DIGITAL SOVEREIGNTY OR DIGITAL COLONIALISM?

Renata Ávila Pinto

- *New tensions of privacy, security and national policies* -

ABSTRACT

Beyond tensions of privacy and security, we are witnessing today a real confrontation between control and freedom, not only of the individual, but of entire populations and regions, enhanced by technologies and massive collection and analysis of data – from predicting and influencing behaviours, to the automation of public services and the ability to fully control and disrupt those services, even remotely. From gaining access to a global communications platform to losing the ability to protect the rights of those who are interconnected through those platforms. Are we witnessing a new form of digital colonialism?

This article focuses on regional, national, and community solutions to restore control and ownership on key information and communications infrastructures – the only possible first step to fix the current massive violation of privacy rights. It will later suggest some local measures to experiment with and advance alternatives at different levels of intervention and action, including proactive policy, capacity building, and new designs inspired in a set of values and principles different from those of the dominant actors in the market.

KEYWORDS

Surveillance | Technology Sovereignty | Digital colonialism | Free software | Privacy | Data control | Economic espionage | Indigenous peoples

Every digital application that can be used for surveillance and control will be used for surveillance and control.
Professor Shoshana Zuboff[1]

1 • Defining the problem: digital colonialism and technological feuds

A simplistic analysis of the current situation of tensions between privacy and security (the prevalent narrative in media) will probably state the following: States are spying on national and foreign citizens and the trend will only increase as they acquire cheaper technologies, proportional to their military and technological power. The private sector does it too, but not with inherently bad intentions or political purposes. What the private sector is concerned about is the "experience" of the user and the maximum capture of their data and how to offer the best products and services. Collateral damage, such as the abuse of Facebook data, by companies like Cambridge Analytica, is the exception to the rule.[2] As for the people, they are not really concerned about their government spying on them. They are somewhat concerned about private sector surveillance, but they are willing to allow it, especially if that enables them to enjoy "free" services or improve their overall experience. This is despite the fact that privacy awareness is gradually increasing and rules are slightly improving in some regions, especially in Europe for example after the entering into force of the General Data Protection Directive (GDPR), patching a broken system of systemic privacy erosion and data extractivism.

Beyond this simplistic analysis, however, the situation is more complex and involves an additional element that is often overlooked. The power of surveillance and the concentration of the data gathered by both public and private mechanisms is focused on a small number of actors, public and private, based mainly in one jurisdiction and leading to a rapid erosion of state sovereignty and democracy.

Never before has a small sector had so much power over the entire World, to monitor the present and predict future behaviours of not just individuals, but entire populations. The problem is more alarming when we consider how the public and private sectors are merging in joint ventures in a quest for global domination, penetrating every government, every citizen movement, mediating every action in every connected person's life through digital devices and data collection.

Information communication technologies (ICT), artificial intelligence innovation and the ability to deploy systems and infrastructure rapidly in emerging markets, are concentrated in just a few countries, which are now engaged in a race to be the number one.

On top of that, those countries and companies have three elements that most developing nations and even middle-income countries currently lack. The first element is resources,

both capital resources (ownership and control of cables and servers and data) and intellectual resources (the most advanced technicians and research institutions). The second element is the current domestic and international legal architecture, which blocks small countries from adopting policies that favour the production and purchase of goods and services produced domestically, with the threat of legal proceedings in international courts for adopting anti-competitive measures. This limits the ability for developing and middle income countries to research and innovate; the current patent and copyright system artificially restricts the sharing of knowledge and the ability to innovate at a rapid pace. Such restrictions will only increase, with little possibility of reversal, due to the new group of Free Trade Agreements the Trans Pacific Partnership (TPP), Transatlantic Trade and Investment Partnership (TTIP), and Trade in Services Agreement (TISA). Some of the provisions of the new generation trade agreements even consider tighter privacy laws and policies in a country as a barrier for trade, disregarding the superiority of human rights laws over any other law.[3]

The third element, readily accessible to only a small group of countries, is the availability of financial capital to experiment and design new models, via either public funds, venture capital or public private partnerships. Those countries are investing heavily in research and development, not only to maintain their dominant position in the industry and to aggressively expand to as many markets as possible, but also to explore innovative ways to integrate information technology in every aspect of the public administration, the private sector, their defence and security, and the application of citizen rights.

