Surveillance Capitalism and Digital Alternatives

Published (with links) on *Ideology, Theory, Practice*, November 2021:
https://www.ideology-theory-practice.org/blog/surveillance-capitalism-and-digital-alternatives

Luke Martell

Following the explosion of the internet since the 1990s, and of smartphones and the growth of big tech corporations more recently, the politics of the digital world has drawn much attention. The digital commons, open access and p2p sharing as alternatives to enclosures and copyrighting digitally are important and have been well covered, as providing free and open rather than privatised and restricted online resources[1]. Free and open-source software (FOSS) has been important in projects in the Global South[2]. Also discussed has been the use of social media in uprisings and protest, like the Arab Spring and the #MeToo movement. There is consideration of the anxiety of some when they are not connected by computer or phone, which raises questions of the right or perceived obligation to be connected and, on the other hand, the benefits of digital detox. There are many other important analyses in the digital politics literature about matters such as expression, access, equality, the digital divide, power, openness, and innovation[3]. I focus here on alternatives in the light of recent surveillance and privacy concerns that have come to the fore since the Snowden affair in 2013, the Cambridge Analytica scandal in 2018, and the Pegasus spyware revelations in 2021. US intelligence whistleblower Edward Snowden exposed widespread phone and internet surveillance by US and other security agencies. The firm Cambridge Analytica collected extensive personal data of tens of millions of Facebook users, without their consent, for political advertising, although they may have exaggerated what they did or were able to. The NSO technology company were found to have installed Pegasus surveillance spyware on the phones of politicians, journalists, and activists for number of states. There have been numerous hacks and mega-leaks of individual and company data.

Big tech corporations like GAFAM – Google (Alphabet), Amazon, Facebook (Meta), Apple and Microsoft - have come to dominate and create oligopolies in the digital and tech worlds (another acronym FAANG includes Netflix but not Microsoft). More internationally communications social media like WeChat, Line, Discord and QQ have become pervasive. GAFAM have an extensive hold over sectors such that we are constrained inside their walled gardens to get the online services we want or have come to rely on. Google is a prominent example; it is difficult, for instance, to operate an Android phone without using them, the company's early motto 'Don't be Evil' not to be seen any more these days. These companies' oligopolies over tech and the digital are of concern because they limit our ability to choose and be free, and so is their invasion of personal spaces with surveillance and the capturing of personal information. Many of the corporations gather information about our digital activities, searches, our IP addresses, interests, contacts, and messaging, using algorithmic means. The information is captured and aggregated, and value is created from surveillance, the extractive process of data mining, the selling of personal information, and the creation of models of user behaviour for directing advertising and nudging. In this system, it is said, the user or consumer is the product, the audience the commodity. Data is seen as the new oil, where the oil of the digital economy is us. The produce is the models created to manipulate consumers.

We are often so reliant on such providers it is difficult to avoid this information being collected, something done in a way which is complex and opaque, so hard for us to see and respond to. It is often in principle carried out with our consent but withdrawing consent is so complicated and the practices so obscure and normalised for many that in effect we are giving it without especially wanting to. The information gathered is also available on request, in many cases to varying degrees in different contexts, to governments and police. Sometimes states use the corporate databases of companies like Palantir, avoiding legal restrictions on government use of citizen data, especially in the USA, to monitor some of the most mainstream, benign, and harmless groups and individuals. There are reports of a 'chilling effect' where people are hesitant about saying things or using online resources like searches in a way they feel could attract unjustified government attention.

Questioning approaches to this situation have focused on critique, and action has homed in on boycotts, e.g. of platforms like Facebook, and more general disconnection and unplugging. There is a degoogling movement of people who wish to go online and use the Internet, computers and smartphones in ways that avoid organisations like Google. For many degoogling (or de-GAFAMing) is a complex process, technically and in the amount of work and time involved. Privacy concerns are also followed through by the avoidance of non-essential cookies and using tracking blockers, encryption, and other privacy tools like browser extensions and Virtual Private Networks. Apple builds privacy and blocking means into its products to the consternation of Facebook who have an advertising-led approach. Mozilla has taken a lead in making privacy tools available for its Firefox browser and beyond.

At state level, responses have been oriented to attempting to limit monopolisation and ensure competition, although these have not stopped oligopolies in digital information and tech. There is variation internationally in anti-monopoly attempts by states or the supra-national EU. States have varying privacy laws limiting access to personal information digitally, with governments like the Swiss being more rigorous and outside the 'eyes' states that share intelligence, while states like the Dutch have moved from stronger to weaker privacy laws. The five eyes states Australia, Canada, New Zealand, the UK and USA have a multilateral agreement to spy on citizens and share the collected intelligence with one another. So, those beyond the eyes states are not obligated to sharing citizens' private data at the request of other powers. EU GDPR (General Data Protection Regulation) legislation is important in this context.

