
Gokcen Y. Karanfil
Izmir University of Economics

Follow this and additional works at: https://digitalcommons.uri.edu/mgdr

Part of the Anthropology Commons, Communication Commons, Digital Humanities Commons, Economics Commons, Film and Media Studies Commons, Marketing Commons, Other Business Commons, and the Sociology Commons

Recommended Citation
Available at: https://digitalcommons.uri.edu/mgdr/vol5/iss3/4https://digitalcommons.uri.edu/mgdr/vol5/iss3/4

This Book Review is brought to you for free and open access by DigitalCommons@URI. It has been accepted for inclusion in Markets, Globalization & Development Review by an authorized editor of DigitalCommons@URI. For more information, please contact digitalcommons@etal.uri.edu.

Markets, Globalization & Development Review

Istanbul

Copenhagen

Tokyo

San Salvador

Moscow

Jakarta

Warsaw

Santiago

Cairo

Abu Dhabi

Tegucigalpa

Zagreb

Delhi

Karachi

Hong Kong

This book review is available in Markets, Globalization & Development Review: https://digitalcommons.uri.edu/mgdr/ vol5/iss3/4
Book Review


Introduction
Capitalism, surveillance and colonialism have long been integral components of social life in modern times, so they are not new problems that contemporary societies face. With the digitalization of the world, the invention and widespread use of the internet, the unprecedented developments in information and communication technologies and the transition into what is commonly referred to as the information age it seems the power struggles and the divide between the ‘oppressor’ and the ‘oppressed’ have taken new forms and deepened. What people face today are subtle yet pervasive forms of oppression, through the opportunities made abundant by the globe-spanning contemporary technological infrastructure – and none of the major societies seem to be exempt from techno-enabled forms of domination. People around the world have become much more vulnerable to these ever-increasing forms of coercion. If one of the reasons for this increased vulnerability can be traced to the above-mentioned subtlety and pervasiveness of new forms of oppression, the other stems from the fact that people are to a great extent uninformed and uneducated as to how to resist and/or avoid these new forms of oppressions. This is where Michael Kwet’s book People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment makes its mark. People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment is a brief but detailed open access booklet, written in support of the Right2Know Campaign – a non-profit organization established in 2010 in South Africa with the goal of increasing access to information and protecting freedom of expression mainly on digital platforms. The booklet is intended to equip ordinary citizens with the necessary knowhow and the skills to challenge digital forms of state and corporate surveillance in their everyday engagements with technology, and it excels in being a straightforward, to-the-point guide that is both informative and reader friendly. Kwet (2020b) states in the very first page of the book’s introduction (p. 2):
This guide, which is tailored to the South African context – but applicable to other societies – will equip you with the info needed to protect yourself against government and corporate spying. It provides you with knowledge about People’s Tech for People’s Power: technologies which empower individuals and societies to control their own digital experiences.

As indicated in the above quote the book is intended primarily for the South African reader. Since the problems of digital surveillance and digital colonialism along with potential forms of protection from them are universal, the skills, knowledge and guidance offered in the pages of this booklet, however, are beneficial to readers across the world. Furthermore, the content of the book is geared to readers from all parts of the spectrum when it comes to tech savviness. That is, while a certain amount of basic knowledge on the workings of the Internet would be beneficial to better grasp and better implement the alternative technological practices offered in the book, this is by no means an absolute necessity. This shines as one of the strengths of this guidebook, the information it provides is both basic but effective at the same time so that it becomes highly valuable for both beginner and more experienced readers.

More on the Content of the Book

People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment consists of 86 pages and a total of 19 chapters, including the Introduction and the Conclusion. The first three chapters are allocated to formulating the context and the framework of the general discussions to be found in the coming pages. In the first chapter (the Introduction), Michael Kwet introduces to the reader concepts such as digital colonialism, digital socialism, and surveillance capitalism. In the second and third chapters he writes consecutively about Threat Modelling and the Basics of Information Security and Software. In chapter four the reader is informed about the safe use of mobile phones. From here onwards, most of the remaining chapters are dedicated to specific digital practices like emailing, web browsing, searching the web, video chatting, document collaboration etc. In each of these chapters, the author explains potential hazards with regards to that particular digital practice and offers alternative software and/or forms of engagement for a safer use that would protect the users’ privacy.

