

Citizenship Forecast: Partly Cloudy with Chances of Algorithms



Costica Dumbrava

In his thought-provoking kick-off contribution, Liav Orgad enthusiastically embraces the idea of a global digital citizenship that could remedy some of the deficiencies of the present system of territorial national citizenships and, potentially, transform the meaning of democratic citizenship. Technologies such as blockchain could allow people to create virtual communities based on shared interests and sustained by instantaneous consent, beyond the reach of nosy governments and regardless of national borders. By widening access to rights, expanding political voice and creating more secure and diverse identities, digital citizenship could address current challenges related to the imperfect attribution of status and rights (statelessness, disenfranchisement), widespread political apathy among citizens and artificial divisions created by national borders. To paraphrase the text of a famous cartoon: ‘on the internet nobody knows you are a foreigner’.

Other contributors to this Forum have pointed out several important tensions and dangers lurking in Orgad’s proposal. Rainer Bauböck worries that replacing political communities, which are based largely on ascribed but equal citizenship, with freely chosen cloud communities would be ‘fatal for democracy’. Purely consensual political communities cannot work because political associations need coercive systems capable to enforce laws. As ‘exit-based conflict resolution systems’ (Primavera De Filippi), virtual communities are too volatile to ensure stable membership and commitment to rules. They are also ill equipped to do the policing and punishing required by political organisation (Robert Post, Michael Blake). Orgad’s cloud communities could be seen instead as akin to civil society organisations. As novel forms of coagulating solidarity, interests and identities, they can be instrumental for checking, challenging or complementing governments, but they have neither the means, nor the legitimacy to replace democratic citizenship.

I agree that technologies may offer surprising opportunities for improving and reimagining our social and political life (Francesca Strumia, Peter Spiro). Information and communication technologies already offer to some people better access to legal status (digital IDs), allowing them to participate more effectively in political deliberations and decision making (e-forums, e-voting), to mobilise against authoritarian regimes (twitter revolutions) and to transcend borders in order to engage with communities of origin (diaspora politics).¹ Using powerful computers, myriads of sensors and sophisticated algorithms, ‘smart cities’ can identify and address public issues and concerns, such as traffic congestions and security threats. However, I worry that we too often take technologies for granted and fail to discern between technological opportunity and mythology.

My contribution to this debate is to raise two general points about the risks involved by linking citizenship to technology, namely making citizenship vulnerable to biases and failures that typically affect technology and increasing citizenship’s dependence on technology.

Technologies are not neutral. They are embedded in and tend to reinforce certain values, norms and expectations to the detriment of others. For example, predictive algorithms used by police are more likely to identify black persons as suspects of crime² and facial recognition software seems to recognise better white male faces.³ When they are not biased by design, smart technologies may quickly pick up biases from their surroundings. In 2016, Microsoft created Tay, a chatbot that used machine learning to emulate a teenage user on Twitter. However, after a few hours of ‘learning’ on the social media platform Tay began posting Hitler-praising and other racist

¹ Dumbrava, C. (2017), ‘Citizenship and Technology’, in Shachar, A., R. Bauböck, I. Bloemraad & M. Vink (eds.), *Oxford Handbook of Citizenship*, 767–788. Oxford: Oxford University Press.

² ‘Big data may be reinforcing racial bias in the criminal justice system’, *The Washington Post*, 10 February 2017, available at https://www.washingtonpost.com/opinions/big-data-may-be-reinforcing-racial-bias-in-the-criminal-justice-system/2017/02/10/d63de518-ee3a-11e6-9973-c5efb7ccfb0d_story.html?utm_term=.5513fe110740

³ ‘Facial recognition software is biased towards white men, researcher finds’, *The Verge*, 11 February 2018, available at <https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error>

and sexist remarks⁴, which forced Microsoft to shut it down with an apology. Bitcoin, the most well-known blockchain technology, can also be regarded as deeply political, a product of particular ‘right-wing, liberation, anti-government politics.’⁵ Such ideological bias makes blockchain unsuitable for becoming the repository of democratic citizenship. If the platform itself is biased towards a particular conception of the good, how can we expect it to serve as an arena and mediator between different conceptions of the good?

