

Michigan Journal of Race and Law


Volume 24

2019

Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws

Danielle Coleman
University of Michigan Law School

Follow this and additional works at: <https://repository.law.umich.edu/mjrl>

 Part of the [Comparative and Foreign Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Danielle Coleman, *Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws*, 24 MICH. J. RACE & L. 417 (2019). Available at: <https://repository.law.umich.edu/mjrl/vol24/iss2/6>

This Note is brought to you for free and open access by the Journals at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Journal of Race and Law by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

DIGITAL COLONIALISM: THE 21ST CENTURY
SCRAMBLE FOR AFRICA THROUGH THE
EXTRACTION AND CONTROL OF USER DATA AND
THE LIMITATIONS OF DATA PROTECTION LAWS

Danielle Coleman[★]

ABSTRACT

As Western technology companies increasingly rely on user data globally, extensive data protection laws and regulations emerged to ensure ethical use of that data. These same protections, however, do not exist uniformly in the resource-rich, infrastructure-poor African countries, where Western tech seeks to establish its presence. These conditions provide an ideal landscape for digital colonialism.

Digital colonialism refers to a modern-day “Scramble for Africa” where large-scale tech companies extract, analyze, and own user data for profit and market influence with nominal benefit to the data source. Under the guise of altruism, large scale tech companies can use their power and resources to access untapped data on the continent. Scant data protection laws and infrastructure ownership by western tech companies open the door for exploitation of data as a resource for profit and a myriad of uses including predictive analytics.

One may believe that strengthening data protection laws will be a barrier to digital colonialism. However, regardless of their relative strength or weakness, data protection laws have limits. An analysis of Kenya's 2018 data protection bill, the General Data Protection Regulation (GDPR), and documented actions of large-scale tech companies exemplifies how those limits create several loopholes for continued digital colonialism including, historical violations of data privacy laws; limitations of sanctions; unchecked mass concentration of data, lack of competition enforcement, uninformed consent, and limits to defined nation-state privacy laws.

[★] Danielle Coleman - J.D. Candidate, May 2020, University of Michigan Law School. Danielle is an emerging movement lawyer in the tech space dedicated to the intersection of entrepreneurship, technology and Black lives. Thank you to Professor Laura Beny, my advisor, for her dedication in teaching and representation of Black excellence, Donna Scaffidi for her unparalleled support during this process, the Michigan Journal of Race & Law and its editors, especially Cleo Hernandez for ensuring this piece came to fruition and my family and friends who have supported me throughout my academic experiences.

TABLE OF CONTENTS

INTRODUCTION	418
I. COLONIZATION AND THE ROLE OF CORPORATIONS.....	419
II. DIGITAL COLONIALISM.....	422
A. <i>Defining Digital Colonialism</i>	422
B. <i>Data as a Resource</i>	424
III. LIMITATIONS OF DATA PROTECTION LAWS.....	431
A. <i>The General Data Protection Regulation (GDPR) and Kenya's Data Protection Laws</i>	431
B. <i>Violation of Data Privacy Laws</i>	433
C. <i>Limitations of Penalties, Fines, and Sanctions</i>	434
D. <i>Mass Concentration of Data and Lack of Competition Enforcement</i>	436
E. <i>Consent</i>	437
F. <i>Limits to Defined Nation-State Privacy Laws</i>	439
CONCLUSION	439

INTRODUCTION

To discuss the extraction, synthesis, and control of user data is to discuss the pulse of commerce, the ever-looming power of large tech companies, and the shift of human emotional interaction to everything in our daily lives. However, to discuss the extraction, synthesis, and control over user data and critical connectivity infrastructure by Western tech companies in African countries with limited infrastructure, limited data protection laws, and limited competition—combined with social, political and economic power imbalances and decades of resource pillaging—is to discuss digital colonialism.

This Note argues that digital colonialism is part of the modern day “Scramble for Africa” that takes place through the extraction and control of user data by large scale tech companies. Part I will establish the background of colonization and the role of corporations so as to enable the comparison between nineteenth century colonialism and twenty-first century colonialism. Part II will explain the definition of digital colonialism, why data is a rich resource comparable to natural resources, and how large tech companies exploit this resource for profit and for use in predictive analytics. Part III will explain the limits to the purported solution to digital colonialism—data protection laws—using examples from the General Data Protection Regulation (GDPR) and Kenya’s 2018 Data Protection Bill.