In the very early pages of the book Kwet sets out to define some of the principal concepts around which the main concerns of the book revolve. In essence the book is intended to be a guide for ordinary people in their struggles to resist and to find ways around digitalized state and corporate
surveillance. On this account, Kwet starts with highlighting the importance of such resistance and in doing so emphasizes a need for a transition from digital capitalism to digital socialism. He argues (p. 2):

Problems of privacy, security, and surveillance connect to the broader themes of capitalism and authoritarianism. People’s Tech is essential to creating a more prosperous society that replaces digital capitalism with digital socialism – a society in which the people directly own and control the means of computation, and develop it for the well-being of humanity instead of profit and control.

Then he argues that “today’s surveillance is much more pervasive than in times past” (p. 5), and introduces the concept of surveillance capitalism (see also Murray 2020, Zuboff 2019) which he defines as “the economic exploitation of society through corporate and state mass surveillance” (p.5). This enables him to get to the notion of digital colonialism, defined as political, economic and social control through the use of digital technologies. Kwet claims that “digital colonialism is principally achieved through the ownership and control of the digital ecosystem – software, hardware, and network connectivity – which is then designed by its owners for profit and plunder” (p. 6). The issues of contestation and control in digital ecosystems of course are familiar to MGDR readers through past articles and reviews (see Ozgun 2018).

According to Kwet, digital colonialism is the contemporary form of the conventional colonialism experienced during the late nineteenth century. He argues that “today, the “open veins” of the Global South are the “digital veins” crossing the oceans, wiring up a tech ecosystem owned and controlled by a handful of mostly US-based corporations” (p. 6). He offers People’s Tech as an empowering tool in the struggle for resistance to this exploitation, thus formulating the definitive aim of the booklet – to offer guidance in fight against digital colonialism.

The booklet is very reader friendly and informative. Throughout the chapters Kwet shares some valuable, basic and easily implementable information with the reader that would either allow an ordinary citizen to avoid proprietary technologies (see Kwet 2020a) or to open up new avenues for challenging digital surveillance and digital colonialism. He claims that “by using Big Tech’s core products and services, the forces of digital colonialism and surveillance will tighten their stranglehold on South Africa and other societies” (p. 49). He then puts forth People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment as a potential way out from this oppression by suggesting that “this guide
demonstrates, there are many simple steps you can take to drastically improve your privacy” (p. 8).

This is exactly what he does throughout the pages. Most of the knowledge shared in the booklet is of technical nature rather than theoretical, which in turn offers tangible forms of protection of privacy. After explaining what free and open-source software entails (p. 13) he talks about how the use of ‘big tech’ products should be avoided whenever possible. He introduces Sign and Wire as alternatives to WhatsApp, following a brief discussion on how the latter invades privacy (Kwet 2020b, pp. 5-6). He explains the hazards of using proprietary browsers such as Safari or Google Chrome and suggests the use of VPNs, Tor Browser or Chromium and Mozilla Firefox with addons (pp. 18-19). After briefly discussing the problematic aspects of using big tech search engines he urges the reader to use DuckDuckGo and/or Qwant (p. 23). Throughout the booklet, organized under brief chapters, the reader is informed on issues such as data protection, password management, possible choices for operating systems and app stores, video surveillance and internet decentralization. In each section, first the problematic aspects of these digital practices are discussed briefly and then means to tackle them are shared with the reader. The booklet is full of information of this kind that empowers the reader with alternatives to proprietary, big tech products. One thing that makes all this information particularly useful and easily implementable is that whenever he introduces an alternative software or an application or a resource, Michael Kwet provides a link to them and a basic explanation of how one can go about acquiring and using them.

This abundance of easily understandable, easily implementable and technically oriented information shared in the book is perhaps its main strength. Ironically, if I was to think of a shortcoming for this guidebook, I would think that this same simplicity and technicality might also be it. Although Kwet briefly elaborates on concepts such as digital colonialism, digital surveillance and surveillance capitalism (mainly in the early and final pages of the booklet), these conceptual treatments are relatively light in nature. An in-depth intellectual discussion on power relations and how they affect everyday lives of ordinary people is missing. While I realize that this is a guidebook intended for equipping ordinary citizens with the skills and the knowhow to protect their privacies and to resist against oppression, it is also my contention that a deeper understanding of the underlying importance of such empowerment is also a necessity – perhaps even a prerequisite for the success of a resistance against digital colonialism, or any form of oppression.
One chapter, thus a topic, that stands out as particularly emphasized and discussed in more detail in the *People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment* is the issue of education – in particular public education. In fact, the title of the chapter allocated to this topic is “Public Education: A Key Battleground”. This is precisely how Kwet (rightly) sees the arena of public education as a key battleground. He argues that (p. 61):

The use of Big Tech products like Microsoft Windows and Google Android on learner devices is deeply problematic, for a number of reasons. ...First, product placement in schools will deepen the stranglehold of corporations like Microsoft and Google over South African society. ...Second, the future generation of software developers will likely seek to build products for the software ecosystems they grow up using. ...Third, Big Tech software forcefully subjects students and teachers to corporate and state spying.