Technologies often fall short of expectations and are usually hijacked, if not initiated, by authoritarian governments and powerful groups. For example, India’s population biometric database, Aadhaar, which is intended to provide more than a billion people with digital identities and access to public services, has been criticised for its rigidity and security problems, which affect particularly the poor.⁶ The Chinese government is currently toying with a Social Credit System⁷ designed to measure citizens’ trustworthiness that would further mould their behaviour to align it with the government’s priorities and ideology. Blockchain gurus and their followers claim that this technology is highly secure. However, this has not prevented a hacker to steal about 60 million USD - worth Ether (another major cryptocurrency) in the so-called DAO attack.⁸ Indicative of the ideological underpinning of the blockchain movement, and deeply troubling from many perspectives of social justice, is that some members of the cryptocurrency community sug-

⁴ ‘Microsoft’s disastrous Tay experiment shows the hidden dangers of AI’, *QUARTZ*, 2 April 2016, available at <https://qz.com/646825/microsofts-ai-millennial-chatbot-became-a-racist-jerk-after-less-than-a-day-on-twitter/https://qz.com/653084/microsofts-disastrous-tay-experiment-shows-the-hidden-dangers-of-ai/>

⁵ Golumbia, D. (2015), ‘Bitcoin as Politics: Distributed Right-Wing Extremism’, in G. Lovink, N. Tkacz & P. de Vries (eds.), *MoneyLab reader: An intervention in digital economy*, 118–31. Amsterdam: Institute of Network Cultures.

⁶ ‘In Rajasthan, there is “unrest at the ration shop” because of error-ridden Aadhaar’, *Scroll.in*, 14 April 2018, available at <http://scroll.in/article/805909/in-rajasthan-there-is-unrest-at-the-ration-shop-because-of-error-ridden-aadhaar>

⁷ ‘Big data meets Big Brother as China moves to rate its citizens’, *Wired*, 21 October 2017, available at <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>

⁸ Reijers, W., F. O’Brolcháin & P. Haynes (2016), ‘Governance in Blockchain Technologies & Social Contract Theories’, *Ledger* 1 (1): 134–151.

gested that the attacker should keep the money as s/he did not break the rules but simply exploited a flaw in the system.

As other products of digital technologies, the blockchain exists in online clouds that depend on critical physical infrastructures. Online clouds are no less fragile than on-the-sky clouds. Online systems are emanations of a bunch of machines connected to various grids that require an awful lot of things, such as electricity, computers, data centres, internet servers, etc. Since this enabling infrastructure is vulnerable to hacking and shutdown, so is democratic citizenship if embedded in digital technologies. If digital identities could be compromised (as in the Indian case) and cryptocurrency stolen there is little assurance that digital citizenship solutions, such as universal IDs, e-voting systems and blockchain-based cloud communities, would not succumb to the same illness.

My second point is about the risk of making citizenship (too) dependent on technology. As we regularly worry about our children's addiction to tablets, online gaming and other technologies that could affect their social development, we should also worry about our society's dependence on technologies that might affect its capacity for self-government. It is not only about a technologically mediated withdrawal of citizens from the physical public space, *à la Putnam*,⁹ but also about the dangers of making democratic citizenship dependent on specific technological systems and artefacts.

Exercising citizenship has always involved some forms of technology, from voting pebbles in Ancient Greece to ballot boxes and electoral districting algorithms¹⁰ in modern representative democracies. However, the high levels of sophistication and, ultimately, opaqueness of technologies such as blockchain must be a real concern should we decide to entrust these technologies with the role of embodying democratic self-government. We are asked to take for granted the promises of new digital technologies and are kindly invited to take our places in shiny new cloud communities. However, we rarely understand how these technologies work, who designs and oversees them and whether we would be able to dispense of them if we find them wanting.

⁹ Putnam, R. D. (2000), *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

¹⁰ 'Of the Algorithms, by the Algorithms, for the Algorithms', *Slate*, 13 January 2009, available at http://www.slate.com/articles/news_and_politics/politics/2009/01/of_the_algorithms_by_the_algorithms_for_the_algorithms.html

Some religions tell you that the true God is in the clouds; tech enthusiasts tell you that the true community is in the cloud. I recommend examining the sky carefully before you start packing.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