I. COLONIZATION AND THE ROLE OF CORPORATIONS

In the nineteenth century, many African countries faced imperialist aggression through military invasions, land conquests, economic exploitation, genocide, and violent resource extraction at the behest of European world powers. This colonialist rise began after the end of the Transatlantic slave trade and was formalized at the Berlin Colonial Conference, where soon to be colonial powers gathered to develop a plan that would upset and disrupt the social, economic, and political landscape of Africa forever.¹ Between 1884 and 1885, under the guise of White supremacy, deeply ingrained anti-Black sentiment, and unchecked power, European powers carved up the continent in what has become known as the “Scramble for Africa”—the creation of arbitrary lines equating to colonies, and the forced subjugation of African peoples.² At the end of the conference, the powers present signed the General Act of the Conference of Berlin, giving purported legal effect to their new territories under the baseless premise that African nations had no sovereignty and no legal claim over their state, land, or resources.³ This, coupled with the beliefs inherent within the White imagination that African peoples were “evolutionar[il]ly backward and undeveloped” and that “[i]t was a European responsibility to act as trustees of Africa until Africans were mature enough to govern themselves,”⁴ set the ideological tone for ruthless colonization.

European powers’ proliferation of claims in Africa were characteristically expeditious such that, by 1900, European states including Great Britain, France, Germany, Belgium, Portugal, Italy, and Spain had claimed nearly 90 percent of African territory.⁵ Due to the rise of industrial capitalism, there was a staunch belief that the economic, and thus political, future of an industrial country hinged on exclusive control of its markets and raw materials.⁶ Therefore, colonial powers stole from the

1. Stelios Michalopoulos & Elias Papaioannou, *The Long-Run Effects of the Scramble for Africa*, 106 AM. ECON. REV. 1802, 1807 (2016).

2. *See id.* at 1802.

3. Matthew Craven, *Between Law and History: The Berlin Conference of 1884-1885 and the Logic of Free Trade*, 3 LONDON REV. INT’L L. 31, 32 (2015).

4. Jennifer Tanabe, *Scramble for Africa*, NEW WORLD ENCYCLOPEDIA (May 11, 2015), http://www.newworldencyclopedia.org/p/index.php?title=Scramble_for_Africa&oldid=988092.

5. BERLIN CONFERENCE OF 1884–1885, OXFORD REFERENCE (2010), <http://www.oxfordreference.com/view/10.1093/acref/9780195337709.001.0001/acref-9780195337709-e-0467>.

6. A. ADU BOAHEN, *AFRICAN PERSPECTIVES ON COLONIALISM* 32 (1987).

lands of Africa, violently extracting raw materials such as copper, cotton, rubber, tea, gold, diamonds, and tin.⁷

At the center of this pillaging was a simple colonialist economic agenda, to provide maximum economic benefit at a minimal price.⁸ Accordingly, investing in industrialization, improving the production processes, or strengthening the overall economy of the colonies was not a priority.⁹ Oftentimes, the colonial powers refused to process the raw materials in-country, sending the raw materials to Europe to be processed, obliterating the role of Africans in the export business and robbing them of any economic profit and potential resource flow that could have derived from processing raw materials in country.¹⁰ Although some colonial powers did invest in transportation infrastructure such as railways, such investments were strictly for the benefit of facilitating the efficient transport of raw materials and not for the enrichment of the countries themselves.¹¹ Simply put, “the infrastructure that was developed was designed to exploit the natural resources of the colonies.”¹²

Corporations, aiding in this colonialist economic agenda, also played a dominant role in colonial expansion. As early as the seventeenth century, dozens of companies were granted trading monopolies by their respective governments throughout the world.¹³ Their monopoly over trade in specified territories allowed these corporations the power to safeguard this monopoly and the power to exert rights over their countrymen who lived and worked within the territory.¹⁴ The granting of monopoly status by colonialist governments made these highly risky ventures safer for investors with profit as the primary motive.¹⁵ Investing in trading companies emerged as one of the earliest forms of venture capital as, “money could be raised in return for shares, profits could be divided among shareholders, and shares could be transferred among members and outsiders.”¹⁶

