National Endowment for Democracy
Supporting freedom around the world

forum
International Forum for Democratic Studies

FORUM Q&A: VIDUSHI MARDA ON CIVIL SOCIETY, ARTIFICIAL INTELLIGENCE, AND THE FUTURE OF FREE EXPRESSION

Vidushi Marda is a legal researcher interested in the interplay between emerging technologies, policy, and society. Currently a Digital Programme Officer with ARTICLE 19's Team Digital, her primary focus is on the ethical, legal, and regulatory issues that arise from algorithmic decision making. She also works on strengthening human rights considerations in internet infrastructure, particularly at internet governance bodies like ICANN and the IEEE. Additionally, she is a research associate at DATACTIVE at the University of Amsterdam, where she studies content regulation vis-a-vis increased dominance of private platforms on the Internet. Marda previously worked at The Centre for Internet and Society, where she focused on access to knowledge, network neutrality, big data, and strengthening freedom of expression and privacy in Internet governance. Her work has been cited by the Supreme Court of India in a seminal ruling on the right to privacy and by the United Kingdom House of Lords Select Committee on Artificial Intelligence. She has been interviewed by the BBC, Economic Times, CNN-News18, and other outlets.

Rapid advances in computer technology and the proliferation of "big data" have enabled the development of sophisticated new statistical models capable of making large-scale inferences about the human world. The resulting use of iterative machine learning, or artificial intelligence (AI), has profound implications for the future of democracy, politics, and human rights—particularly the rights to privacy and free expression. The use of artificial intelligence to influence decisions of consequence for average citizens is already a reality in many countries, and is on track to become more prevalent with time. The application of this technology for mass censorship and surveillance is around the corner. Meanwhile, agreed-upon norms and standards around its use are lacking.

Dean Jackson spoke with Vidushi Marda about Article 19's new report, "Privacy and Freedom of Expression In the Age of Artificial Intelligence," for which she served as the primary author. The report makes several suggestions for how civil society can best contribute to the development of a human rights-conscious framework for AI technology. (This interview has been condensed and edited for clarity. The views and opinions expressed within do not necessarily reflect those of the National Endowment for Democracy.)

Dean Jackson: Many people think of AI as a fantastic future technology, but your report makes clear that it is already in use and intersecting with human rights. How might citizens encounter AI in their everyday lives?

Vidushi Marda: The truth is that AI is already a mundane part of everyday life. For example, AI systems are responsible for autocorrect on cellphones, they decide which advertisements you see on platforms like Facebook and Instagram, and they curate your Facebook and Twitter feed. Depending on where you are in the world, AI may aid with criminal sentencing, estimate how likely you are to commit a future crime, identify your face in a crowd, or decide if you are a trustworthy loan applicant.

In fact, AI as a body of work and as field of study has existed for over half a century. Machine learning, or the use of large amounts of data to make statistical inferences, is the most popular AI technique used today and has been practiced for many years.

What's new is that now we have more data, and computers are faster and cheaper than they have ever been before. This has led to the current moment in AI's development, but it is wrong to think of it as a new technology. Its widespread use and application is current and emerging.

The report outlines two broad categories of human rights concerns: those arising from the collection of data, and those arising from the application of that data through AI. Can you describe the implications for rights to privacy and free expression?

It is not just about data collection, but *how* that data is trained, which then informs how it is applied. For example, what are the design choices being made by the algorithm's designers? If you're looking to assess certain types of speech on social media—and governments around the world are increasingly using sentiment analysis tools to ascertain the public mood—you have to tell the computer to look for something. Is that something a particular name, gender, race, or religion? The wide application of this technique creates a chilling effect on speech: if you know you are being watched, you alter your behavior accordingly.

Second, data collection is opaque to individuals. At the time of data collection, there is inequity of information between people who are data subjects and people who are processing that data. To give you an example, new AI applications claim to be able to predict your mood based on the way you type. The user has no control over the application of this technology despite its profound impact on their privacy: not only is data being collected and assumed about users, it's being used to profile them. So your mood can become part of your insurance assessment, or your credit scoring assessment, or other important metrics. The problem isn't just data collection; it's also profiling. The implications for privacy and freedom of expression here are profound. What's worse, there is very little opportunity to appeal because users may not even know it is happening.

Thinking about this as a model, the first choice is the design choice, then comes the data collection, and after that the statistical models based on that data and the chosen design. Do the designers consider human implications before the model is applied? Often, this decision-making process is completely opaque and asymmetric. There are few opportunities to detect or appeal it.

So there's a need for greater transparency around those kinds of applications?