The radical politics of alternatives in the Arab Spring, and the Occupy and anti-austerity movements have often relied on social media such as Twitter to organise and act. Many in such movements believe in independence and autonomy including in conventional media but do not go much beyond critique to digital alternatives, which can remain the preserve still of the tech-minded and committed. The latter sometimes have a political critique and approach but often just privacy concerns within an effectively liberal or libertarian approach. One approach, cyberlibertarianism is against obstacles to a free World Wide Web, such as government regulation and censorship, although Silicon Valley that it is identified with is also quite liberal, in the USA sense, and concerned with labour rights. An emphasis of activists on openness and transparency can be given as reason for not using means, such as encryption and other methods mentioned above, for greater privacy and anonymity in information and communication.

There is less expansion beyond critique, boycotting and evasion of privacy incursions to alternatives. However, alternatives there are, and these involve decentralised federated digital spaces where individuals and groups can access internet resources for communication and media from means that are alternative to GAFAM and plural, so we are not reliant on single or few major corporations. Some of these alternatives promise greater emphasis on privacy, not collecting or supplying our information to commerce or the state and, to different degrees, encryption of communication or information in transit or 'at rest', stored on servers. In some cases, encryption in alternatives is not much more extensive than through more mainstream providers, but we are assured on trust that that our data will not be read, shared, or sold. Many alternatives build free and open-source software provided not for profit or gain and sometimes, but not always, by volunteers. Code is open source rather than proprietary so we can see and access it and assess how the alternatives operate and can use and adapt the code. Some provide alternatives to social media like Twitter, Facebook, and Reddit (such as Mastodon, Diaspora, and Lemmur) and to mainstream cloud storage, messaging (e.g. Signal) and email, although some of the alternative fora have low levels of users and activity and many critical and alternatives-oriented activists are still pushed to using big corporate suppliers for quantity of content and users.

Groups like Disroot, a collective of volunteers, provide alternative email which limits the collection, storage and sharing of personal details. Disroot offers links to many platforms alternative to the big corporations for email, messaging, chatting, social media and cloud hosting. Groups like Riseup, a leftist and activist platform, provide invite-only email, data storage on their own servers, and other means for digital activity beyond big corporations and prying eyes to whom they intend to not divulge information, although sometimes limited by levels of encryption and the laws of the states where they are sited. Email providers like Protonmail and Tutanota promise not to collect information about users and to encrypt our communication more rigorously so we can avoid both GAFAM and surveillance. Some of these are still capitalist corporations, but with a privacy emphasis, although semi-alternative companies like Runbox and Infomaniak are worker-owned. Autistici, like Disroot, is volunteer run on non-capitalist lines, monetary aspects limited to voluntary donation. Both have an anarchist leaning, Autistici more explicitly committed to an autonomous anti-capitalist position. Some alternative providers (like Runbox, Tutanota and Posteo) have green commitments, using renewable energy to reduce carbon emissions. Others go beyond a corporate form and have more of a social movement identity. There are campaigning organisations that focus on digital rights and freedom, and crypto-parties that help people adopt privacy and anonymity means in their digital activity.

Some alternative privacy-oriented platforms gained more attention and users after the Snowden affair, but many otherwise alternatives-oriented people continue to use providers like Google because they do not know about the alternatives or switching to them is, sometimes justifiably, seen as a big job. Others are resigned to the belief that email and such online activity can never be private or take alternative tracking blocking measures while continuing to use mainstream resources in, for example, email. For some users there is much to be gained by what data harvesting allows, for instance personalisation of content and making connections with others across platforms like Facebook and Instagram, or they feel that most of the data collected is trivial for them and so accepted. In such cases the dangers and morality of data harvesting and selling are not worrying enough to resist or avoid it. There may also be less individualistic benefits for social research and improvement of tech and the digital that, for some, make some of the data gathering outweigh privacy incursions.

Many of the alternatives are at the level of software and online providers, but this leaves the sphere of hardware and connectedness, where it is possible for states to stop resistance and rebellion by turning the internet off or censoring it, as in China, Egypt, and Iran amongst many other cases. There are alternatives for hardware, for instance in the open-source hardware movement, and for connectedness through devices linked independently in infrastructure or mesh networks. Interest in these lags behind that in software alternatives and their effectiveness depends on how many join such networks[4].

So, the alternatives are around a politics of privacy, independence and autonomy alongside anti-monopoly and sometimes non-capitalist and green elements. It has been argued that the digital world as it is requires the insertion of concepts of anonymity[5] alongside concerns such as equality, liberty, democracy and community in the lexicon of political ideas and concerns, and anonymity rather than oft advocated openness or transparency, a key actor in digital alternatives having been the network 'Anonymous'.

