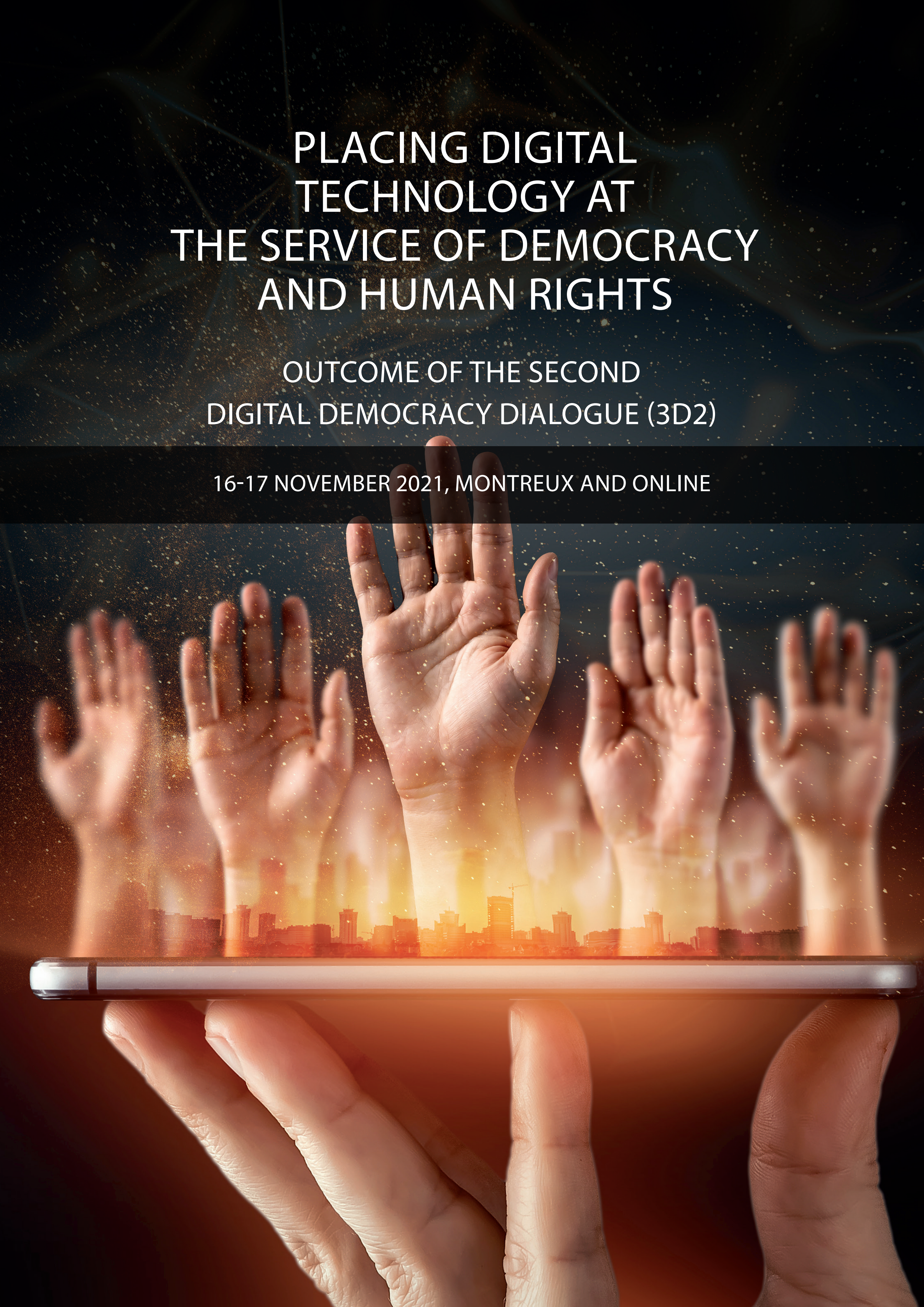
PLACING DIGITAL TECHNOLOGY AT THE SERVICE OF DEMOCRACY AND HUMAN RIGHTS

OUTCOME OF THE SECOND DIGITAL DEMOCRACY DIALOGUE (3D2)

16-17 NOVEMBER 2021, MONTREUX AND ONLINE



UNIVERSAL RIGHTS GROUP
GENEVA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

THE
CARTER CENTER

cdt CENTER FOR
DEMOCRACY
& TECHNOLOGY

INTERNATIONAL
IDEA
INSTITUTE FOR
DEMOCRACY AND
ELECTORAL
ASSISTANCE

Norwegian Ministry
of Foreign Affairs

FACEBOOK

High-level opening

H.E. Simon Geissbühler,
Ambassador, Head of the Peace and Human Rights Division, Federal Department of Foreign Affairs, Switzerland

"Amartya Sen has stated that 'democracy is best seen as the opportunity of participatory reasoning and public decision making - as 'government by discussion.' To be able to assemble, to communicate, to discuss and to participate, fundamental rights must be guaranteed. And here digitalisation comes in. Digitalisation changes the way we assemble, communicate, discuss, and participate. It can have both extremely disruptive effects and very positive ones. A rather optimistic [...] outlook regarding the impact of digitalisation on democracy, democratic mobilisation, and information [...] some ten years ago has been partially displaced by a much more sombre assessment. [...] This Dialogue will help us to better understand the intersection of human rights, democracy and digital technology."

H.E. Uzra Zeya,
Under Secretary of State for Civilian Security, Democracy and Human Rights, United States of America

"Today, the internet remains a bastion of economic growth, innovation and human connection, but it is also a place where people are more censored and surveilled than ever before. The misuse of digital technologies by malign actors poses a serious threat to democratic societies [...] Networks, technologies, and digital infrastructure, originally celebrated for their democratising potential, are now regularly exploited to undermine democratic societies and human rights. Yet, [it is important to recall that] technology is inherently neutral. [While it can be used for] nefarious purposes, [it can also] be harnessed for democratic renewal. New technologies provide opportunities to bolster democratic systems and processes, including by strengthening transparency, boosting civic participation, and combatting corruption."

H.E. Michelle Bachelet,
UN High Commissioner for Human Rights

"How do we shape the online universe in a way that puts people at its centre? In the past decade, we have moved quickly from early excitement at the online world opening to us, to a much darker reality. We now realise that the same evils that exist in the real world, can be replicated in the digital one with far greater intensity and speed."

"We have only just begun to rethink democratic participation in the digital world – how technology can help us engage more people, more deeply [...] We have to make the digital public square a safe place for all of us, and a place where democracy can flourish."

Dr. Michael O'Flaherty,
Director, EU Agency for Fundamental Rights

"We have to engage with a positive state of mind, keeping in mind that digital technology is ubiquitous, is not going to go away, and must be a force for good in our world. It must be tamed, and that's the challenge. Abuses are grave and getting worse. [As we strive to meet this challenge] we must adopt a multi-stakeholder approach, bringing all relevant communities to the table – including civil society. And we must recognise that we are not entering *terra nova* – we already have a ready-made set of standards to guide us: international human rights law [...] Article 19 of the ICCPR, for example, is a sturdy guarantor of free speech, especially in combination with General Comment 34, and [soft law instruments such as] the Rabat principles on addressing hate speech."

Dr. Ahmed Shaheed,
UN Special Rapporteur on freedom of religion or belief, and Chair of the Board of Trustees, Universal Rights Group

"The relationship between digital technology, democracy and human rights is, in some ways, like a game of cat and mouse between activism and authoritarianism. A lot of time has passed since the Arab Spring in 2011, but this game persists, and the cat has become more adept, terrorizing the internet, and manipulating voters, at a previously unthinkable scale. [...]

To turn things around, and place digital technology at the service of democracy and rights, "we must consistently apply human rights standards to the online, as well as the offline world, bridge the digital divide, and strengthen transparency in how technology companies operate."

Dr. Kevin Casas-Zamora,
Secretary-General, International IDEA

"Only a decade ago, we saw digital technology used to help topple dictators and demand democratic reforms during the Arab Spring. Back then, we believed such technology was overwhelmingly a force for good, bringing people together, improving participation, minimizing the gap between citizens and policymakers, boosting transparency, combatting corruption – a powerful new ally for democratic actors all over the world. A lot has changed – and in many cases, gone wrong – since then. Over recent years, we have seen social media used to spread disinformation, distort reality, create polarisation, and erode trust [...] Technology has become the new enabler of democratic backsliding."

"Our latest report on the global state of democracy confirms that authoritarianism is gaining ground. This is in large part a consequence of illiberal and nativist forces' success in weaponizing online information, and using digital technology to curtail rights."

"To fight back, we need to do three things: "First, we need new regulation designed to protect democracy and human rights in the digital age;" second, we need to look at the role of money – "at the moment, it is nearly impossible to control what political parties, candidates and other interest groups are spending online, and this is incompatible with a healthy democracy;" and third, we need a discussion about digital rights and freedoms – including "protection from digital abuse, the right to access the internet, and the right to control and own our data."

Alexandra Reeve Givens,
President and CEO of the Center for
Democracy and Technology

"As we prepare for the upcoming Summit for Democracy, and as governments strive to find common ground on digital technology, democracy, and rights, they should be guided by four principles. First, they should commit to working in close cooperation with civil society, the people most impacted by abusive online content and by government measures to supress rights online [...] Second, it is important that these conversations do not take place in a vacuum, but instead build on work that has come before (e.g., the Freedom Online Coalition) [...] Third, as democratic leaders meet to consider how to address challenges such as abusive content online, it is important that they do not inadvertently strengthen the arguments or practices of authoritarians. [And fourth], we cannot afford to only focus on issues we face at home. Authoritarian regimes are using technology to surveil citizens and crush opposition. This includes shutting down the Internet if necessary, and pressuring technology companies to censor national debates or to share user data. Democratic countries need to oppose these practices and support democratic actors and digital technology companies active in these countries."