The scenario is radically different for developing countries, where austerity is the norm, and where digital inequality is soon going to be a very visible problem including education and research gaps leading to absolute technological dependence. These countries represent a relatively easy terrain to dominate and there is a race to do so by big technology companies, particularly between the United States of America (US) and China, as Europe lags behind and their companies struggle to compete with their US and Asian counterparts.

Therefore, the world's offline populations are the disputed territory of tech empires, because whoever gets them locked into their digital feudalism, holds the key to the future. Tech giants are, without doubt, heavily influencing the way campaigns, governments, and politics operate.

They also influence politics and policy to shape global standards to serve their business models,[4] increasingly based in data collection, monitoring, and pattern identification –inevitably eroding the privacy of many people. Beyond Brussels[5] and Washington, tech giants are currently engaged in aggressive pushes to invest in areas which traditionally belonged to the state or other specialised agencies and providers. Now two California-based technology companies (Facebook and Google), a space giant in California (SpaceX) and a satellite company in New Jersey (OneWeb) are engaged in accelerated races to connect the disconnected.[6] These companies are providing critical infrastructure for citizens in exchange for their personal data and becoming potential

recipients of advertising. In most of the countries, neither the government nor private investors can compete with the speed and resources these major companies have for providing connectivity to under-served areas.

These corporations, one of which usually represents the user's first digital experience, often combine their programmes with the provision of hardware, software, and limited content, giving neither citizens nor the state much choice. New users are typically subjected to private, long-term agreements, which allow the entities full access to any of the user's data. This is compounded by the fact that we are usually talking about territories with absent or limited privacy and data protection. The contracts also often contain severe penalty clauses in case of breach. This situation enables new and disguised forms of exploitation and subordination.

Rapid digitisation programmes are relying heavily on mobile technologies to plug new users into the increasingly commercialised Web. This approach differs from initial programmes, such as One Laptop Per Child, which advocated for the development of creative capacities and literacy for the poor to be able to fully develop the ability to code, create hardware, and even build skills in robotics.[7] Such early programmes stand in contrast to current programmes which only allow users to access a previously installed set of websites, block any ability to create – since it is only possible to do so much with a mobile phone. In addition, they increase the risk of surveillance and profiling of disadvantaged populations, because mobile phones in several countries are linked to a registered SIM card.[8] The monitoring and monetisation of all users' activities online is the main motivation for the quasi-philanthropic efforts to connect the next billion, and therefore get hold of their data. User data is the basic raw material for machine learning and artificial intelligence, when combined with sophisticated algorithms and computational power of the concentrated tech conglomerates.

In most cases, current connectivity policies provided by external corporate actors – as well as some international charities associated with or close to telecommunications or technology companies – disregard the creative power and autonomy of people or the local community. The devices, software, and hardware are often designed for personal consumption instead of creation or collective uses. All programmes act with urgency to connect as many people as possible, as fast as possible, neglecting considerations like content, long-term sustainability, or basic literacy on important issues such as privacy and security online. When the critical infrastructure is provided by someone else, it is difficult to improve or enforce enhanced settings for privacy since the infrastructure and equipment is often designed to serve the purposes of countries where massive surveillance is the norm.[9] In her article "Dark Google",[10] Professor Shoshana Zuboff explains the reasons behind the rush to connect the global poor in a particular way. She also warns of the dangers of revolving doors between the largest companies and their governments, which might be tempted to use technology to their geopolitical advantage:

> *Google, Facebook, and others shifted to an advertising model that required the covert capture of user data as the currency for ad sales.*

> *Profits rapidly materialized and motivated ever more ruthless and determined data collection. The new science of data mining exploded, driven in part by Google's spectacular success.*[11]

And there are experiments already taking place along those lines. For instance, during the former leftist government in Argentina, YCombinator,[12] a venture capitalist fund, supported and funded an emerging opposition political party, a situation that in 2018 could cause unprecedented scandal now it has finally become apparent that technology has the potential to alter politics. The experiment was not successful – the party in question no longer continues as a registered political party – but it demonstrates the possibilities of Silicon Valley intervening in foreign politics. The Zunzuneo Case in Cuba showed how governments are increasingly relying in the tech industry to push for a new form of intervention.[13] And then the Cambridge Analytica scandal, shaking the Western democracies since early 2018, simply confirmed that not even the most powerful countries in the World are immune to such interventions.[14]

