of financial data to identify evidence of money laundering and corruption.

To capitalize on these opportunities, civil society will need to address issues of who owns the data they have access to, consent to use the data, and take steps to improve the quality and quantity of data.

### DECENTRALIZING DIGITAL INFRASTRUCTURE

Of the many emerging technologies examined while developing this paper, blockchain[20] was the most hyped and hotly debated. The decentralized and immutable characteristics of blockchain mean it could be used to prevent fraud and corruption in a variety of settings, including cross-border financial transactions, data sharing, and voting.

In relation to philanthropy, blockchain offers a radical degree of transparency, allowing assets to be tracked through a chain of transactions. Although the idea of using blockchain for

> “Of the many emerging technologies examined while developing this paper, blockchain was the most hyped and hotly debated.”

[20] Blockchain is a distributed public ledger: a way of keeping a record of transactions and ownership within a system without the need for a traditional trusted third party.

cross-border giving is already being tested,[21] there is little clarity about the regulation of blockchain or cryptocurrency for this type of giving. There is also a significant 'last mile' problem: cryptocurrency is not much use unless you can spend it on goods and services or convert it to traditional currency.[22]

## REGISTRATION TECHNOLOGY

CAF has highlighted several ways AI could be used to improve the registration, oversight, and compliance of nonprofits.[23] These include: using AI to scan a large amount of financial data to spot early compliance issues rather than using enforcement as a tool; embedding laws and regulations in smart contracts governing how organizations operate so that it would not be possible to break them, thus minimizing the need for enforcement; and recording transactions on blockchain so that accurate, real-time information on spending would be available to everyone, and annual reporting would no longer be necessary.

## SUPPORTING FLUID ASSOCIATIONS

Democracy activist Pia Mancini from Democracy OS is experimenting with the concept of open platforms that act as fiscal sponsors for those wishing to organize more fluidly than is typically permitted by current laws governing association. The platforms would operate on a model of trust between people and organizations and act as a transparency and accountability mechanism.

## MOVEMENT TECHNOLOGY

Informal and movement-based groups need robust, diverse, value-driven software that keeps them safe and can be used securely in dangerous places. Aspiration Tech is the leader on producing tools that support movement building, including open-source software that supports secure communications and collaboration.

A 2017 report for the Ford Foundation sets out a long term strategy for providing support to develop technology that helps movements. The report identifies needs, including the development and dissemination of software that enables activists to browse securely, divorce their identity and location when using devices, and decentralize how data is held across different countries so access can't be blocked.

[21] Large INGOs and aid agencies like UNICEF are experimenting with using blockchain for their internal money flows. Meanwhile, start-ups like Disberse are trying to build platforms that can harness blockchain technology to make cross-border payments more efficient, transparent and cost-effective.

[22] See: https://www.cafonline.org/about-us/caf-campaigns/campaigning-for-a-giving-world/future-good/blockchain

[23] See: https://www.cafonline.org/about-us/publications/2016-publications/block-and-tackle-using-blockchain-technology-to-create-and-regulate-civil-society-organisations

## CONCLUSION

On the cusp of a new industrial revolution, digital technology has already transformed civic space and democracy in ways that were unthinkable even a decade ago. As recently as 2011, we viewed technology primarily as a force for good, as social networks and messaging apps enabled protests across the Middle East and North Africa. Less than a decade on, we now also recognize the power of the same networks to spread disinformation and hatred. As innovation accelerates, technologists, states, and civil society are struggling to keep up with its societal impacts.

Civil society has a critical role to play in ensuring that digital technology serves the public good; through reform, improved governance, and as equal partners in the design and implementation of emerging technology. Civil society also has the opportunity to embrace the potential of AI to improve impact and ensure its infrastructure is fit for a digital age. In order to do both, civil society will need tech literacy, especially at the leadership level, supportive boards, willing funders, and the ability to share the costs and risks of investing in AI with states and the private sector.

> “Digital technology has already transformed civic space and democracy in ways that were unthinkable even a decade ago.”

ICNL

1126 16th Street NW, Suite 400
Washington, DC 20036 USA

🌐 www.icnl.org
f facebook.com/ICNLAlliance 🐦 twitter.com/ICNLAlliance