Iain Levine,
Senior Human Rights Advisor, Meta

“I also remember the extraordinary optimism we felt at the time of the Arab Spring in 2011 – the potential of social media to be an unassailable tool for democracy and human rights. While we have become more cynical over recent years, it is important not to completely forget that sense of optimism.

Striking a balance between giving people a voice but also keeping everyone safe from hatred and harm, is a huge challenge. That is especially so for a company like Facebook that has over 3.4 billion users around the world, and of course we have made mistakes.

Disinformation also poses a particular challenge for Facebook. We know the serious consequences it can have for democracy and for public health (especially during a global pandemic). However, it is also true that there can be a fine line between fact and opinion.

In some countries we have seen governments using disinformation and hate speech as an excuse to adopt overly restrictive laws. In other countries, politicians accuse us of either not doing enough, or doing too much (for example, through self-regulation).

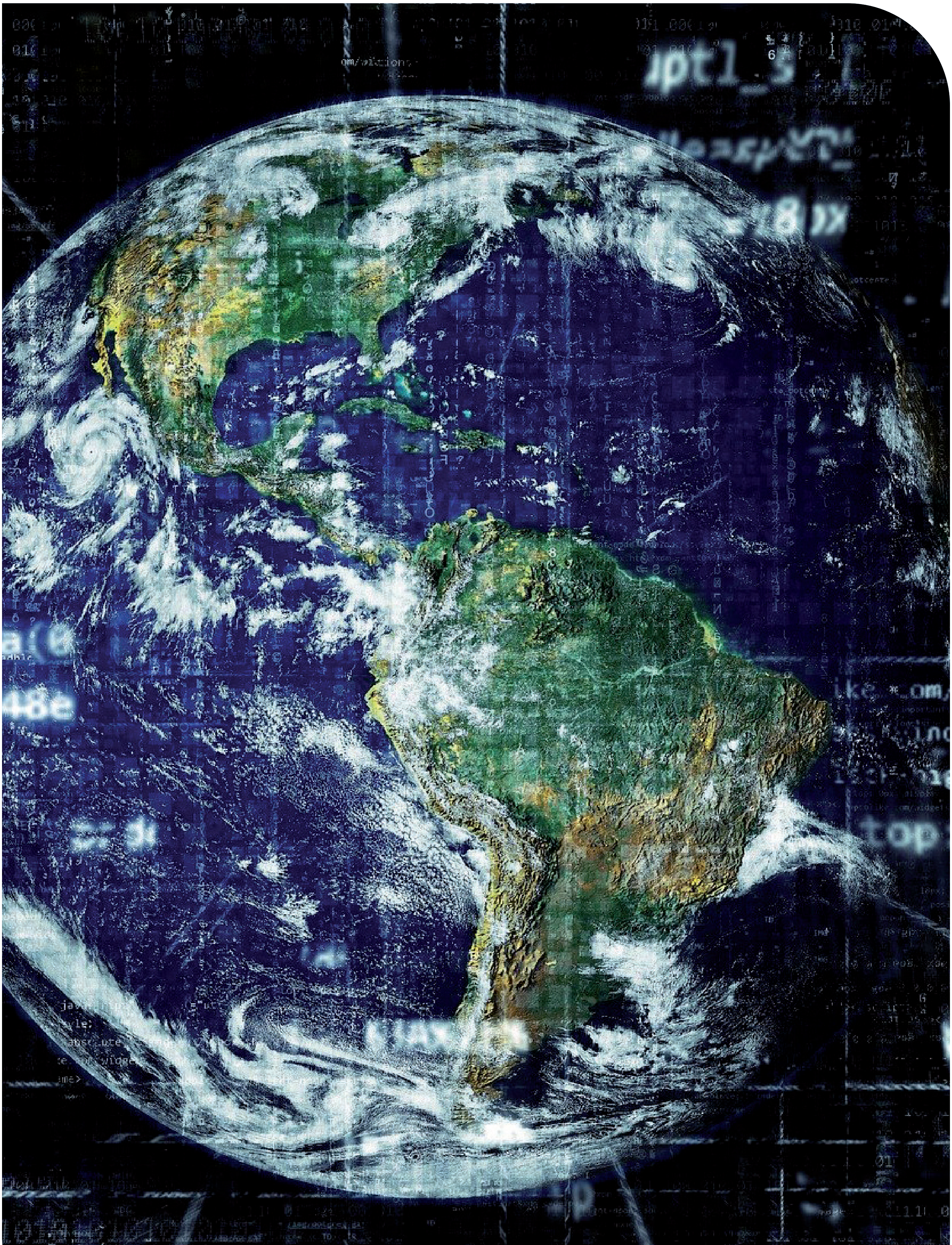
We take hate speech and disinformation particularly seriously during elections. That is why we have invested billions of dollars in our trust and safety work, with a particular focus on democracy and elections.

In taking action to address these and other challenges, technology companies and governments must always be guided by international human rights standards, and must be careful to uphold the principle of an open and unified internet - essential for human rights, sustainable development, and the future of the planet.”

Ideas for possible Summit commitments

- Strengthen international, regional, and national strategies to bridge the digital divide.
- Boost programmes to enhance digital literacy, digital human rights education, and digital civic education.
- Establish a moratorium on the export of surveillance technology, until respect for human rights can be guaranteed.
- Guarantee a multistakeholder approach to addressing challenges such as hate speech and disinformation online, based on an understanding that solutions require States, technology companies, and civil society to be fully involved and to work together.
- Be fully guided, when designing regulatory, self-regulatory, or co-regulatory frameworks, by international human rights law and universal standards. This is especially important for those developed-country democracies whose approaches and laws create new international standards that may well be replicated by others.
- Revise national election laws and infrastructure, to make sure they are fit-for-purpose in the digital age. This should include a review and revision of campaign finance laws.
- Developed-country democracies should integrate digital democracy-related technical assistance and capacity-building support into ODA. So far, international attention to the risks and opportunities posed by digital technology to democracy and human rights has focused on the global North. However, they are also – and increasingly – of importance to democracies in the global South.
- Technology companies should also invest more resources in actions to safeguard human rights online in the global South, for example, by monitoring for hate speech in more languages and more countries, employing more fact-checkers in developing countries, and strengthening connections with local civil society.

- Technology companies should do more to create a safe space for civil society to make a full contribution to democratic society, and to support the work of, and better protect, human rights defenders.
- Begin discussions, at the UN Human Rights Council, on a new Charter of Digital Rights.
- Institutionalise a multi-stakeholder dialogue at the international level to find common solutions to the key challenges at the interface of digital technology, human rights, and democracy – for example, through a new platform at the UN Human Rights Council.



Roundtable 1

ADDRESSING DISINFORMATION AND HATE SPEECH, WHILE SAFEGUARDING ACCESS TO INFORMATION (I.E., TRANSPARENCY, INCLUDING IN THE CONTEXT OF CORRUPTION) AND FREEDOM OF EXPRESSION

The objectives of this roundtable were to take a snapshot of the contemporary challenges posed by 'hate speech' and malicious disinformation, spread online, to human rights and the health of the world's democracies; take stock of government, private sector, and civil society initiatives to address 'hate speech' and 'fake news' while safeguarding free speech and access to information; learn lessons from those initiatives (including nascent laws and government policies); and use those lessons to inform new commitments on the part of States, social media companies, and other relevant stakeholders to strengthen democracy through carefully calibrated and effective policy responses.