Indeed, it is not only a problem of the least developed and more disconnected countries. Increasingly, governments from middle income countries are actively involving companies to assist them to suppress some forms of speech they consider a threat to the security of their countries. Legitimate speech is being monitored and suppressed if the platform the material is published on agrees with the government that such content is harmful, even if the material is produced abroad and intended for different audiences.[15] (For examples, see Online Censorship Project: https://onlinecensorship.org.) Furthermore, governments are increasingly falling victim to attacks on key systems, assets, and individuals, such as the recent attack on proprietary software in Ukraine's power grid[16] or the targeted hacking of the accounts of high-rank officials in various countries in Latin America.[17]

Entire nations and their industries are fully dependent on critical infrastructure, software, and hardware provided by a handful of companies based in a small group of countries. Almost every activity is mediated by our interaction with technologies and services offered by an increasingly concentrated conglomerate. Looking at the case of software and hardware, it is increasingly alarming, and it is one of the most urgent questions to address when discussing security of our information and communications infrastructure.

Despite recent revelations about the capabilities and practices of intelligence agencies, few global leaders, (all of whom are well aware of the problem) are taking any real steps towards solutions that are designed to respect universal human rights effectively and which are also compatible with a global, interconnected world, and that are affordable, reliable and scalable. Furthermore, any efforts in that direction are precipitously labelled as Internet fragmentation or balkanisation of the Internet.

Most of the key elements that enable any individual, corporation, or government to connect to the Internet are concentrated in the jurisdiction of California. Most of the

companies are US companies, with the majority of the capital coming from the US. In a troubled geopolitical environment, this concentration of tech companies could result in a lawful but illegitimate suspension of products and services to a foreign government or key industries in another country.[18]

Commercial organisations are susceptible to political pressure – as proven by the WikiLeaks case when Visa, MasterCard, American Express, Western Union and PayPal blocked payments to the organisation.[19] Consumer defences are weak and expensive to enforce, and even for European Union citizens, there is often no remedy in such circumstances, which was the case for Wikileaks[20] and also during the Catalonian crisis of 2017.[21] In the case of a government, sanctions could severely disrupt day-to-day business. Dependency on certain technologies to manage public administration are widespread as few companies in the world, located in even fewer countries, fulfil the requirements to provide governments with the software and hardware they need to conduct public affairs at an affordable price that fits the increasingly uniform public procurement rules, which generally favour the lowest-priced option. The result is a scenario whereby governments are heavily dependent on key infrastructure from a small set of providers – providers that are generally susceptible to secret orders, political pressure, and suspension of services due to sanctions. And when considering replacing a provider in favour of a national provider who might offer lower pricing, the government faces severe penalties.

As technology continues to penetrate the core activities of each and every branch of the government, the government itself becomes more vulnerable than ever, relying on key infrastructure they do not control. Any local or national government is certainly less free when the market is "free" although in reality dominated by quasi-monopolies.[22] When we discuss digital technologies on a massive scale, we find a set of companies which grew out of subsidies and heavy funding from a government, which at the same time dominated and continues dominating the rules of international trade.[23] These rules severely erode the freedom of public procurement offices to either choose more expensive local alternatives or subsidise their local industries.

The dependence on foreign technology only increases when dealing with critical infrastructures. On 14 April 2008, Microsoft announced[24] the company would no longer provide security update to their Windows XP operating system. The announcement left thousands of state systems completely vulnerable because they relied on it to operate crucial infrastructure, such as the entry system at the border of a Latin American nation. While a similar situation in the physical environment – a border full of holes and weak controls – would likely result in a Congressional inquiry, the level of awareness on crucial technology infrastructures let this issue remain unresolved way for months.

Several governments rely on communications infrastructure that are completely located in the cloud (i.e., in foreign data centres under foreign-applicable laws). Furthermore, those services are provided under constantly changing terms of use and arbitrary suspension of services.

The problem is not only about dependency on a foreign provider or applicable laws to digital data; the problem is also about the absence of public policies to address the issue at all levels. The situation of digital domination, close to colonialism, still fails to fill the top priorities of the global political agenda. Almost forty years after the invention of the Internet, the ability of politicians and social leaders to understand the dimensions of the problem still falls short.