When people talk about transparency and AI, they often focus on the transparency of the model and the transparency of the algorithm, but I'm also interested in transparency of application. When it comes to things like speech, if we're talking about Facebook and the newsfeed, for example, how do I know what I'm not seeing?

I use the terms opacity not only to refer to the data collection, profiling, statistical analysis, and assumptions made about individuals, but also to a more basic question: when is AI being used and when are these statistical inferences being applied to me? If I'm using Facebook one day and I apply for a loan the next, is there any explanation for whether or how my data from yesterday becomes a deciding factor in my fate today? Beyond this, pushing for greater transparency is important, but not always desirable or even possible. Pushing for intelligibility, scrutability, and explainability helps us get closer to accountability.

The report highlights the risk that the private sector will develop AI-driven censorship tools in response to public pressure to police hate speech and online extremism; however, Chinese state-affiliated companies are already poised to market AI-enhanced mass surveillance and censorship around the world. How can or should civil society respond to this challenge?

This is very much in line with the culture of thinking about development of AI as a race. There is a great amount of fear that new AI systems will be developed and applied with terrible consequences in one place and then spread to other places as other governments or companies feel pressure to apply it in the same way.

Some instances of this are inevitable. We see an emerging trend of using AI to curb hate speech and fix misinformation, but I also think it is more productive to step back and ask if the application of technology was a good one in the first place. In the debate over AI's impact on democracy, there is a tendency to take the effectiveness and application of AI techniques as a given, but we should be asking simpler questions: *should* a given technique be applied? Is it even effective? AI models are often so imperfect that they can be detrimental not only to human rights, but to their developers' objectives. And AI can be used for great things and for terrible things depending on the design choices developers make and the data they use.

More so than worrying about the development of AI technology, civil society should work to minimize applications of AI that are detrimental to human rights and civil liberties. One way of doing this is through standard-setting organizations like the Institute of Electrical and Electronics Engineers (IEEE), which developed the Wi-Fi standard, among others. Another is by ensuring that the legal and policy environment within which AI systems function have adequate safeguards.

Data privacy is an area of increasing concern, with many in democracies calling for a consumer right to opt out of data collection. In the future, how conceivable will it be to opt out of AI's growing role in human life?

The unfortunate truth is that we have very little say in how our data is used currently, and that must change. Every time I do a Google search, I have no idea how many people are collecting that data. Every time I see a Facebook widget on a website, I have no idea what information it is collecting about me. Even if I'm not a Facebook user, Facebook can create a shadow profile of me. This goes back to the asymmetry problem: there's no way of appealing the use of this data until it's too late. We do have the European Union's General Data Protection Regulation, which came into force in May 2018 and which has an higher standards for knowledge of, and consent to data collection, but I'm not sure what anyone can do once your data is already in any particular system or is already publicly available and ready to be harvested.

So, unfortunately, I doubt it will be possible to "opt-out" in the future, unless we see radical shifts across stakeholder groups. There isn't much you can do, for example, when your anonymity in a public space is completely broken because facial recognition software can identify you, access publicly available data on you, and then use that data to infer sensitive information about you.

There are now many jurisdictions that distinguish between types of data, especially personal data. In India, for example, there is a provision in the current Information Technology Act that talks about sensitive personal data and what you can do in the case that sensitive personal data is leaked or hacked; but AI challenges such safeguards. It can take publicly available data and use it to extract more sensitive data about you, and that process is beyond your control.

Because technology moves much quicker than law and is much more inscrutable, we need to figure out a way to make technology human rights respecting by design. Otherwise, society is never going to keep up with it through legal rulings or monetary fines.

Has civil society been succeeding in framing the debate and setting priorities in the international arena? Why or why not?

A big barrier to civil society engagement in this area has been that the effects are to a large extent unknown. In meetings, whether with the government, the private sector, or other civil society organizations, one of the first problems that comes up is "we don't have enough evidence." When you don't have enough evidence, you don't know what you're up against. So for example, people can be worried about the use of AI in Malaysia, but unless

you have evidence of exactly how it's been applied, there's not much you can do about it. We don't have much of that information.

In terms of civil society's role, I think the emerging focus on multistakeholder engagement is really important. Many key civil society organizations are in those spaces, which is fantastic. It's critical for civil society and companies to work together as peers, not as two opposite sides of a table which don't trust one another. Civil society has been successful in slowly getting a foot in the door into key spaces. But there is also huge scope for improvement in figuring out what kind of engagement is useful. Do we need to talk about the implications of these technologies? Do we need to become technical standard-setting bodies? Do we need to be at policy development processes? Perhaps all of the above. These are all things that, as a stakeholder group, civil society needs to decide and organize around.