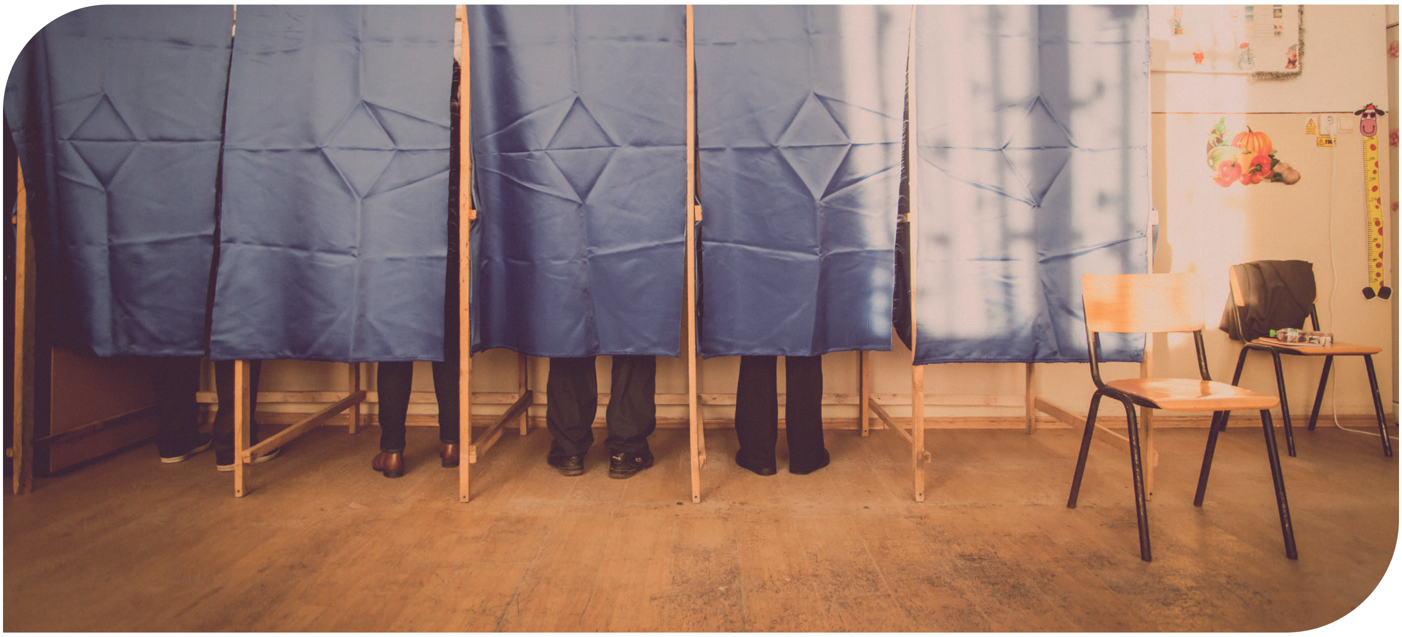
Key conclusions

- Participation and the free exchange of knowledge are fundamental to human rights and democracy.
- While social media platforms are an immensely powerful means of facilitating that participation/exchange, digital technology also carries with it important challenges and risks for the enjoyment of human rights. The rapid spread of speech that seeks to incite hatred or violence ('hate speech'), and of malicious disinformation designed to manipulate or harm ('fake news'), are two such challenges. Both pose a clear and present threat to human rights, especially of those in already vulnerable or marginalised situations, as well as to democratic society (because, in short, they serve to limit political participation).
- Effectively tackling these challenges, while respecting and protecting all human rights, including freedom of expression and access to information, requires a multi-stakeholder approach (involving governments, technology companies, and civil society), and an internationalist approach, founded on international cooperation and the sharing of good practices and lessons learnt. Several participants in Montreux, from government, business, and civil society, argued that "a real opportunity exists for such a unified approach; today, all of us face the same threats, and all of us share common goals."
- Linked with the above point, tackling these challenges will also require a mix of regulation, self-regulation, and co-regulation. "We have seen great examples of such collaborate approaches in the recent past, such as the Christchurch Call on hate speech."
- In designing and implementing these regulatory, self-regulatory and co-regulatory responses, governments and digital technology companies must always be guided by and consistent with international human rights law (both hard legal instruments like the ICCPR, and soft law instruments like the Rabat Plan of Action). Any interventions must also be consistent with the principles of legality, legitimacy, proportionality, and necessity. Technology companies should also be guided by the UN Guiding Principles on Business and Human Rights.

- Social media companies are becoming far more sophisticated in how they deal with issues of hate speech and disinformation online. Partly that is about the use of universal human rights standards as the basic framework for dealing with these difficult issues. But it is also about the development of a wider range of tools. "When I look back at the early days of Twitter, everything was binary: if a post was very obviously inciting hatred or violence, we took it down; if it wasn't, we left it up. Today we have different levels of enforcement, whether that is labelling a post with correct information, placing warming labels over individual tweets, limiting user engagement so they are unable to amplify their message, or actually removing the user – to promote the idea that they are accountable for what they post."
- This raises one of the key challenges for regulators: the ways in which technology companies are responding to hate speech and disinformation (as well as other online harms) are shifting rapidly. Increasingly, those changes are being driven by individual users (see below). Thus, there is a constant risk of government regulation being "stuck in the past," especially if that regulation takes a piecemeal approach focused on specific services or products, rather than on global principles and systemic approaches.
- A key conclusion of the roundtable, which came up repeatedly in the context of both hate speech and disinformation, is that governments need to address such challenges in a more holistic manner, focusing not only on blunt tools such as 'take downs,' but on "improving the wider information and communication eco-system." "The best way to prevent disinformation and call out hate speech is by fostering a diverse and pluralistic media environment (including journalistic environment). Fostering such an environment, where diverse viewpoints can be heard, is a State obligation under human rights law."
- Another key conclusion was that social media companies need to be more transparent, both in terms of the measures they are taking to address hate speech and 'fake news,' and in terms of the effectiveness of those steps. "At the moment, we simply don't know how effective policies such as take downs or labelling are."

Hate speech

- Online expression that incites hatred or violence (hate speech), particularly when directed at already vulnerable or marginalised groups, serves to increase their marginalisation (further excluding them from democratic life), and to polarise democratic discourse.
- Taking the civil and political rights of women as one example, the European Institute for Gender Equality has found (in a 2018 survey) that over half (51%) of young



women in Europe are now too afraid to engage in online debate, especially political debate, because of the often-toxic nature of the discourse. Another survey found that women are 27 times more likely to experience harassment online than men – and that figure increases even further for women of colour.

- "Striking the right balance between fighting hate speech and protecting freedom of expression and opinion," and "distinguishing between harmful content and illegal content" is not easy – for either governments or social media companies. To help, the UN human rights system has issued a range of guidance notes and recommendations to States, including the Rabat Plan of Action. Importantly, these universal human rights norms are also increasingly being taken up by digital technology companies, including social media giants like Facebook and Twitter, and used as the basis of content moderation policies and decisions.
- Beyond grappling with these challenging legal questions, there are a range of practical steps that governments can take – and are taking – to respond to the spread of hate speech online. One is to mobilise civil society, especially young people, to help educate users, catalyse a social rejection of hate speech, and replace it with positive speech. In Norway, for example, the Government supports the 'No Hate Speech' campaign – a youth-led initiative begun by the Council of Europe (and now covering over 40 States). Another example is the Norwegian Youth Council for Freedom of Expression – which seeks to promote freedom of expression and access to information (e.g., by developing educational materials), as a key contribution to mitigating the impacts of hate speech and 'fake news.' A third example is a recent collaboration between the World Jewish Congress, Facebook, and UNESCO: *aboutholocaust.org.* This aims to educate users on anti-Semitism and its consequences.
- Representatives of social media companies agreed that, for the moment, we are perhaps taking a too-narrow and legalistic approach to dealing with challenges such as

‘fake news’ and hate speech. “The debate right now seems to be focused solely on what is and is not permissible speech, and therefore what social media companies can/ should ‘take down.’ This means we are ignoring many other practical solutions that might look at, for example, improving access to accurate information, strengthening social media literacy, improving the diversity of the media landscape.”

- As an example of the power of user awareness-raising and education, as a means of preventing hate speech, Twitter has found that where it tells a user that they have violated its policies, and explains why, in 64% of cases those individuals do not ‘repeat offend.’
- Another approach being taken by some social media companies, like Twitter, is to give power back to users. “The hashtag was originally an idea of one of our users, and so it has continued – we see a huge amount of inspiration and wisdom coming from our userbase. So, we are now making a conscientious effort to give our platform and tools back to those users – so they can better shape their online environment. That includes enabling them to mute, block, and report malign accounts, but also better allowing them to shape their online conversation.”
- Interestingly, experiments like this are also helping to energise civil society (which are routinely consulted on how to create safe civic spaces online) and create “open online public spaces” – “digital town squares” (see ‘roundtable 2,’ below). The link between addressing hate speech and disinformation, creating a safe online space for civil discourse and political debate, and democratic renewal, was also highlighted by numerous civil society representatives in Montreux. Their reasoning was simple: if hateful or false expression serves to dissuade rights-holders from engaging in democratic debate and problem-solving, then making online spaces more open and safer will help encourage people to participate in democratic processes.
- This point also helps to illustrate the potential pitfalls of over-regulation or badly designed regulation. If, for example, new government regulations undermine end-to-end encryption or prohibit anonymous accounts, ostensibly to dissuade users from promoting hate speech, it may in fact risk making the online world less secure for NGOs and human rights defenders, especially in autocratic countries.
- Politicians in some democratic societies (e.g., UK) have recently begun to focus on the issue of anonymity online and have framed this as a root cause – even *the* root cause – of incitement to hatred and violence online. It is important to push-back against this narrative. A recent study, for example, into online hatred levelled at black footballers in England, found that 99% of such content originated from non-anonymous accounts. On the other hand, anonymity is crucial for activists, especially those working in non-democratic settings – allowing them to speak freely and to organise.
- A social media representative confirmed that pushback against anonymity on the part of various democratic governments is a real concern. “We are being asked to gather more and more data on our users, to hold that data for longer, and to hand it over to law enforcement agencies more regularly.” A civil society representative agreed this trend could end up hurting civil society: “upholding end-to-end encryption is just so important for civil society everywhere, but especially for human rights defenders working within authoritarian regimes.”

Disinformation

- As with hate speech online, disinformation has serious negative implications for democracy, in particular by sowing seeds of distrust in democratic institutions and processes (e.g., elections). Recent surveys show increasing levels of popular distrust in democratic politics and politicians. This erosion of trust is both a precondition for, and is further exacerbated by, disinformation.
- This (downward) cyclical relationship between disinformation (and hate speech) and popular trust in democracy means taking deliberate yet careful action must

be a policy priority for democratic governments – including via commitments to be made at the upcoming Summit for Democracy. The need for concerted action is given even greater urgency by the fact that autocracies are both using disinformation at home to tighten control and abroad to weaken the foundations of democratic government.

- On this last point, the past decade has seen the world's major autocracies significantly increase their efforts to use social media to spread disinformation and incite hatred/division in democratic societies, as a way of destabilising those societies and (in the case of new democracies) reversing democratic gains.
- As noted above, one key strategy to mitigate the human rights impacts of disinformation is to incubate a diverse and independent quality media landscape, including local and community media outlets. Moreover, there should be close cooperation between traditional media outlets, social media platforms, and independent fact-checking services. For example, since 2018, the Norwegian fact-checking organisation faktisk.no has been part of Facebook's global third-party fact-checking network.
- The wider issue of digital literacy and 'information literacy' (i.e., developing skills to reflect on and scrutinise information before forming and sharing an opinion on it) is also extremely important, especially as a way of preventing the spread of disinformation and hate speech online. For example, the Norwegian Media Authority has established a national network of civil society organisations and private companies, to improve digital skills and media literacy. "Providing all parts of the population with the skills they need to safely and calmly navigate the internet is key."
- Instead of increasing public access to (accurate) information as a way of counteracting disinformation, authoritarian governments are increasingly adopting the opposite approach – restricting public access to information and curtailing free expression (sometimes under the guise of

anti 'fake news' laws) so as to create a *de facto* monopoly on (dis)information.