7. See Felix K. Ekechi, *The Consolidation of European Rule, 1885-194*, in COLONIAL AFRICA, 1885–1939, at 27, 36 (Toyin Falola ed., 2002); Julius O. Adekunle, *West Africa*, in COLONIAL AFRICA, 1885–1939, at 377, 384 (Toyin Falola ed., 2002)

8. Joshua Dwayne Settles, *The Impact of Colonialism on African Economic Development* 8 (May 1, 1996) (unpublished thesis, University of Tennessee Honors Program) (on file with University of Tennessee, Knoxville).

9. *Id.* at 7.

10. BOAHEN, *supra* note 7, at 61–62.

11. Settles, *supra* note 9, at 10.

12. *Id.*

13. Janet McLean, *The Transnational Corporation in History: Lessons for Today?*, 79 IND. L.J. 363, 365 (2003).

14. *Id.*

15. *Id.*

16. *Id.*

After a brief hiatus, the nineteenth century saw the resurgence of trading companies as weapons wielded for colonial expansion and as additional revenue streams for the emerging economic system of industrial capitalism.¹⁷ By then, the experience of companies from the seventeenth and eighteenth centuries such as the British East India Company had helped establish the corporate form as a dominant force for settlement and colonization.¹⁸ This second wave of colonization by trading companies proved to be robust, as “more than 75 percent of British acquisitions south of the Sahara were acquired by chartered companies”—not by equitable trading practices, but by monopolized consent, violence, and a virtual absence of competition in extracting raw materials and resources.¹⁹

The four major trading companies of the nineteenth century consisted of the British South African Company, the Germany East African Company, the Imperial British East African Company, and the Royal Niger Company.²⁰ Over the span of decades, trading companies expanded indirect colonial rule through possessing new “protectorates or spheres of influence”,²¹ exploited local faction rivalries, arming them in exchange for better trading deals,²² and established para military forces to facilitate trading goals and increase profit,²³ laying the foundation for the eventual mass exploitation of mineral resources and agricultural opportunities across Africa including Niger, Nigeria, South Africa, Central Africa, and East Africa.²⁴ The control of territories by companies established for the “explicit purpose of making money, meant, inevitably, that the territories were administered simply for profit,” and that the companies took no in-

17. *Id.* at 368.

18. *Id.* at 370.

19. McLean, *supra* note 14, at 370.

20. EUGENE STALEY, *Modern Chartered Companies, in WAR AND THE PRIVATE INVESTOR* (1937), <https://net.lib.byu.edu/estu/wwi/comment/investor/Staley11.html>.

21. William Reno, *Order and commerce in turbulent areas: 19th century lessons, 21st century practice*, 25 *THIRD WORLD QUARTERLY* 607, 613 (2006), <https://www.tandfonline.com/doi/full/10.1080/01436590410001678889>

22. *Id.* at 611.

23. STALEY, *supra* note 20. (“In connection with the colonial expansion of Europe in the late nineteenth century, there appeared a brief revival of the type of organization known as the chartered company. The hallmark of these— called privileged companies or sovereign companies—was their possession of authority to govern as well as to carry on commerce in territory placed under their jurisdiction. They were empowered to establish forts and police systems, to lay out roads, encourage colonization, levy duties and taxes.”); See also *British South Africa Company*, *ENCYCLOPEDIA BRITANNICA* (2018), <https://www.britannica.com/topic/British-South-Africa-Company>.

