At the same time as the ICT revolution has given rise to new forms of political and economic activity, it has also aided the move of neoliberalism even deeper into the self and has reinforced the powers of the carceral state; that is, it has enabled another response to the financial crisis in the form of surveillance capitalism. By transforming data into wealth, surveillance capitalism moves neoliberalism into the individual herself. Not only are her most intimate interactions, those with her friends and family, her thoughts and bodily processes (such as sleep) monetized, but she is also urged to use these tools against herself and others in the arena of the market. She can obsessively track and manage her productivity, create and curate her public image. Yet, what she would find perhaps impossible is imagining a public space where such metrics have been rendered meaningless.

Cities often use the militarized tools of surveillance capitalism against their own citizens: facial recognition, CCTV cameras, drones, and artificial intelligence. Such systems are now global, originating in one place, often the United States, and ported into far-off cities and cultures where their darker potential is more likely to be realized in the light of weaker institutions to preserve civil liberties. In the end, whether the citizens of the global city are likely to leverage technology to liberate themselves from capitalism's logic and engender new political and economic forms, or such technology will instead be used to create a hardened and unmasked version of neoliberalism is not a question Rossi answers.

One way forward, though not fully developed in Rossi's analysis, is that the progressive left share its successful policy initiatives globally much as neoliberalism managed to spread and replicate itself. Policy innovation seems likely to originate not in the world's dominant cities, but in struggling urban areas, in the global economy's periphery, and among marginalized and oppressed groups who now bear the brunt of neoliberalism's injustice. What this century ultimately looks like will depend on what those who live in its cities now, and in the near future, choose – or do not choose.

Rick Searle
Institute for Ethics and Emerging Technologies, Boston, MA, USA
rsearle.searle@gmail.com http://orcid.org/0000-0001-7028-2427

https://doi.org/10.1080/08109028.2018.1503453

Will the Internet fragment?: Sovereignty, globalization and cyberspace, by Milton Mueller, New Jersey, Wiley, 2017, 140 pp., $45.00 (hardback), ISBN 9781509501212

The intersection of politics and the Internet – not 'politics-on-the-Internet', but 'politics-of-the-Internet' – is, like popular sports and economics, a fertile field for big-picture 'hot takes' from non-experts. *Will the Internet Fragment?* is anything but. Its author, Milton Mueller, is not just a professor in the School of Public Policy at the Georgia Institute of Technology, but has participated in ICANN – one of the most important non-profit institutional actors in the area of Internet governance – for more than 20 years. He also co-founded and co-directs the Internet Governance Project. Although deliberately non-technical, this is a book written by somebody with a strong academic and policy background, one of the most respected scholars in the field, who has participated in, and not just studied, the governance conflicts that shaped and continue to influence the Internet.

The book probes whether the Internet is on a path towards fragmentation. This is not mere high-concept analysis. The book is concerned with analyzing the present and future of concrete

patterns of governance, with precise definitions and the evaluation of possibilities with a view towards their practical application. The first goal of the author is to clarify the concept of 'fragmentation'. Despite the frequent use of 'Balkanization' as a metaphor for real or feared trends in Internet governance, the metaphor is no more transparent in the realm of technical governance than in its original geopolitical context. Mueller explores a taxonomy of different ways in which the Internet can fail to be a wholly connected communication space, from transient technical errors to long-term, complicated interdiction efforts. He shows, I believe satisfactorily, that some forms of partial, transient fragmentation (and network responses to them) are a healthy aspect of self-protective mechanisms built into the technical fabric of the Internet, and that states seldom, if ever, attempt to sever completely parts of the network from the rest. As the author indicates, to do so in a drastic manner would merely negate most of the value of the Internet for that state.

What is it, then, that states seek, and to what degree are they successful in finding it? The author introduces, convincingly, the concept of 'alignment'. In this view, states do not try to interrupt connectivity between different parts of the Internet, but instead try to make sure that, at least within the scope of their influence, they are in compliance with (or at least functional to) the state's laws and interests. This is an empirically more adequate framing of the issue; few states have attempted to build purely 'local' Internets, while many, if not most, attempt to play a part in its governance through their influence over both local servers and users, and over those located outside national territories.

The book answers the question in its title with both no and yes. Topological fragmentation of the network is not, except in isolated (pun not intended) cases, a plausible danger, as this is not in the interests of any powerful actor. However, increased levels of alignment with legal systems and strategic interests are definitely a realistic concern. The author notes that many of the benefits accrued from the Internet by civil society during the last decades have derived in part from its relative independence from these constraints. From the point of view of many states, though, to have their citizens interact with a more strongly aligned version of the Internet would be of political and strategic value; they do not want to disconnect from the Internet, but rather to have more of a hand in modulating what happens in the parts they regard as located in their territory.