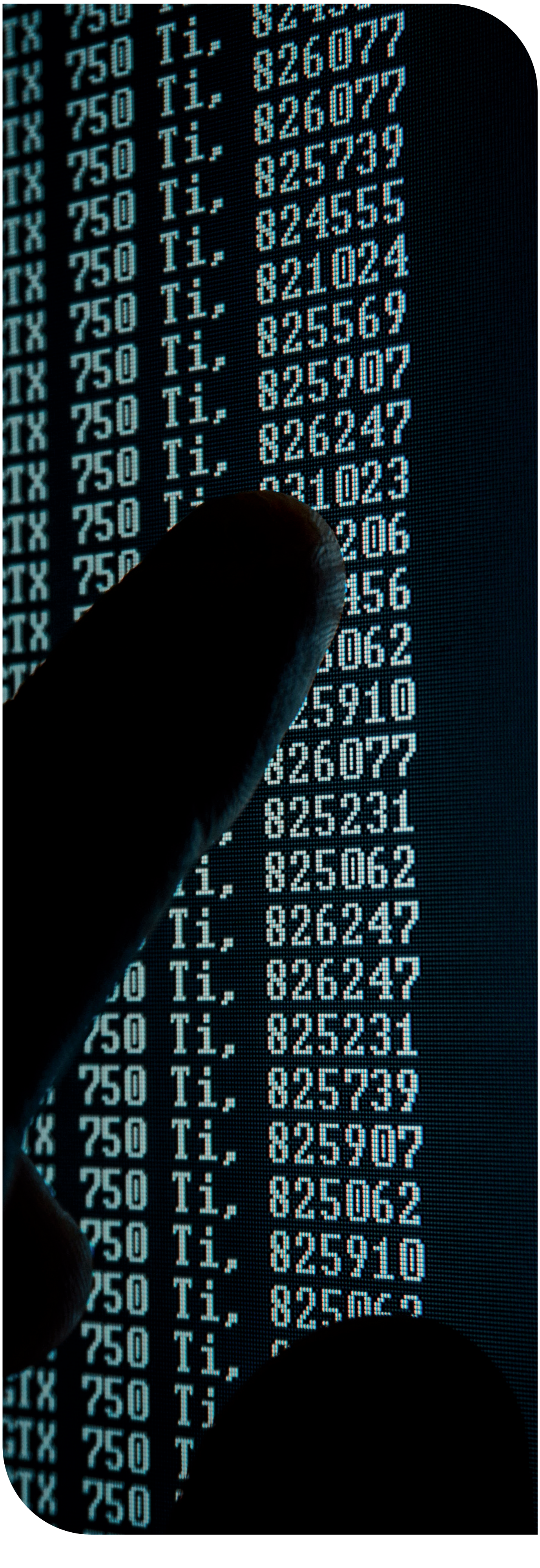
- This last point helps explain the importance, if we are serious about protecting human rights and halting the roll-back of democratic government, of safeguarding "an open, global, free and secure Internet."
- According to a representative of a social media company: "We are willing to play an active role in improving the information ecosystem online, including as a contribution to promoting human rights and democracy, however, there are limits to what we can do in the face of determined authoritarian governments. What's happening online isn't isolated form the offline world, and we can't defend democracy or solve all of society's problems with technology alone."
- It is important to recall that 'official' disinformation is not only a problem in the autocratic world. In democracies too, political leaders (especially populist leaders) including former President Donald Trump in the US and President Jair Bolsonaro in Brazil, have regularly shared information with the public that they knew to be false or misleading (including, in the case of the former, the 'Big Lie' that the 2020 elections was stolen). A recent report from Article 19, a free speech NGO, showed that President Bolsonaro gave 1,682 false or misleading statements in 2020 (so, on average, 4.6 per day). Typically, these attacks on the truth are accompanied by political attacks against any media organisation or journalist that dares expose or contradict such 'official' disinformation, or any social media company that acts (e.g., by 'de-platforming' the politician in question).
- Finally, and adding another layer to this complex picture, independent journalists, and civil society organisations (especially those closely linked to government officials or political parties) can also be important sources of disinformation. The question is, how to address this while at the same time respecting freedom of expression?

Ideas for possible Summit commitments

- Take decisive action to address hate speech and disinformation online (considering the seriousness of the threat to democracy and human rights), but do so through multistakeholder engagement and cooperation, through a mix of regulatory, self-regulatory, co-regulatory and non-regulatory approaches, and be fully guided by international human rights law.
- Mindful that disinformation, especially when authored by governments/elected officials, erodes the basic foundations of democracy, commit to formulating codes of conduct (drafted, for example, by parliaments) on the matter, to be signed by all elected officials when taking office.
- Develop international principles or guidelines at the Human Rights Council (through multi-stakeholder consultations and building on existing work such as the Rabat Plan of Action) on addressing hate speech and disinformation online, while respecting and protecting freedom of expression. This could build on the Council's resolutions on 'digital technologies and human rights' (led by Denmark, Republic of Korea, and others) and a recent Joint Statement on the subject of disinformation, led by Ukraine and sponsored by over 50 States.
- Take steps to improve the wider national "information and communication eco-system," including by improving access to accurate information; strengthening digital literacy, 'information literacy,' and social media literacy; and improving the diversity of the media landscape, including local and community media outlets.
- Mobilise civil society, especially young people, to help educate users, catalyse a social rejection of hate, and replace it with positive speech.
- Adopt a gender perspective when seeking to understand and regulate challenges to human rights and democracy in the digital world.
- Protect encryption and anonymity on social media, especially in view of growing pressures on civil society and human rights defenders in autocratic regimes.
- Social media companies should improve transparency, both in terms of the measures they are taking to address hate speech and 'fake news,' and in terms of the effectiveness of those steps.

Roundtable 2

BOOSTING DEMOCRATIC PARTICIPATION BY FIGHTING DISCRIMINATION AND EXCLUSION; REINVIGORATING AND SAFEGUARDING CIVIL SOCIETY SPACE IN THE DIGITAL WORLD

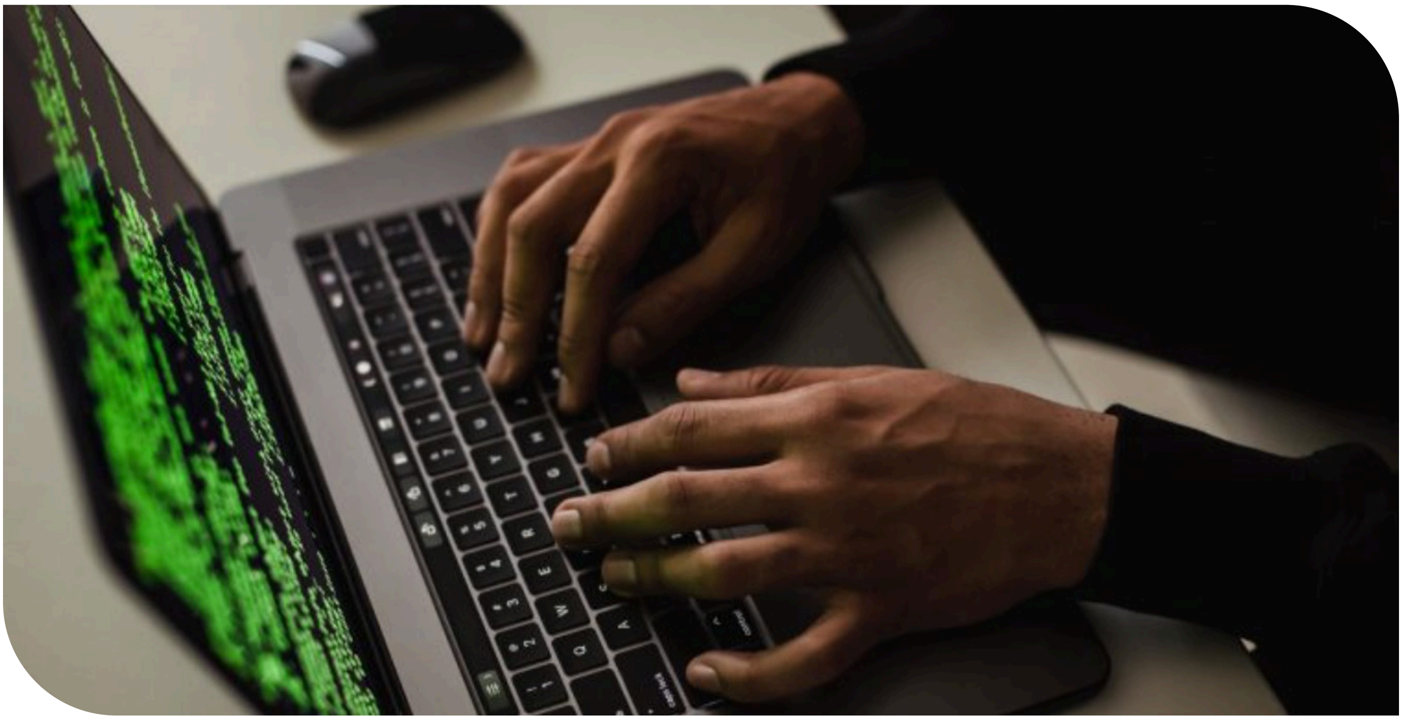


The aims of roundtable 2 were threefold. First, to consider how the Internet has been used, by domestic and foreign actors, to 'game' democracy by supressing the participation of already marginalised groups, and what governments and other stakeholders should do in response. Second, to consider the impacts of the Internet and social media on civic space and democratic debate/discourse, and to identify ways to reimagine digital technology as a tool for revitalising civil society. Lastly, the roundtable aimed to take stock of the growing trend, especially in autocratic States, of manipulating/fragmenting the Internet and digital technology to restrict civic space and stifle dissent.