2 • Exploring spaces of resistance and technology sovereignty

Latin America led the early steps towards digital sovereignty in the early 2000s. A few countries took adequate steps to be ready to replace foreign providers with local ones. Although in India the use of open source software by the state has been mandatory since 2005,[25] Latin America countries such as Brazil[26] and Venezuela[27] (Decree No. 3.390 2004) were even earlier, enacting laws in 2004 establishing free software migration of government data. Similar initiatives followed in Ecuador (Decree No. 1014 2008),[28] Uruguay[29] (Law No. 19.179 2013) and Bolivia[30] (Supreme Decree No. 1793 2013). In all of these countries, the shift was combined with strategies to increase free software literacy among primary school children, developing projects such as Plan Ceibal in Uruguay and Canaima in Venezuela. The Latin American countries had enough human capacity to produce domestically at least part of the software that they needed, even exporting some production, while simultaneously investing in building capacity. As a way to circumvent the US embargo, Cuba developed its own operative system, Nova. Cuba did this not only because of the embargo but also as a way to control their own systems. Such adoption was vital, as the country has restrictions to access software licenses and security updates provided by the largest providers. Full migration to free software was announced by Russia recently, as a way to pre-empt the impact of current and upcoming sanctions.[31]

But simply adopting free software is not enough for a state to build a comprehensive policy that guarantees technology sovereignty over its communications. In attempting to replace either proprietary or dominant choices, governments and community initiatives are finding growing challenges to meet user expectations, in terms of both speed of delivery and quality of the user experience. Sustainability is also among the challenges, as is reaching mass adoption, unless dictated by law and a resourced public policy implementation as in Plan Ceibal, where the entire education system was migrated to open source software (and hardware). In the case of hardware and equipment, a group of medical doctors are deploying 3D printing machines to provide Gaza hospitals, affected by Israeli blockades, with stethoscopes.[32] Similar models could be explored by other countries who remain reliant on other states for key equipment. Developing new models allowing for domestic production is particularly important after the numerous revelations of implants and security holes enabled by foreign providers to permit foreign espionage, compromising the security of users.[33]

Indian scholar Sunil Abraham also points in that direction, highlighting the importance of developing technologies that take human rights into consideration in

their design, and including code that cannot be restricted by copyright law or used as a tool of resistance against certain laws, which would lead to further tensions. Abraham describes how "code could be used to resist regulation through law, thereby converting both the software and hardware layers of devices and networks into a battleground for sovereignty between the free software hacker and the state."[34]

As people across the globe gain access to the most sophisticated personal technology they have had access to since television, a new generation of developers and creators are emerging. The next generation of technologies, produced outside the tech giants, might bring the solutions we are looking for, provided that they are designed, developed, and distributed taking into consideration a different set of values, societal behaviours, and dynamics. But such creative power might be blocked if we do not stop the current direction of technology architecture that restricts creativity rather than enabling it and which encourages consumption, and centralises power.

Once technological autonomy is achieved, individuals and communities can embed their principles in the way they choose to communicate. As stated by the Maori indigenous peoples, when considering the urgent need for indigenous people to develop their own ICT policy: "...the deliberate replacement of local technologies with Eurocentric values-laden, profit-driven technologies has been part of the colonising agenda for many centuries".[35]

Constant innovation also plays a key role in resisting and defeating technological domination. Thinking beyond the market is something that developed nations are already doing. As Dr. Francesca Bria states:

> *Alternative forms of public and common ownership for platforms will help to create a more democratic economy, transcending the logic of market-based, rent seeking, privatized network systems. Too often this leads to decisions based on short-termism, value extraction, and the appropriation of common resources for private gain. A much longer-term approach to technology, economy and politics is required where public resources and assets are owned, managed and distributed for the collective good. This task is about building XXI century democracy.*[36]

For middle-income and low-income countries that are still struggling to catch up and realise the potential of new technologies – and at the same time avoid violations of their citizens' rights – there are a number of options that need to start to be deployed with urgency. Most of these options exist in medium-to long-term national and regional commitments at multiple layers and involving a fluid collaboration between the governments, citizens, and national companies. At the constitutional level, countries must ensure that they keep the ability to legislate and regulate emerging technologies and

their impact on fundamental rights of their citizens. Constitutions should be amended so as not to permit the executive's engagement in international commitments that would strip the government of its ability to enforce rights domestically. Constitutions should also guarantee that the state exercises autonomy and control over critical technology infrastructures[37] and key positions[38] in important assets and industries.