24. BOAHEN, *supra* note 7, at 61-62.

terest in developing local industrialization outside of its benefits for administering the movement of natural resources and raw materials.²⁵

Although these companies were principally chartered to facilitate “trade,” they were also legal extensions of the crown, a fact that afforded them the right to assert sovereign powers over the non-European peoples within the colony—a power they frequently exerted.²⁶ Trading companies gradually became more intrusive in the governance of the colonies to further their economic interests and those of the colonial powers.²⁷ As the intrusion grew, more demands were made on non-European states, through threat of military action, to concede to the interests of the trading companies.²⁸ Eventually, chartered companies, as extensions of the crown, were an authoritative force in territories, playing an imperative role in territorial annexations and profiting from raw materials and valuable minerals—their primary reason for existing.²⁹

Steeped in desperation to serve the industrial capitalist structure built upon the backs of African people and lands—the foundation for neo-mercantilism—colonial powers violently took over nations and exploited resource-rich African lands for their own economic benefit and global economic prowess, both directly and via chartered companies.

II. DIGITAL COLONIALISM

A. *Defining Digital Colonialism*

Earlier colonialists arrived on African shores to expand their empires by exploiting local labor to extract valuable natural resources and raw materials, building critical infrastructure like railroads in the process to facilitate the import and export of these often dispossessed goods.³⁰ Today’s colonialists, however, are digital. They build communication infrastructures such as social media platforms and network connectivity for the express purpose of harvesting data, churning a profit, and/or storing the data as raw material for predictive analytics.³¹

“Digital colonialism” is the decentralized extraction and control of data from citizens with or without their explicit consent “through com-

25. ANTONY ANGHIE, *IMPERIALISM, SOVEREIGNTY AND THE MAKING OF INTERNATIONAL LAW* 68 (2007).

26. *Id.* at 68-69.

27. *See id.*

28. *See id.* at 68, 72.

29. STALEY, *supra* note 20.

30. *See generally* Michael Kwet, *Digital Colonialism: US Empire and the New Imperialism in the Global South* 60 *RACE & CLASS* 3 (2019).

31. *Id.*

munication networks developed and owned by Western tech companies.”³² As professors Hendricks, Marker, and Vestergaard from the University of Copenhagen posit, this structure has four fundamental actors:

- (1) The Western tech companies who create and provide the technology and infrastructure that harvest the data for ad targeting and ad distribution;³³
- (2) The advertising and consulting firms who use the technology provided by (1) to target various groups with highly personalized ads and messages aimed at increasing profits;³⁴
- (3) The “local companies, parties, and organizations who pay (2) to help them impose their different agendas for the respective countries”;³⁵ and
- (4) The citizens who knowingly and unknowingly act as data sources for (1) and as target groups for (2) and (3).³⁶

Scholar Michael Kwet further explains:

Under digital colonialism, foreign powers, led by the United States, are planting infrastructure in the Global South engineered for its own needs, enabling economic and culture domination while imposing privatized forms of governance. To accomplish this task, major corporations design digital technology to ensure their own dominance over critical functions in the tech ecosystem. This allows them to accumulate profits from revenues derived from rent (in the form of intellectual property or access to infrastructure) and surveillance (in the form of Big Data). It also empowers them to exercise control over the flow of information (such as the distribution of news and streaming services), social activities (like social networking and cultural exchange) and a plethora of other politi-

32. Silas L. Marker, Mads Vestergaard & Vincent F. Hendricks, *Digital Colonialism on the African Continent*, 10 AFR. STAT. NEWSL. 6, 6 (Jan. 2019), https://www.uneca.org/sites/default/files/PageAttachments/asn_jan_2019_v_10_no1_v1_.pdf.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

cal, social and economic and military functions mediated by their technologies.³⁷

Laying critical connectivity infrastructure owned by Western tech companies, to extract and control untapped user data, however, is the vanguard for this cultural and economic dominance. The extraction, analysis, and control of data in African countries with limited infrastructure, limited data protection laws, and limited competition, combined with social, political, and economic power imbalances and decades of resource pillaging is what gives the above consequences true power.

B. *Data as a Resource*

According to the Oxford New English Dictionary, currency is defined as a system of assets, property, and resources owned by someone or something in general use in a particular country.³⁸ Data is the new currency, and access to data—rather than money, natural resources, or advanced weaponry—is now the most valuable asset available to nation-states and corporations.³⁹ This development lays the foundation for large Western tech companies' movement into African markets.