Key conclusions

- “The key point, as we consider the interplay of digital technology, democracy and human rights, is that – whether we are talking about autocracies or democracies – it is fundamentally intertwined with issues of politics, money and power.” Even in well-established democracies, essential institutions and processes are often captured by vested interests. Where digital technology helps further those interests, it is welcomed. Where it is used to hold them to account, it is denounced – as are those who use it, including civil society and journalists.
- Political-economic elites have very little interest, therefore, in driving meaningful change. The story of the role of Cambridge Analytica in the Brexit referendum is a case in point. Because those who won that referendum are in power, there is no real appetite to look at issues such as disinformation and micro-targeting, and how this may have undermined the integrity of the vote. There is even less interest in regulating to prevent such things from happening again.
- “There are those in society who have given up on the Internet. Parents, for example, who understandably want to keep their children away from social media because it may damage them or radicalise them. Yet, the Internet is neither inherently bad nor good – it is neutral. If we want a better online world, we need to actively participate in it.”
- The same broad point was made about civil society participation. “It is clear that the Internet and social media are currently not ‘safe’ for civil society. Yet, at the same time, we have to recognise that there is no alternative for civil society – for people who want to engage with their governments and participate in democracy - than to be active online.”
- “A key goal must be to educate the billions of people who use the Internet every day on how to engage with the online world - how to engage with one another, how to talk to one another, how to avoid the types of language that lead to division and a coarsening of public discourse, and prevent us from understanding one another.” “There is a tendency to think that digital technology is causing all of our problems, and thus that solutions must focus on that same technology. Yet good discourse, good communication is, in the end, a human, not a technological proposition.”

- “That is not to say that technology companies aren’t part of the problem. They are. Their algorithms reinforce our biases, their platforms amplify our worst instincts.” Rather, it is to point out that if we want to strengthen democracy in the digital age, we cannot focus narrowly on, for example, algorithms. We must look more holistically at the entire civic environment.
- Therefore, if we want to strengthen civic participation and civil discourse online, as a means of strengthening democracy, we should think outside the box, and find innovative ways to build ‘digital public squares’ or ‘digital town halls’ that promote dialogue, understanding and consensus-building.
- This also means a greater focus on civic education online. What does it mean to be a citizen of a democracy in the digital age? What are the rights and responsibilities of ‘digital citizens’?
- Others agreed with this reading. “In principle, the Internet and social media can and should be an enormous boon for democratic participation. They allow us to engage with candidates and our elected representatives, to participate in political debates, and to hold those in power to account, in ways that would have been unimaginable only two decades ago.” Yet we must not be blind to the fact that things have not turned out that way.”
- One speaker proposed a three-part course of action. First, democratic States need to set the essential guardrails (nationally but also internationally – at the UN) within which social media platforms operate, to ensure that the online world is safe for civil society. Where companies stray beyond those guardrails, States should hold them accountable. Second, “social media companies need to take a long hard look at themselves, and whether the way they operate at the moment is conducive to civic participation and civil discourse.” Third, States and civil society should encourage “alternatives” – “it is not enough for us to criticise existing options, we need to come up with alternative platforms that are more rights-respecting, more inclusive, more secure, and that foster dialogue and understanding.”
- Regarding the first part of this plan of action, it was noted repeatedly during the dialogue in Montreux that setting guardrails that respect and protect human rights is not an *option* for States, it is an *obligation* under international law. Where States do not regulate companies in a way that protects us all from harm, they are failing to meet those human rights obligations.
- The above points mainly refer to what is happening, and what needs to happen, in democratic societies. But it is important to recognise that many governments “are



actively trying to close down civic space, to use technology and the regulation of technology to attack civil society and stifle dissent."

- Just as there are different kinds of States, so there are different kinds of companies. Some are keen to engage on questions of human rights and democracy. Others, such as Google, are not. There are also different types of digital technology companies. Much of our focus is on social media companies – but there are many others working in different areas of digital technology whose operations have enormous implications for human rights and democracy.
- A further human rights concern is the gender dimension of attacks against civil society online. Such attacks are disproportionately severe for women – which in turn undermines democracy by deterring over half of the population from participating.
- One speaker proposed a two-dimensional response to these challenges: "keeping the Internet on and keeping it safe."
- Regarding the latter, "we need to combat and push back on oppressive legislation. We know that much of the national legislation currently being developed is overbroad and vague and will be misused." This is being done deliberately in powerful autocratic States. But elsewhere, especially in the developing world, it is often inadvertent. This places a particular responsibility on developed democracies with strong rule of law systems (e.g., EU member States). The second point under 'keeping it safe' is the importance of regulatory transparency, accountability, and remedy. This is more than a procedural nicety: we need to know what is happening online (e.g., "the character of attacks, who is performing them") so that interventions can be properly designed to keep civic space open. Third, "we need to expand our efforts to protect and support civic space." This means breaking down the now artificial divide between human rights defenders and journalists – in the digital world, they can be, and often are, one and the same; it means democratic States and digital technology companies backing each other up in defending civic space in repressive environments; it means (on the part of States and companies) providing civil society in such environments with more 'digital support' to undertake their work effectively and safely; and it means defending encryption and anonymity, even if that means we will never be able to completely eradicate hate speech in democratic societies.
- Regarding 'keeping it on,' democratic States should engage more, and in a more systematic way, on

the issue of Internet shutdowns. “At the moment, we are failing on this front.” That means agreeing international standards that apply to shutdowns (necessity, proportionality, etc.). Companies should also do more, both to legally challenge shutdowns, and to update the public about what is happening.

- Linked with the above, in September 2021, Facebook, Twitter, Amazon, and Microsoft, together with various civil society actors, issued a joint letter expressing concern about the growing threat of ‘Internet fragmentation,’ caused by, *inter alia*, the expansion of the ‘surveillance State’ - ubiquitous data collection systems, including biometric surveillance, powered by artificial intelligence (AI) and algorithmic decision-making; more ‘traditional’ methods of repression and social control such as Internet shutdowns and other network disruptions; and an increasing use of ‘next generation repression toolkits’ such as State-sponsored hacking or online harassment campaigns. Such developments, the signatories argued, pose a significant threat to human rights and democracy.

- Several other participants in Montreux also underscored the enormous threat to human rights and democracy posed by the growth of the surveillance State, and the export of “digital technology solutions that enable governments to target civil society.” “There is a danger,” according to one speaker, “that while we sit here talking about the finer points of platform governance, various autocratic States are sharing technologies and know-how with governments around the world that could undermine everything we – and the Summit for Democracy – are trying to achieve.”

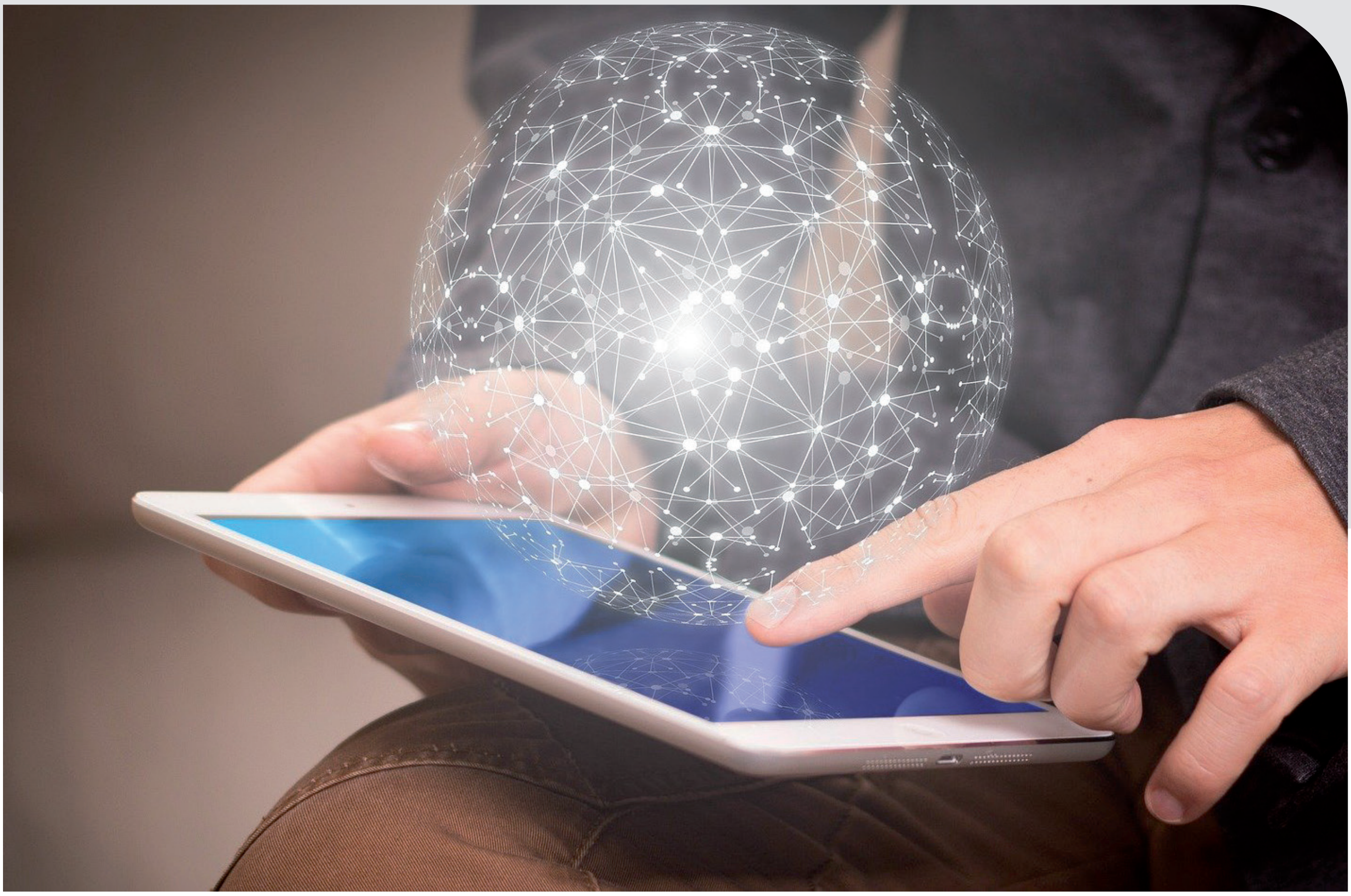
- As the struggle goes on between those States that believe digital technology should be placed at the service of human rights, and those that see technology as an efficient way of supressing rights and maintaining control, several State representatives working on internet governance urged participants to look beyond the Human Rights Council, especially in the direction of the International Telecommunications Union (ITU) – “the most important UN organisation you’ve probably never heard of.”