In parallel, it is also necessary to develop a state-funded strategy for digital sovereignty. This should cover all aspects, including modifying the curricula to develop the human resources needed for the next 50 years; investing heavily in funds like CAPS and other research and development initiatives so local experiments can be conducted; taking into consideration the specific needs, skills, and vision of each country; and proactively investing resources in social applications of technology. Exchange of skills, information, and research within the Global South could be encouraged and funded.

In the meantime, the simple regulation of open standards, free software, openly available hardware, and transparency of algorithms could be developed, at least for the state purchases and practices. Bolivia did this recently,[39] under the leadership of the indigenous Vice Chair of the Bolivian Parliament, Nelida Sifuentes and under the advice of Richard Stallman.[40] Achieving equal rights for all and effective remedies against mass surveillance for citizens in the Global South will only be achieved with funded, long-term, and comprehensive changes in policy, technology, and politics towards autonomy and sovereignty. This will gradually enable a culture of digital dignity with human rights standards embedded in protocols at the regional and international level.

3 • Conclusion

It is necessary therefore that global leaders – especially those advocating for equality and social justice – become aware of the dangers that the rapid digital commodification represents for the vulnerable people around the world and its impact on democracy and dignity.

As the scholar Dan Schiller warns:

> *For most of the world's peoples, whether profitable growth for capital may be renewed, and by whom, are far less important than the consequences of digital commodification for employment and exploitation and inequality; for the prospect of democratic self-government; for the ravaged environment; and for the character and quality of cultural services needed to sustain meaningful lives. The shocks of digital commodification are writing a new chapter in capitalism's long history of violent dislocation. This makes discussion of strategies for social alternatives essential, indeed, urgent.*[41]

To start addressing global digital inequalities and embrace a future that places digital autonomy and human dignity at its core, social innovation should be encouraged and institutionalised at the community and citizen level to guarantee its scalability and permanence. Autonomous and linguistic communities should be encouraged to develop their own technology and digital content and to preserve and export their cultures to the digital environment. Public policies should be enacted to guarantee that the adoption of new technologies at a massive scale does not create further inequality, exclusion, or imposition of values and practices that are foreign to the host communities. Instead, it could be an opportunity to rescue and develop further local knowledge. Rooted in the local, in the decentralised and in the digital commons logic: those are the characteristics of the policies that will defeat digital colonialism.

NOTES

1 • Shoshanna Zuboff, "Dark Google." Frankfurter Allgemeine Zeitung, April 30, 2014, accessed January 18, 2016, http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html.

2 • Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." The Guardian, March 17, 2018, accessed June 20, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

3 • Michael Geist, "How the TPP Puts Canadian Privacy at Risk." Michael Geist website, October 14, 2015, accessed January 18, 2016, http://www.michaelgeist.ca/2015/10/how-the-tpp-puts-canadian-privacy-at-risk/; see also Tyler Orton, "From IP to Privacy — Why TPP is 'Potentially Dangerous' for B.C. Tech Sector." Business Vancouver, November 17, 2015, accessed January 18, 2016, https://www.biv.com/article/2015/11/trade-deal-potentially-dangerous-bc-tech-sector.

4 • James Fontanella-Khan, "Brussels: Astroturfing Takes Root." Financial Times, June 26, 2013, accessed June 20, 2018, https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de; Nancy Marshall-Genzer, "Why US Tech Lobbyists Have Descended on Brussels." Marketplace, August 11, 2014, accessed June 20, 2018, https://www.marketplace.org/2014/08/11/world/why-us-tech-lobbyists-have-descended-brussels.

5 • Tony Romm, "Tech Giants Get Deeper Into D.C. Influence Game." Politico, January 1, 2015, accessed June 20, 2018, http://www.politico.com/story/2015/01/tech-lobby-apple-amazon-facebook-google-114468#ixzz3wV2vx4H0.

6 • Tim Cross, "Connecting the World: Four Firms Hope to Bring Internet Access to Everybody." The World in 2016, November 6, 2015, accessed January 18, 2016, http://www.theworldin.com/article/10646; the companies are Google, Facebook, SpaceX and OneWeb.

7 • Anna Heim, "Uruguay's One Laptop Per Child Program: Impact and Numbers." TNW News, April 17, 2013, accessed January 18, 2016, http://thenextweb.com/la/2013/04/07/uruguays-one-laptop-per-child-program-impact-and-numbers.