Data is collected by corporations of all sizes through online behavioral tracking technology which “refers to the practice of tracking web users (and mobile apps users) on the Internet”⁴⁰ This technology records a large variety of data including, but not limited to, ad clicks, device specific information, face scan, ISP, ad name, phone numbers, search queries, time, date, browser history, email addresses, IP addresses, location, operating system, and profile information.⁴¹ The method of tracking this data includes, but is not limited to, cookies, doubleclick and Adsense, profile information, device tracking technology, facial recognition software, and search queries.⁴² Collectively, this data creates an “anonymous” digital profile of millions of users that is ultimately used to integrate multiple accounts to produce personalized content for location services and

37. Kwet, *supra* note 28, at 7–8.

38. *Currency*, ENGLISH OXFORD DICTIONARY ONLINE, <https://en.oxforddictionaries.com/definition/currency> (last visited Dec. 21, 2018).

39. *Data is the New Currency of Geopolitics*, CIPHER BRIEF (Sept. 16, 2018), https://www.thecipherbrief.com/column_article/data-is-the-new-currency-of-geopolitics.

40. Ankur Arora & Monika Arora, *Digital-Information Tracking Framework Using Blockchain*, 7 J. SUPPLY CHAIN MGMT. SYS. 1, 1 (2018).

41. Mark van Rijmenam, *What Data Do The Five Largest Tech Companies Collect - Infographic*, DATAFLOQ (July 15, 2018), <https://datafloq.com/read/what-data-do-the-five-largest-tech-companies-colle/427>.

42. *Id.*

notification, and, most importantly, to be sold to data brokers, used as a means for selling access to users for targeted advertising by third party corporations, or collected and stored for future predictive analytic use.⁴³ With over 1.25 billion people living in Africa,⁴⁴ this market represents a treasure trove of data, much of which is as yet untapped by Western tech companies.⁴⁵

Due to this robust and efficient online behavioral tracking technology, consumerism has now shifted from a story of mass consumption to a “story of one.”⁴⁶ Because of the rapid development of portable technological devices like iPhones, smart watches and tablets, coupled with the constant and ever-increasing use of social media across generations,⁴⁷ the potential for consumer engagement can now operate twenty-four hours a day, making the transition from mass advertising to targeted advertising a lucrative pursuit. Now, advertisers no longer must make assumptions about consumers’ behavior⁴⁸ and can instead target consumers with extreme precision based on hyper-personalized data.⁴⁹

This helps corporations attract new business and “maximize engagement among target audiences,” resulting in a higher return on investment,⁵⁰ and creating a more efficient and cost-effective process for

43. Suneel Grover, *Big Digital Data, Analytic Visualization, and the Opportunity of Digital Intelligence*, SAS INSTITUTE INC. (2014), <https://support.sas.com/resources/papers/proceedings14/SAS171-2014.pdf>; Steven Melendez & Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, FAST COMPANY (2019), <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information>.

44. Benjamin Elisha Sawe, *How Many People Live In Africa?*, WORLD ATLAS (2018), <https://www.worldatlas.com/articles/how-many-people-live-in-africa.html>.

45. Acha Leke & Landry Signé, *Africa’s Untapped Business Potential: Countries, sectors, and strategies*, https://www.brookings.edu/wp-content/uploads/2019/01/BLS18234_BRO_book_006.1_CH5.pdf (last visited July 5, 2019).

46. Michelle Evans, *Why Data Is The Most Important Currency Used In Commerce Today*, FORBES (Mar. 12, 2018), <https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/#be5259854eb3>.

47. *Percentage of U.S. population with a Social Media Profile from 2008 to 2019*, STATISTA (2018), <https://www.statista.com/statistics/273476/percentage-of-us-population-with-a-social-network-profile/> (last visited Dec. 17, 2018).

48. Rebecca Walker Reczek, Christopher Summers & Robert Smith, *Targeted Ads Don’t Just Make You More Likely to Buy - They Can Change How You Think About Yourself*, HARV. BUS. REV. (Apr. 4, 2016), <https://hbr.org/2016/04/targeted-ads-dont-just-make-you-more-likely-to-buy-they-can-change-how-you-think-about-yourself>.