Ideas for possible Summit commitments

- Fulfil States' obligations under international law to promote freedoms of expression, association, and assembly, and protect civil society space, by setting the essential regulatory guardrails within which social media platforms must operate.
- Avoid 'over-regulation' or 'bad regulation.' "Much national legislation currently being developed is overly broad and vague and risks being misused or copied" either in democratic or autocratic States.
- Instead, (and as noted above), adopt a holistic approach, including through non-regulatory measures such as boosting digital civic education - how to behave towards others in the digital world, what does it mean to be a citizen of a democracy in the digital age, and what are the rights and responsibilities of 'digital citizens'?
- Strengthen information literacy and social media literacy to educate the billions of people who use the Internet every day on how to engage with the online world: how to engage with one another, how to talk to one another, how to avoid the types of language that lead to division and a coarsening of public discourse and prevent us from understanding one another?
- Social media companies should reflect on whether the way they currently operate is conducive to civic participation and civil discourse, and what more could be done to create safe and inclusive 'civic spaces' on their platforms, as a contribution to participatory democracy.
- States and civil society should encourage "alternatives" to the social media platforms that

are “more rights-respecting, more inclusive, more secure, and that foster dialogue, understanding and consensus-building,” for example, by building “digital public squares or ‘digital town halls.”

- Democratic States and digital technology companies should “back each other up” in defending civic space in repressive environments, for example, by providing civil society in such environments with more ‘digital support’ to undertake their work effectively and safely.
- Defend encryption and anonymity, which are crucial for civil society in autocratic systems, even if it makes tackling problems such as hate speech online more difficult in democratic societies.
- Engage more, and in a more systematic way, on the issue of Internet shutdowns, including by agreeing international standards on shutdowns (covering necessity, proportionality, etc.).
- Digital technology companies should also do more, both by legally challenging shutdowns and by updating the public about what is happening.
- Use international forums like the UN to call out attacks against human rights online (within and by autocratic States), with as much force as attacks against human rights offline. This should include regular debates at the Human Rights Council about the human rights consequences of the ‘surveillance State,’ Internet shutdowns and other network disruptions, and State-sponsored hacking or online harassment campaigns.