8 • Mohammed Lubowa, "Invasion Of Privacy:

The Legal Implications of Mandatory SIM Card Registration on Mobile Users in Uganda." Master Thesis, 2013, accessed June 20, 2018, https://www.duo.uio.no/handle/10852/38120.

9 • "The Problem with Cell Phones," Electronic Frontier Foundation, February 15, 2015, accessed January 18, 2016, https://ssd.eff.org/en/module/problem-mobile-phones.

10 • Zuboff, "Dark Google." 2014.

11 • *Ibid*.

12 • Max Chafkin, "Why YCombinator Funded a Radical Political Party in Argentina." Fast Company, March 12, 2015, accessed January 18, 2015, http://www.fastcompany.com/3043388/the-y-combinator-chronicles/why-y-combinator-funded-a-radical-political-party-in-argentina.

13 • Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government." The Guardian, April 3, 2014, accessed June 20, 2018, http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.

14 • Cadwalladr and Graham-Harrison, "Revealed..." 2018.

15 • For different examples, look at Online Censorship Project, Homepage, 2018, accessed June 20, 2018, https://onlinecensorship.org/.

16 • Nick Buckley and Hanna Kuchler, "Hackers Shut Down Power Grid in Ukraine." Financial Times, January 5, 2016, accessed June 20, 2018, http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html.

17 • Claudio Guarnieri, John Scott-Railton, Morgan Marquis-Boire, and Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor." Citizen Lab, December 8, 2015, accessed June 20, 2018, https://citizenlab.org/2015/12/packrat-report/.

18 • See Yochai Benkler, "WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons," *Dœdalus* 140, no. 4 (2011): 154-64, accessed January 18, 2016, http://benkler.org/WikiLeaks_PROTECT-IP_Benkler.pdf.

19 • Parmy Olson, "Has Western Union Snubbed WikiLeaks?" Forbes, December 10, 2010, accessed June 20, 2018, http://www.forbes.com/sites/parmyolson/2010/12/29/has-western-union-snubbed-wikileaks.

20 • Don Reisinger, "Credit Card Companies' WikiLeaks Block Just Fine, EU Says." CNET.com, November 27, 2012, accessed January 18, 2016, http://www.cnet.com/uk/news/credit-card-companies-wikileaks-block-just-fine-eu-says.

21 • Sam Jones, "Catalan Leaders Compare Spain to North Korea After Referendum Sites Blocked". The Guardian, September 27, 2017, accessed June 20, 2018, https://www.theguardian.com/world/2017/sep/27/catalans-compare-spain-to-north-korea-after-referendum-sites-blocked.

22 • Christopher Williams, "Google Charged with Monopoly Abuse." The Telegraph, April 15, 2015, accessed June 20, 2018, http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11537546/Google-charged-with-monopoly-abuse.html.

23 • Bruce Upbin, "Debunking the Narrative of Silicon Valley's Innovation Might." Forbes, June 13, 2013, accessed January 18, 2016, http://www.forbes.com/sites/bruceupbin/2013/06/13/debunking-the-narrative-of-silicon-valleys-innovation-might.

24 • "Your Windows XP Computer Isn't as Secure as it Used to Be," Microsoft, [n.d.], accessed January 18, 2016, http://www.microsoft.com/windows/en-us/xp/default.aspx.

25 • Eileen Yu, "Indian Government Mandates Use of Open Source Software." ZDNet, March 31, 2015, accessed January 18, 2016, http://www.zdnet.com/article/indian-government-mandates-use-of-open-source-software.

26 • Todd Benson, "Brazil: Free Software's Biggest and Best Friend." The New York Times, March 29, 2005, accessed June 20, 2018, http://www.nytimes.com/2005/03/29/technology/brazil-free-softwares-biggest-and-best-friend.html.

27 • In Venezuela, a decree was approved in 2004 declaring free software and open standards the default for public administration. "Decreto 3390," Software Libre, 2004, accessed June 20, 2018,

http://www.softwarelibre.gob.ve/images/stories/leyes/decreto3390softwarelibre.pdf.

28 • "Decreto 1014," Esteban Mendieta, 2008, accessed June 20, 2018, http://www.estebanmendieta.com/blog/wp-content/uploads/Decreto_1014_software_libre_Ecuador.pdf

29 • "Ley 19179," Parlamento Del Uruguay, 2014, accessed June 20, 2018, www.parlamento.gub.uy/leyes/ley19179.htm.