49. Louise Matsakis, *Facebook’s Targeted Ads Are More Complex Than It Lets On*, WIRED (May 25, 2018), <https://www.wired.com/story/facebooks-targeted-ads-are-more-complex-than-it-lets-on/>.

50. Chris Dobson, *Targeted Advertising Requires Good Data*, FORBES (Apr. 5, 2018), <https://www.forbes.com/sites/forbestechcouncil/2018/04/05/targeted-advertising-requires-good-data/#4a1537fd29db>.

promotion, price point decision making, and distribution of products and/or services.⁵¹ Within the modern capitalist society, this is the most valuable information any company can possess.

However, the value of this data is based on the ability to “make sense of the avalanche of data,”⁵² and companies like Alphabet and Facebook have a leading edge due to their size, access to data, resources, and data science infrastructure.⁵³ For less robust companies and marketers, harnessing data effectively can be challenging,⁵⁴ as “the abundance of data produced by disparate sources has made the task of identifying and unifying relevant insight seem colossal.”⁵⁵ The inherent technical challenges in turning large stores of data into valuable currency means that behemoths like Alphabet and Facebook are well-positioned to dominate new large markets with their highly-equipped platforms and resources by synthesizing the data into usable information, effectively controlling the market.

Artificial intelligence, specifically machine learning and natural language processing, gives companies the capability to better synthesize billions of data points and make inferences about users.⁵⁶ This data can be used to infer personal information such as a person’s background, religion and beliefs, political views, sexual orientation and gender identity, social connections, health, ethnicity, income levels, educational attainment, marital status, family composition, financial stability, and creditworthiness, all without the user directly giving this information.⁵⁷ “The result is the creation and amalgamation of digital footprints that provide in-depth knowledge about [one’s] life.”⁵⁸ This data is eventually synthesized, used, and sold for immense profit.⁵⁹

What is more alarming is that a handful of tech companies, like Alphabet and Facebook, are able to use artificial intelligence for predictive analytics, which is “the use of data, statistical algorithms and machine learning techniques to identify the likelihood of future outcomes based

51. Susan Ward, *Use Target Marketing & Market Segmentation to Improve Your Bottom Line*, BALANCE SMALL BUS. (Dec. 8, 2018), <https://www.thebalancesmb.com/target-marketing-2948355>.

52. Evans, *supra* note 43.

53. *Id.*

54. Dobson, *supra* note 47.

55. *Id.*

56. Vivian Ng & Catherine Kent, *Smartphone Data Tracking Is More Than Creepy – Here’s Why You Should Be Worried*, THE CONVERSATION (Feb. 7, 2018), <https://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110>.

57. *Id.*

58. *Id.*

59. *Id.*

on historical data.”⁶⁰ The goal is to go beyond knowing what is happening and what has happened to provide a best assessment of how users will behave in the future.⁶¹ Although predictive analytics can have positive effects in many sectors, such as the healthcare industry, they can also distort the lines of privacy when dealing with individualized human behavior, particularly when only a handful of companies have this information.

These possible intrusions into basic concepts of privacy can be seen in Facebook’s uncanny ability to predict when a person is motivated to do something,⁶² when a person is feeling a range of emotions, such as feeling down,⁶³ and when a couple’s relationship will end⁶⁴—all before the users even know it themselves. Predictive analytics allows a handful of companies to understand even the innermost emotions, and to predict how this will affect future behavior. This information is extremely useful to millions of corporations across the globe. It can affect the global economy, workforce development, small and large scale investments, resource allocation, advertising, presidential elections, and every single segment of global capitalism.

Furthermore, since machines are not humans and cannot “think,” artificial intelligence needs gargantuan sets of data to “learn” from and derive its predictive accuracy—to which only a handful of corporations have access. Facebook itself has access to over two billion people’s sensitive information, including what they “like” and “dislike,” who their friends are, to whom they talk the most, and where they physically travel⁶⁵—a level of intimate personal data that no other company in the world has. Google dominates search engines with the ability to collect data on over 1.17 billion global users.⁶⁶ Companies like Facebook and Google then use these highly personal inferences and sensitive data as a means of selling access to individuals to third-party corporations⁶⁷—

60. *Predictive Analytics: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/predictive-analytics.html (last visited Dec. 22, 2018).