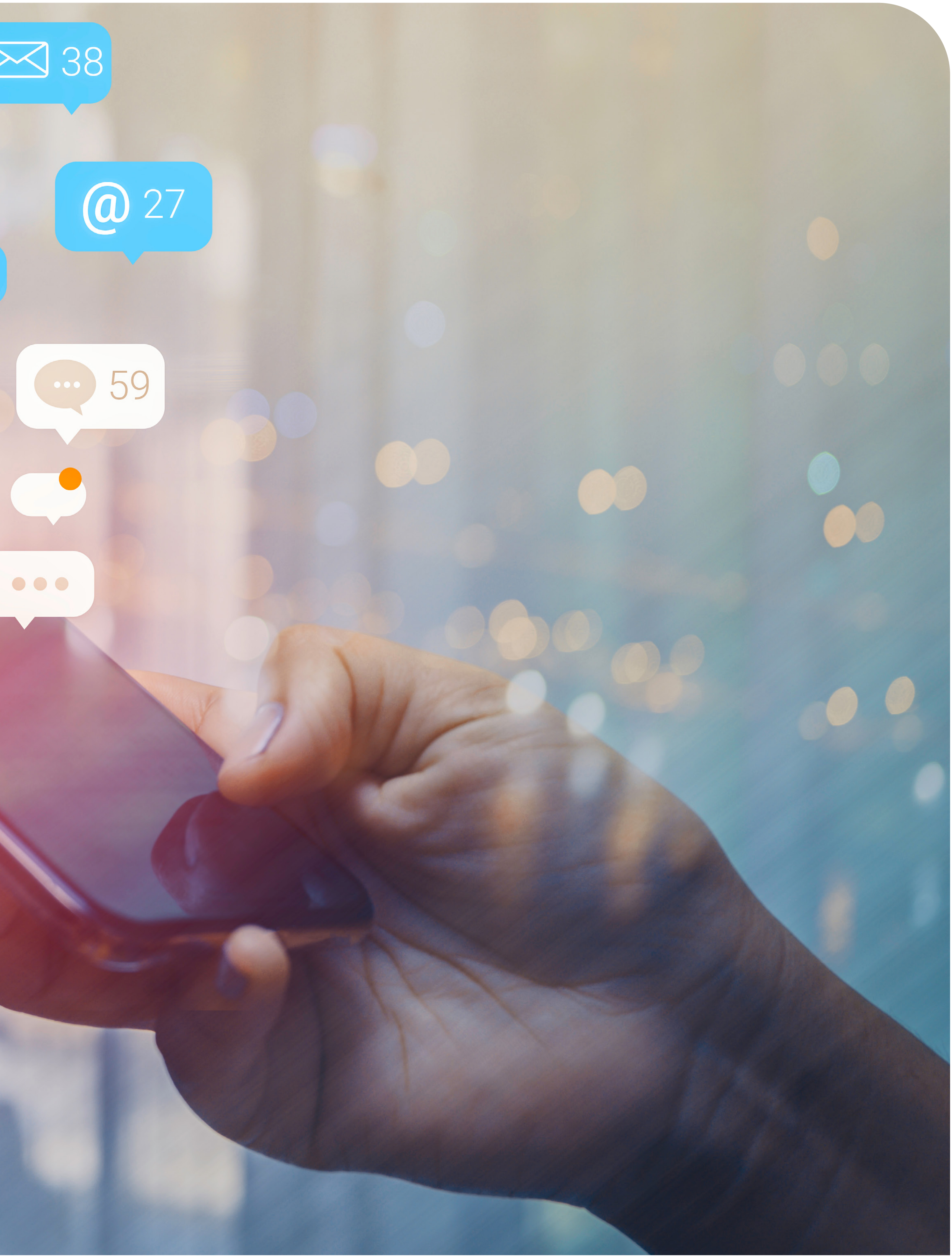


GAFAM
amazon
Faceb
Amazon
Google
Microso
Apple

Roundtable 3

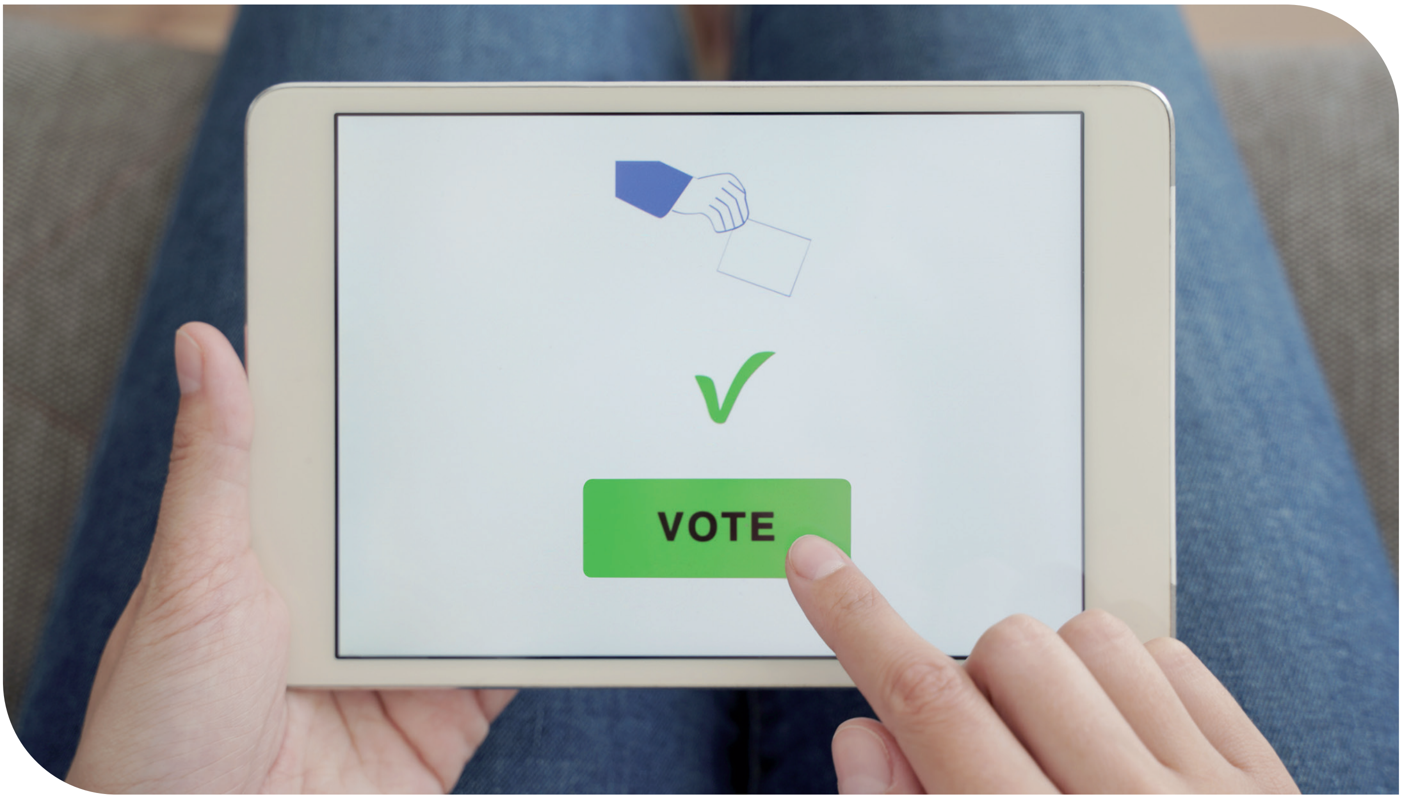
PLACING DIGITAL TECHNOLOGY AT THE SERVICE OF FREE AND FAIR ELECTIONS

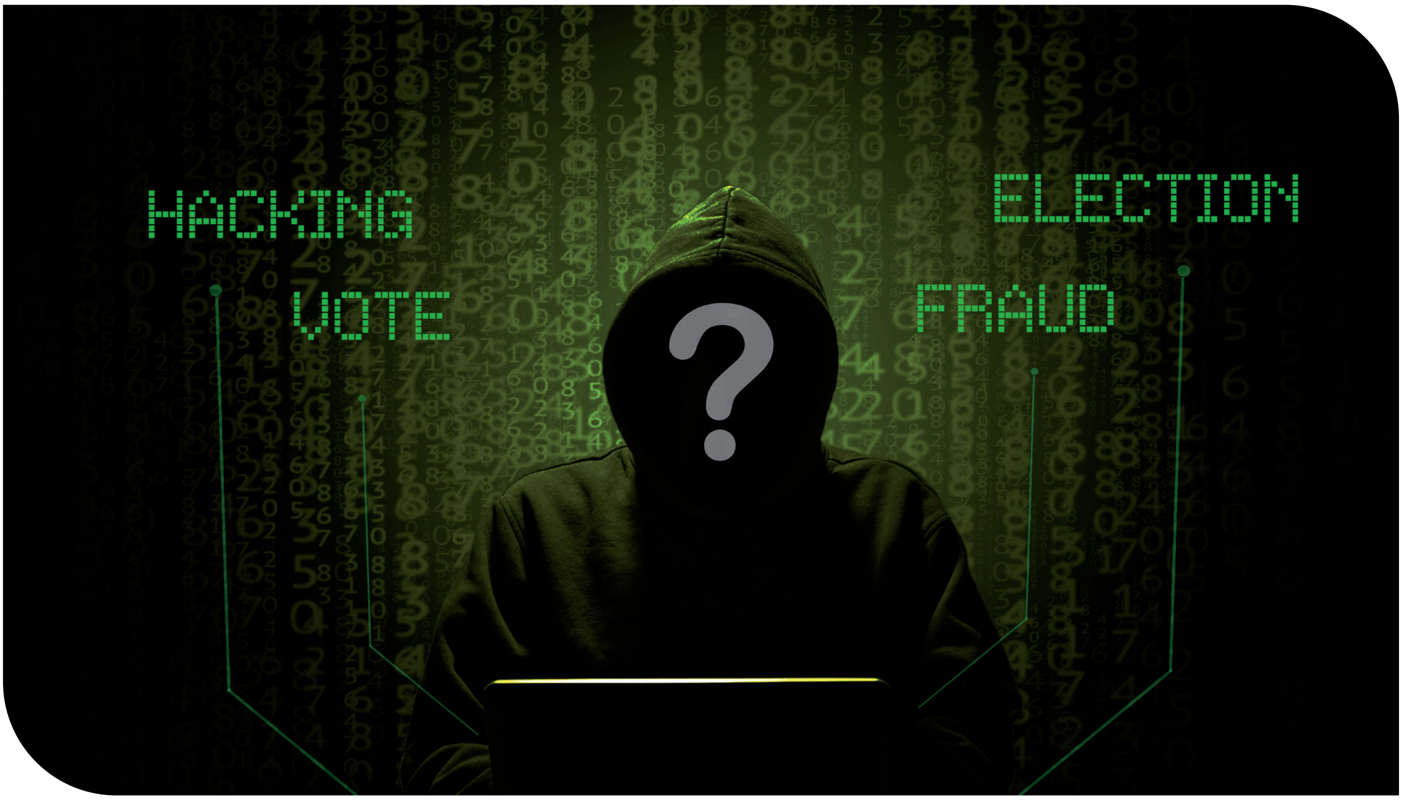
This roundtable discussion aimed to shed light upon key questions related to the use of digital technologies in elections, looking at both negative and positive implications thereof, and to identify concrete recommendations for participating States at the Summit for Democracy. The discussion took a broad view of the role of technology and how it can be put at the service of free and fair elections, by considering the implications of different technologies, and their regulatory contexts, for the achievement of free and fair elections, and for strengthening public trust in the vote outcomes.


38
@ 27
59

Key conclusions

- Many countries have taken steps to integrate digital technology into national election systems – with different levels of success. While some have persevered, others have 'rowed back' once it became clear that insufficient public trust in technology solutions risked undermining their faith in the integrity of elections and in democracy.
- One country where there has certainly been no 'rowing back' is Estonia, where digital democracy, as well as the digitalisation of other key aspects of society, has become the new normal. While there are some historical reasons for the country's firm embrace of digital technology (for example, the USSR's Cybernetics Institute was based there), and perhaps some cultural reasons, "the most important word is trust." In other words, "people have trust in our system of government – and are thus happy to accept digitalisation, even in a sensitive area like democratic elections."
- Today, Estonia is a digital society, where more than 3,000 public services (99% of the total – the exceptions being marriage and divorce) are available online. Moreover, this has been achieved with high levels of transparency and data protection. Around 99% of all residents have a digital ID card, which grants easy and secure access to all e-services, including democratic 'services' such as Internet voting, petitioning, and participative budgeting.
- High levels of transparency and data protection are crucial for public trust in Estonia's digital society. The individual citizen is the sole owner of his or her personal data – not the government and not any private company. This fact is guaranteed by the Constitution. Practically speaking, this means that there is no one government department or agency (except for the security services, in exceptional circumstances) that stores or otherwise has access to *all* personal data. On the other hand, because all personal data is tracked, every individual can, at any time, know exactly what data is being collected and held about him or her.
- "Since 2005, Internet voting has become the norm in local, parliamentary, and European elections". The citizen uses his or her digital ID card to vote, but the identity of





the voter is then removed from the electronic ballot before it reaches the national election commission for counting – thereby ensuring confidentiality. The voter can use a QR code to verify whether the vote was successfully cast, and the ballot counted (again, building trust in the process). "Internet voting, and digital democracy in a broader sense, bring people closer to decision-making, and help boost political participation and civic engagement."

- Other parts of Europe have enjoyed less success. "On several occasions, the technology failed us. On others, people lost trust in the technology," noted one representative of a European intergovernmental organisation. "How to push forward this agenda once again?" he asked. "Unfortunately, at the moment, we don't have an answer to that question."
- "For a long time, when we spoke about using technology to strengthen elections, we were essentially talking about introducing, for example, electronic voting, electronic voting machines (EVMs) or Internet voting, to improve efficiency and transparency." Experience showed the integration of digital technology in these ways to have several advantages, including making voting easier, especially for citizens living abroad (though, surprisingly, technology did not really help boost voter turnout), improving the accuracy of counting, and strengthening the process of tabulating results. "However, in the end, such benefits counted for little in the absence of public trust."
- In that regard, European States seem to be caught in a catch-22 situation. Technology is, in principle, a good way of building trust in election processes, but to integrate technology into those processes, one needs public trust (in the government, in the electoral process, and in the technology). As a result, organisations like OSCE recommend that "where there is already public mistrust in the electoral process," States should avoid introducing new variables like technology.
- It is also the case that there is "room for improvement in election technology." Elections should incorporate key democratic principles such as universality, equality, integrity of results, transparency, and accountability. For now, however, "there are no e-voting systems that satisfy all these criteria." As a result, together with the (critical) issue

of a lack of public trust, "we simply do not have enough to offer people to convince them that the outcome of the election will be an accurate reflection of the votes they have cast."

- As with the first two roundtables, a key overall conclusion is therefore that it is impossible – and somewhat meaningless – to separate the online world from the offline world. In other words, just as technology is only *part* of the problem when it comes to free and fair elections, so it can only ever be *part* of the solution – "it is not a magic bullet." The key issue is public confidence in democracy, in the government, and in the overall electoral process. Where such confidence exists, technology can be introduced to strengthen democratic polls (e.g., Estonia, Switzerland[1]). Where it does not exist, "technology cannot magic it into existence."
- As the foregoing suggests, placing digital technology at the service of free and fair elections is partly about the *willingness* of citizens and governments to embrace digital democracy; but it is also about the *capacity* of States to do so. "Sadly, the digital divide is very real for the peoples of the global South," said one speaker. Many developing countries, for example, in Africa, simply do not have the capacity to establish digital election systems/ Internet voting. Moreover, *within* developing countries, unequal access to the Internet and digital technology (for example, between urban and rural areas) also makes the wide roll-out of digital technology in elections highly impractical.
- So, there are difference between the developed and developing world. But there are also similarities – in both cases, public trust is critical. In Africa, the wave of democratisation in the 1990s has, in many cases, given way to democratic backsliding, as leaders try to establish autocratic systems behind a veneer of democracy. This has naturally knocked popular faith in democratic institutions and processes. Against such a background, the integration of digital technology solutions into national election systems would likely erode, rather than enhance, trust in the voting process and result.