30 • Bolivia Implementation plan of Free Software and Open Standards: "Plan de Implementación de Software Libre y Estándares Abiertos 2015-2022," Comité Plurinacional de Tecnologías de la Información y Comunicación – COPLUTIC, August 2015, accessed June 20, 2018, http://coplutic.gob.bo/IMG/pdf/propuesta_plan_de_implementacion_de_software_libre_y_estandares_abiertos.pdf.

31 • Adrian Offerman, "Russia to Replace Proprietary Software with Free Software." Joinup, June 23, 2015, accessed June 20, 2018, https://joinup.ec.europa.eu/community/osor/news/russia-replace-proprietary-software-open-source.

32 • Kashmira Gander, "Gaza Doctor Tarek Loubani Creates 3D Printed Stethoscopes to Alleviate Medical Supply Shortages Caused by Blockade." The Independent, September 10, 2015, accessed June 20, 2018, http://www.independent.co.uk/news/world/middle-east/gaza-doctor-tarek-loubani-creates-3d-printed-stethoscopes-to-alleviate-medical-supply-shortages-10495512.html.

33 • Glenn Greenwald, "How the NSA Tampers with US-made Internet Routers." The Guardian, May 12, 2014, accessed June 20, 2018, http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

34 • Sunil Abraham, "The Fight for Digital Sovereignty," *Economic & Political Weekly* XLVIII, no. 42 (October 19, 2013), accessed January 18, 2016, http://cis-india.org/a2k/blogs/epw-vol-xlviii-42-october-19-2013-sunil-abraham-the-fight-for-digital-sovereignty.

35 • Tania Wolfgramm, "Re-Claiming our Technological Sovereignty." Planet Maori, 2015, accessed June 20, 2018, http://planetmaori.com/Files/Content/2015/Re-Claiming_our_Technological_Sovereignty_-_Paper_-_Tania_Wolfgramm_2014.pdf.

36 • Francesca Bria, *Public Policies for Digital Sovereignty* (New York: OR Books, 2015).

37 • Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras." The Guardian, September 9, 2013, accessed January 18, 2016, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

38 • AFP, "NSA Spied on French Economy Ministers, Top Companies: Reports." Yahoo! News, June 30, 2015, accessed January 18, 2016, http://news.yahoo.com/nsa-spied-french-economy-ministers-top-companies-reports-061342870.html; see also Spiegel Staff, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin." Spiegel Online, October 27, 2015, accessed January 18, 2016, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

39 • "Plan de Implementación de Software Libre y Estándares Abiertos," Comité Plurinacional de Tecnologías de la Información y Comunicación - COPLUTIC, July 2016, accessed June 20, 2018, http://coplutic.gob.bo/rubrique3.html.

40 • "Free Software Designer in Bolivia," Prensa Latina, April 1, 2013, accessed January 18, 2016, http://www.ssig.gov.my/blog/2013/04/01/free-software-designer-in-bolivia.

41 • Dan Schiller, "Geopolitics and Economic Power in Today's Digital Capitalism." Presentation to the Hans Crescent Symposium, December 13, 2015, accessed June 20, 2018, http://informationobservatory.info/2015/12/14/geopolitics-and-economic-power-in-todays-digital-capitalism.

RENATA ÁVILA PINTO – *Guatemala*

Renata Avila, Guatemalan, is an international lawyer and digital rights advocate. Specialising in intellectual property and technology, her work addresses the crucial intersection between human rights, digital trade, information, technological change and the power disparities between the Global North and South. As a lawyer in Guatemala, Avila has represented indigenous victims of genocide and other human rights abuses, including the prominent indigenous leader and Nobel Peace Prize Laureate Rigoberta Menchu Tum.

As part of her longstanding advocacy work in the field of Internet and human rights, she leads with World Wide Web inventor Sir Tim Berners – Lee a global campaign to uphold human rights in the digital age in more than seventy-five countries. Avila sits on the Board of Creative Commons, is a trustee of the Courage Foundation - an organisation set up to assist whistleblowers at risk - and is an advisory board member of Diem25, exploring the potential of decentralised technologies in Europe. She is currently based in Belgrade and Guatemala, and is writing a book about Digital Colonialism and advises the Web Foundation on their new Digital Equality strategies. She also represents Civil Society at the OECD's Committee on the Digital Economy Policy.

email: *renata.avila@webfoundation.org*

Received in May 2018.
Original in English.