He states that “schools are a key battleground for South Africa’s digital society. In the 21st century, there can be no decolonisation of education, economy, or society without the decolonisation of technology” (p. 62). He then concludes this topic by stating that “it is critical that People’s Tech is used in the education system instead of Big Tech products and services. Around the world, there are pockets of Free Software deployments in the public education system” (p.61).

**Concluding Observations**

*People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment* is a book that is geared around ideas of resistance and avoidance. On one level it teaches skills to its potential readers that would allow them to avoid state and corporate surveillance in their everyday engagements with technology – mainly communication technologies. On another level, it imparts knowledge on these issues to readers – to empower them with means to potentially resist and even subvert digital colonialism. What I find quite intriguing in all this is that in both circumstances these acts of avoidance and resistance are carried out from within the confines of the hegemonic arrangements, that is, the infrastructure of digital technology. In the words of Michael Kwet (p. 7):

People’s Tech incorporates the technologies, laws, and educational changes needed to make tech work for the people, not corporations and governments. This guide explains the set of tools needed to
defend yourself and your communities against digital surveillance and corporate colonialization. It links these struggles to the broader context, digital colonialism, and provides some of the concepts needed to think critically about how to build a digital society by and for the people.

While Kwet introduces a multitude of free/open-source software and applications alternative to proprietary technology, ultimately the oppressed and the oppressor are making use of the same technological infrastructure. Sure, we may choose to use Tor Browser as an alternative to Safari or Chrome, or we may use Sign instead of WhatsApp for private messaging, we may use VPNs to protect our privacy, we may even run our mobile phones with alternative operating systems — and all of this is obviously important and effective. It is important, however, to realize that eventually, we are all using the same tech ecosystem predominantly owned and controlled by giant conglomerates. I am not suggesting this as a criticism to the book. To the contrary, I believe this makes the content of this guidebook all the more valuable. In essence, what People’s Tech entails might be defined as a form of resistance from within. Resistance that makes use of the means, tools, apparatuses and the language of the hegemonic structure itself — a means of thwarting the system from within.

Here I am reminded of Michele de Certeau’s (1984) concepts of “strategy” and “tactic”, which he introduced to discuss the power struggles between the oppressed and the oppressor within the context of everyday cultural practices in a given society. In the words of Mitchell (2007), Michele de Certeau’s work “concerns precisely the relationship between ‘the system’ and human action – or between strategy and tactics” (pp. 90-91). Michele de Certeau defines strategies almost as infrastructures that are accessible only to those who are in control of the established power structures. Strategies are the tools of the powerful. In this case the technological ecosystem itself. Tactics, on the other hand, offer to the weak opportunities to adapt to – but more importantly to resist/subvert – the ‘system’ created by those in power through their use of strategies (1984). In de Certeau’s words (1984), a tactic “must vigilantly make use of the cracks that particular conjunctions open in the surveillance of the proprietary powers. It poaches in them. It creates surprises in them. It can be where it is least expected. It is a guileful ruse” (p. 37). De Certeau underlines how this resistance/subversion deconstructs the predominant structures in a society when he says, “the tactics of consumption” are “the ingenious ways in which the weak make use of the strong” (1984, p. 18).

Reading *People’s Tech for People’s Power: A Guide to Digital Self...*
Defense and Empowerment I am acutely reminded of the ways in which we can deploy Michele de Certeau’s analysis of everyday life as a productive optic in making better sense of how ‘grassroots’, ‘user generated’, ‘free/open-source’ digital initiatives mentioned in this booklet may become potent forms of resistance against and subversion of the hegemonic digital colonialist infrastructures through the manipulation of those same infrastructures (for a culturally distinct view on similar and related issues in a very non-western context, viz. Japan, see Kobayashi and Taguchi 2018).

On a final note, while the core concerns of this book – surveillance, loss of privacy and oppression – readily brings to mind George Orwell’s (1949) dystopian imagination of a future where a big brother is going to surveil and oppress us, I believe it may be argued that the current situation seems to be more in line with Aldous Huxley’s (1932) take on the topic – where not what/who we hate/fear but what we enjoy/love will bring our demise (see, for example, Darmody and Zwick 2020). People’s Tech for People’s Power: A Guide to Digital Self Defense and Empowerment is a concise and powerful guidebook that excels in offering ordinary people alternatives to keep doing what they enjoy, all the while equipping and empowering them with the knowledge and skills to resist oppression.
References