61. *Id.*

62. Matsakis, *supra* note 46.

63. *Id.*

64. Alexis Kleinman, *Facebook Can Predict With Scary Accuracy If Your Relationship Will Last*, HUFFPOST (Dec. 6, 2017), https://www.huffingtonpost.com/2014/02/14/facebook-relationship-study_n_4784291.html.

65. Kwet, *supra* note 28, at 11.

66. Felix Richter, *1.17 Billion People Use Google Search*, STATISTA (Feb. 12, 2013), <https://www.statista.com/chart/899/unique-users-of-search-engines-in-december-2012/>.

67. Kurt Wagner, *This Is How Facebook Uses Your Data for Ad Targeting*, RECODE (Apr. 11, 2018), <https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg>.

making 40 billion dollars in 2017 alone.⁶⁸ Additionally, when only a select few companies have access to the largest sets of valuable data, they have a supreme advantage over competitors, ultimately controlling that market and deciding who gets access, both presently and in the future, while making the most profit.⁶⁹

For tech companies, the treasure trove of citizens' data that lies in Africa is a natural resource. The data may be extracted and sold as a commodity to corporations and political interests who base their revenue model on knowing their target groups so that they are able to push political messages and agendas or sell targeted products to citizens, thereby increasing their bottom-line.⁷⁰ The essence of this business model is already established in the West. Tech companies "provide seemingly free communication services and search engines" and track users across platforms, apps and the internet, all to enable advertisers to target consumers and voters with hyper-personalized ads based on behavioral patterns, making an enormous profit. However, when this business strategy is pursued in countries with limited infrastructure, limited data protection laws, and limited competition—while rooted in neoliberal notions of human rights—it transitions from a business model into a form of digital colonialism.

Facebook's Free Basics and Project Aires, and Google's Project Csquared and Project Loon, are just a few projects deployed by Western tech companies in Africa as they expand their global reach for profit.⁷¹ Much like the colonialists of the nineteenth and twentieth centuries, who built critical infrastructure like railroads for the sole purpose of continuing to economically exploit the natural resources of Africa, giant tech companies like Facebook and Alphabet are building network connectivity infrastructure for the benefit of profiting from the use of their online

68. Press Release, Facebook, Facebook Reports Fourth Quarter and Full Year 2017 Results (Jan. 31, 2018), <https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx>.

69. Kwet, *supra* note 28, at 11.

70. Marker et al., *supra* note 30, at 6.

71. Paul Sawers, *Google and Partners Commit \$100 Million to African Broadband Project CSquared*, VENTUREBEAT (May 16, 2017), <https://venturebeat.com/2017/05/16/google-and-partners-commit-100-million-to-african-broadband-project-csquared/>; Tom Simonite, *Project Loon*, MIT TECH. REV. (Mar./Apr. 2015), <https://www.technologyreview.com/s/534986/project-loon/>; Njeri Wangari Wanjohi & Kofi Yeboah, *Free Basics: Facebook's Failure at 'Digital Equality'*, AL JAZEERA (Aug. 31, 2017), <https://www.aljazeera.com/indepth/opinion/2017/08/free-basics-facebook-failure-digital-equality-170828083453067.html>; Frederic Lardinois, *Facebook's Terragraph and ARIES Antennas Bring Internet to Underserved Areas*, TECHCRUNCH (Apr. 13, 2016), <https://techcrunch.com/2016/04/13/terragraph/>.

services, rather than building local infrastructure for sustained economic development in African countries.