[1] Though, in the case of Switzerland, the Government eventually went back to more traditional voting methods due to concerns over the integrity and security of digital solutions.

- Linked with this point, it is important to ask the question: "Who is building and who owns Africa's digital infrastructure? The answer, increasingly, is China, and, with it, China is promoting a certain type of digital governance." Again, this impacts on trust: voters would, understandably, be worried about who would have access to their data – including which candidate they voted for.
- Another challenge for developing countries is that digital technology moves very fast – far faster than the election laws and infrastructure. This reduces the likelihood of national election systems, which are often already under strain, being able to cope with technological advance and thus ensure free, fair, and digitally secure votes. Digital campaigning and campaign financing offer but two examples of where national elections laws, for example in Africa, are already struggling to cope (as they are in many developed countries). "Thus, the introduction of further digital technology solutions (e.g., EVMs or Internet voting) seems especially far-fetched."
- There are examples in Africa of EVMs being mobilised in national elections. Namibia is one. However, even here, it was not easy. Trust, as always, was an issue. Do people trust the government to pass the right legislation? Do they trust the election commission to use the technology correctly, and to keep their ballot secret?
- While there are very few successful examples of technology being mobilised in developing countries to facilitate/improve voting procedures, there are examples (e.g., the Maldives) of technology being mobilised to increase transparency – and public trust – in vote counting and vote tabulation.
- Several speakers from Africa, Asia, and Latin America, made a plea for international technical support to help developing countries review, revise and strengthen national electoral laws, processes, and institutions, so that they are "fit for purpose in the digital age." They argued that, despite setbacks, the internet and digital technology still hold out enormous hope: hope for more inclusive, transparent, and secure elections, and for a more level playing field for all candidates (irrespective of background).

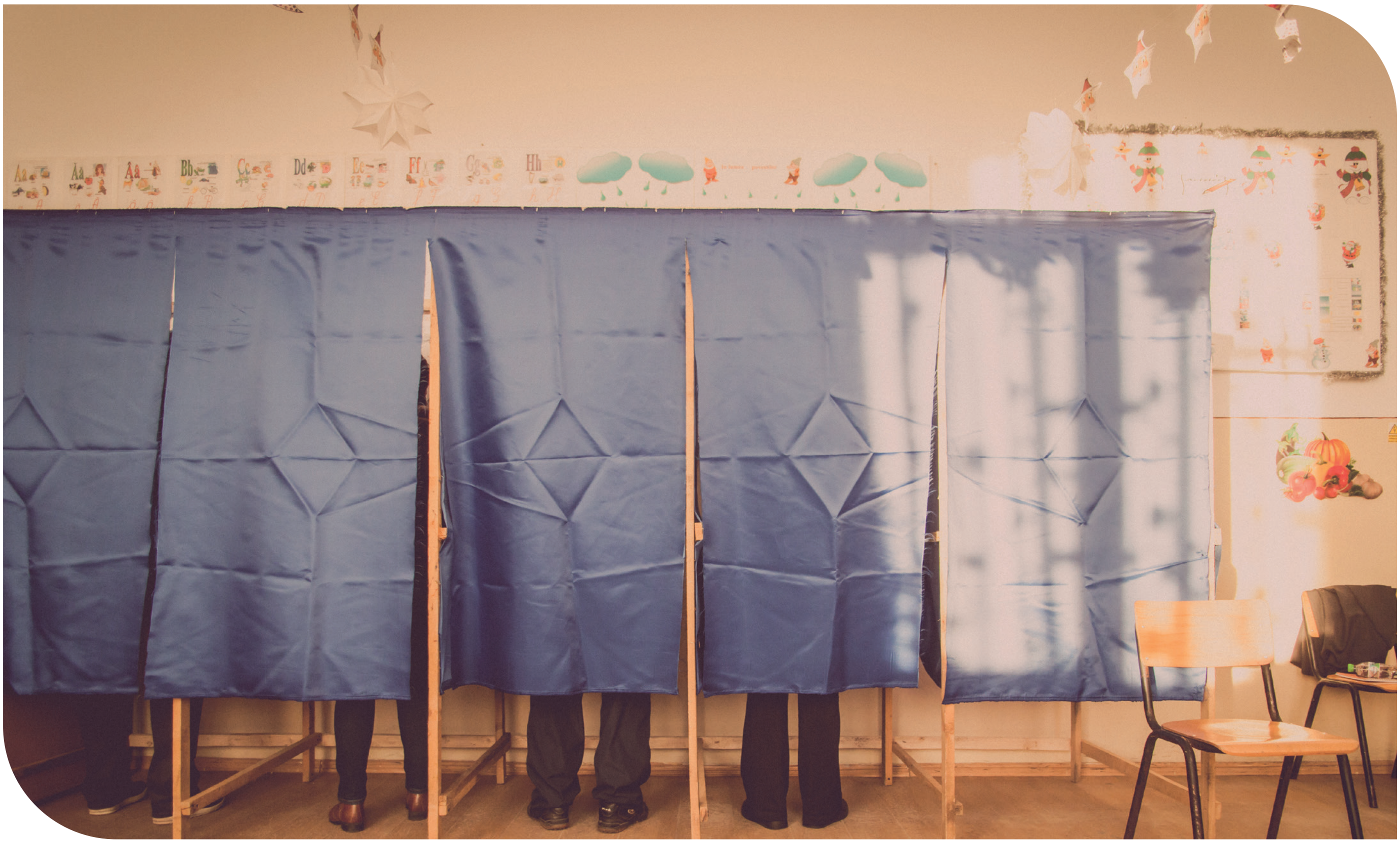
- Regarding the latter point, a key aspect of national electoral reform must be to bring changes to campaign finance laws. "At present, money in politics is usually wielded by incumbent parties or the existing political-economic elites to maintain their grip on power. They use loopholes in campaign finance laws to swamp the Internet with messaging. If this situation could be brought under control, it would offer an enormous boon to smaller parties and independent candidates (e.g., anti-corruption candidates) because, in principle, the Internet and social media are a great equaliser in terms of running effective campaigns at relatively low cost."
- For their part, digital technology companies like Facebook/Meta are keenly – and increasingly – conscious that elections are times of heightened social tension and human rights risk, and that they have a particular responsibility at such moments to take steps to reduce tension and mitigate risk. Steps being taken include, for example:

  I. Preventing interference in elections by cracking down on fake accounts, and disrupting 'bad actors' – i.e., those (foreign or domestic) seeking to run coordinated 'information operations' to undermine the integrity of elections. Facebook reports that, since 2017, it has removed over 150 'info-op' networks across 50 countries, which were seeking to manipulate public debate and/or voting.

  II. Removing harmful content, including disinformation designed to confuse voters (e.g., giving incorrect information about where, when, or how to vote), as well as other disinformation, for example about public health measures during the pandemic (Facebook now has factcheckers in 60 countries covering over 70 languages).

  III. Increased transparency to support an informed society.

- Facebook/Meta has noted, over recent years, that 'info-ops' designed to undermine democracy are also, increasingly, targeting human rights defenders and civil society. These campaigns of coordinated harassment (known as 'brigading') aim to silence dissent and reduce civic discourse, especially during elections.



Ideas for possible Summit commitments

- Strengthen national 'digital defences' to protect the integrity of democratic elections.
- Review and revise electoral laws, including campaigning rules and campaign financing rules, to make them fit-for-purpose for the digital age. All such reform efforts must be comprehensive in nature, reflecting the need to adopt a holistic approach to elections, with digital technology just one – albeit important – part of the picture. The goal of updated legal and institutional frameworks must be to build public trust in elections and democracy – including the digital component.
- The challenges and opportunities posed by digital technology in the context of elections and democracy are not restricted to Europe or the US. They are also very real for developing country democracies. Thus, the international community should provide technical assistance and capacity building support to help democracies in the global South to also update and strengthen electoral laws and bodies for the digital age.
- Replicate good practice from those democratic States, including new democratic States, that have leveraged digital technology to increase transparency (and thus public trust) in vote counting and vote tabulation.
- Draft and share a 'model law' on elections and technology, to act as a template and inspiration for necessary legislative reforms in Africa, Asia and Latin America.
- Invest in civic education and civil society in developing country democracies, so that they are trained and equipped to ensure that governments place technology at the service of free and fair elections, and can themselves leverage digital technology to make elections more transparent and credible.
- Social media companies, and other digital technology companies, should scale-up their efforts, working in cooperation with relevant government agencies, to prevent interference in elections by cracking down on fake accounts, disrupting 'bad actors' (foreign or domestic) seeking to run coordinated 'information operations' (info-ops), and removing content designed to confuse voters (e.g., giving incorrect information about where, when, or how to vote).
- Social media companies should also scale-up their efforts to disrupt coordination info-op campaigns targeting human rights defenders and civil society (i.e., 'brigading'), especially during election periods.

Christine Löw,
Deputy Head of Division, Peace and Human Rights Division, Federal Department of Foreign Affairs, Switzerland

"Human rights challenges in the online world cannot be divorced from human rights challenges in the offline world. As it has become clear over the past two days, we must consider how to turn things around so that digital technology is placed at the service of democracy. We must take a comprehensive approach covering improvements in the real world as well as improvements in the digital world. This may include, for example, supporting a diverse media, empowering civil society to 'fact check,' promoting civil discourse, and strengthening the integrity of national election systems [...]"

"Furthermore, in searching for these solutions, whether they be through regulation, self-regulation, or co-regulation, we must adopt a multi-stakeholder approach and, importantly, an inclusive approach – including with the full involvement of women."

"If we are to truly place digital technology at the service of democracy, we must follow a human rights-based approach, both to effectively address threats (e.g., Internet shutdowns, surveillance technology) and challenges (e.g., hate speech and 'fake news'), and to mobilise the Internet and digital technology to re-energise democracy and rebuild public faith in democratic institutions and processes."