So much for the diagnosis. The book's final part proposes a solution based on the concept of sovereignty; in short, that Internet governance should be controlled not by individual countries, but by the collective of its users. This is the weakest part of the book. Regardless of the possible benefits from such an arrangement, the author does not make a sufficient case to show it to be sustainable without the agreement and sufferance of national states, a requirement that makes the proposition itself somewhat moot. Mueller raises this concern, only to dismiss it cursorily with the observation that political entities have, in the past, extricated themselves from the control of parent states. The author's background makes it implausible for him to have ignored in his analysis the fact that those entities, in general, gained and sustained their independence through the military defense of contiguous territories over which they asserted and maintained physical control – a feat that seems implausible for cyberspace, which is only a space in one of the most influential but limited of modern metaphors. As the issue is not really explored, we must doubt the practicality of the proposal in question, to say the least.

The other missing factor in the book's analysis is the role of corporations. Internet companies, after all, are among the wealthiest on the planet, the physical assets they own, rent, or use dispersed through it to the degree that would shame the largest empires in history. The daily experience of the Internet for most users is, directly or indirectly, heavily mediated by them. A lack of in-depth exploration of the Internet Balkanizing in user experience, even if not connectivity, between different walled gardens, is perhaps understandable, given the book's specific focus on state-politics issues. A more serious objection is that, insofar as users' experience of the Internet is, to varying but large degrees, their experience *of* these large companies, the ability (and motivation) of states to

align this experience to their own ends will be highly correlated with the degree of influence they might have on these companies. Their unique size and, in many cases, global footprint make them both easier and harder to control than traditional websites, and their centrality to the online habits of users means that alignment efforts by states take place not just at the network level of the Internet, but also in their influence on the practices of individual online companies. Control by the Chinese government of local Chinese media, or the cluster of issues related to the influence of Facebook in different elections, are but two examples of this.

These objections are not intended to diminish the book's importance. In a way, the very salience of issues at the level of the largest Internet companies makes it essential to prevent the critical lower layers of the Internet falling from the attention of activists, analysts, and policymakers. There are few things more useful when engaging with a problem than a proper understanding of what the problem is. By reducing fear of a fragmented Internet, and replacing it with a more analytically powerful account of different attempts to increase alignment, Mueller has made another substantial contribution to the discussion (and, hopefully, practice) of Internet governance.

Marcelo Rinesi
Institute for Ethics and Emerging Technologies, Boston, MA, USA
marcelo.rinesi@gmail.com

https://doi.org/10.1080/08109028.2018.1505877

Philosophy and the precautionary principle: science, evidence and environmental policy, by Daniel Steel, Cambridge, Cambridge University Press, 2018, 256 pp., £22.99 (paperback), ISBN 9781107435094

The precautionary principle was originally an axiom of scientific forestry, according to which one should harvest only as many trees as will be replaced. Georg Ludwig Hartig first advanced the principle in Germany at the dawn of the Industrial Revolution. Concerns about the potential consequences of exploiting natural resources also exercised his British contemporaries, the classical political economists Thomas Malthus and David Ricardo. Together they were completing the domestication of the concept of 'Nature', which the Greeks had portrayed as the indifferent if not erratic dispenser of human fate. However, once the Christian deity in whose image humans are created stood above Nature, the tables started to turn. And once Francis Bacon invented what we now call the 'scientific method' in the early seventeenth century, Nature's own fate was explicitly placed in the hands of humans who were encouraged to experiment to get Nature to reveal its secrets. Since that time, humanity has put Nature on permanent trial. Arguably one downstream effect is anthropogenic climate change. Might not this reveal that Nature is wreaking its revenge?

Already in the early nineteenth century, Malthus and Ricardo were debating this prospect. On the one hand, Malthus argued that if we don't respect Nature by living within its means, we ourselves will be – and have been – part of its cull. Malthus inspired Charles Darwin's formulation of the principle of natural selection, though Malthus himself – an Anglican pastor with a strong Calvinist streak – interpreted Nature's agency as the hidden hand of God. The precautionary principle's focus on the need to maintain a state of 'equilibrium' with Nature comes from this line of thought. On the other hand, Ricardo presumed that necessity is the mother of invention, such that we might innovate our way out of any resource constraints by substituting the fruits of our