While anonymity is desirable, just as it is when wished for in the offline world, it faces limits in the face of what has been called 'surveillance capitalism'[6]. Firstly, this is because, as offline, anonymity and privacy are difficult to achieve if faced with a determined high-level authority like a government, as the Snowden and Pegasus affairs showed. Secondly, seeking anonymity is a reactive and evasive approach. For a better world what is needed is resistance and an alternative. Resistance involves tackling the power of big tech and the capturing of data they are allowed. Via social movements and states this needs to be challenged and turned back. And in the context of alternatives, alternative tech and an alternative digital world needs to be expanded. So, implied is a regulated and hauled back big tech and its replacement by a more plural tech and digital world, decentralised and federated. One advocate of the latter is Tim Berners-Lee, credited as the founder of the World Wide Web. Anonymity may be desirable individually and for groups, but collectively what is required is overturning of big intrusive tech by state power, through regulation, anti-monopoly activity and public ownership. The UK Labour Party went into the 2019 General Election with a policy of nationalising broadband, mainly for inclusivity and rights to connectedness reasons, but opening up the possibility of other ends public ownership can secure. But state power can be a problem as well as a tool so the alternative of decentralised, collectivist, democratic tech is needed too in a pluralist digital world.

So, to recap and clarify key points. Oligopoly and the harvesting and selling of our digital lives has become a norm and a new economic sector of capitalism. State responses, to very different degrees, have been to resist monopolisation and ensure modest privacy protections or awareness. Individual responses and those of some organisations have been to use software that blocks tracking and aims to maintain privacy and anonymity. But positive as these methods are, they are in part defensive, limited in what they can achieve against high-level attempts at intrusion, and some of these individualise action. Alongside such state and individual processes, we need a more pro-active and collective approach. This includes stronger regulation and breaking up and taking tech into collective ownership. In the sphere of alternatives, it means expanding and strengthening a parallel sphere, decentralised and federated. And alternatives require putting control in the hands of those affected, so collective democracy with inclusive participation. Then oligopolies are challenged and there is a link between those affected and those in control.

But alternatives must be made accessible and more easily understandable to the non-techy and beyond the expert, and do not just have to be an alternative but can be a prefigurative basis for spreading to the way the digital and tech world is more widely. This involves supplementing liberal individual privacy and rights approaches, often defensive within the status quo, with collective democracy and control approaches, more proactive and constructive of alternatives[7]. If there is an erosion of capitalism out of such an approach so there will be also to profit incentives in surveillance capitalism. With an extension of collective control not-for-profit, then motivations for surveillance and data capture are reduced. But this must be done through inclusive democratic control (by workers, users and the community) as much as possible rather than the traditional state, as the latter has its own reasons for surveillance. It should be supplemented by a pluralist, decentralised, federated, digital world to counter oligopoly and power. Democratisation that is inclusive globally is also suited to dealing with differences and divides digitally, e.g. by class or across the Global North and Global South. Taken together this approach implies pluralist democratic socialism as well as liberalism, rather than capitalism or the authoritarian state.

I am grateful to David Berry for his very helpful advice on this article.

[1] Berry, D. (2008) *Copy, Rip, Burn: The Politics of Copyleft and Open Source*, London: Pluto Press.

[2] Pearce, J (2018) Free and Open Source Appropriate Technology, in Parker, M. et al (eds) *The Routledge Companion to Alternative Organization*, London: Routledge.

[3] For a good overview and analysis of the area see Issin, E. and Ruppert, E. (2020) *Being Digital Citizens*, London: Rowman and Littlefield. See also Bigo, D., Issin, E., and Ruppert, E. (eds) (2019) *Data Politics: Worlds, Subjects, Rights*. London: Routledge, and Muldoon, J. (2022) *Platform Socialism: How to Reclaim our Digital Future from Big Tech*, London: Pluto Press.

[4] See Lopez, A. and Bush, M.E.L., (2020) Technology for Transformation is the Path Forward, *Global Tapestry of Alternatives Newsletter*, July. https://globaltapestryofalternatives.org/newsletters:01:index

[5] Rossiter, N. and Zehle, S., (2018) Towards a Politics of Anonymity: Algorithmic Actors in the Constitution of Collective Agency and the Implications for Global Economic Justice Movements, in Parker et al (eds) *The Routledge Companion to Alternative Organization*, London: Routledge.

[6] Zuboff, S., (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Profile Books.

[7] See Liu, W. (2020) *Abolish Silicon Valley: How to Liberate Technology from Capitalism*, London: Repeater Books.