In 2017, Google and its partners committed \$100 million to Csquared, a broadband project in Africa aimed at providing high-speed, affordable, and reliable connectivity infrastructure to further grow internet access in Africa.⁷² This is a laudable goal; however, by “doubling down on its efforts to support the underlying internet infrastructure, which, in turn, opens up new markets for the internet giant’s own online services,” it increases their access to data.⁷³ In 2012, the idea for Project Loon was born in order to get billions of people online where cell towers do not exist via helium balloons.⁷⁴ This type of technological advancement could be revolutionary for rural communities and other places in which millions of people are in desperate need for internet access yet physical hardware connectivity is not always possible, particularly after natural disasters. However, as scholar Tom Simonite in the MIT Technology Review notes:

It is odd for a large public company to build out infrastructure aimed at helping the world’s poorest people. But in addition to Google’s professed desires to help the world, the economics of ad-supported Web businesses give the company other reasons to think big. It’s hard to find new customers in Internet markets such as the United States. Getting billions more people online would provide a valuable new supply of eyeballs and personal data for ad targeting.⁷⁵

Although software is not technically infrastructure, it is also central to the overall development of technological connectivity being used to harvest data for economic profit. Free Basics, Facebook’s mobile application, gives users in developing nations access to limited online services and content for free. “Fundamentally, Free Basics is a *data-lite* mobile application that allows users to browse a narrowed down version of the internet”⁷⁶ as an “on ramp” to introduce internet to those who otherwise would not have access.⁷⁷ By using neoliberal code words like “democra-

72. Sawers, *supra* note 69.

73. *Id.*

74. Simonite, *supra* note 69.

75. *Id.*

76. Kush Fanikiso, *Free Basics and the Age of Digital Colonialism*, MEDIUM (Sept. 23, 2017), <https://medium.com/@makushline/free-basics-and-the-age-of-digital-colonialism-329e1041477e>.

77. See Ellery Roberts Biddle, Opinion, *The More We Connect, the Better It Gets - for Facebook*, N.Y. TIMES (Sept. 26, 2017), <https://www.nytimes.com/2017/09/26/opinion/facebook-free-basics.html>.

cy,” “equality,” and “internet as a basic human right,” Facebook masks its true long-term goal of collecting data on “the next billion.”⁷⁸ Free Basics harvests an enormous amount of metadata on users.⁷⁹ When a user clicks on a website in Free Basics, “that click sends packets of data to Facebook’s servers.”⁸⁰ Furthermore, “[s]ince all of the data exchanged on Free Basics goes through Facebook’s Proxy servers, Facebook now has a way to access users [sic] data outside of Facebook.”⁸¹ Research by Citizen Media and activist group Global Voices found that the Free Basics program has enabled Facebook to gather data about the habits, interests, and behaviors of users in the developing world, where Facebook aspires to have a strong presence as more users come online.⁸² In sum, “Free Basics is a closed space where Facebook picks the content—and profits from users’ data along the way—creating what some people call a ‘poor internet for poor people.’”⁸³

Only 31 percent of people on the continent of Africa have access to the internet,⁸⁴ making it clear that Africa faces connectivity, access, and infrastructure issues. However, it is by no means certain that this is a problem for foreign tech companies.⁸⁵ Due to this lack of infrastructure and connectivity, giant tech companies are acting as the “White savior,” much like colonial powers who disguised the Scramble for Africa as liberalization intended to help the “noble savage.” These companies claim that they want to bridge the digital divide and give internet access to the millions of people who otherwise would not have it, but their true purpose is simply to extract data for profit and predictive analytics.

Furthermore, by capitalizing on “‘first mover’ advantage” with an army of lawyers and operating on such a massive scale, giant tech companies face extremely limited competition, both locally and internationally, and can outcompete or simply buy up competitors around the world.⁸⁶

78. Olivia Solon, *‘It’s Digital Colonialism’: How Facebook’s Free Internet Service Has Failed Its Users*, THE GUARDIAN (July 27, 2017), <https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets>.

79. *Id.*

80. Biddle, *supra* note 75.

81. Fanikiso, *supra* note 74.

82. *Can Facebook Connect the Next Billion?*, GLOBAL VOICES: ADVOX (JULY 27, 2017), <https://advox.globalvoices.org/2017/07/27/can-facebook-connect-the-next-billion/>.

83. Biddle, *supra* note 75.

84. Monique Maddy, *The Intensifying Battle for Africa’s Burgeoning Tech Landscape*, TECHCRUNCH (Feb. 23, 2018), <https://techcrunch.com/2018/02/23/the-intensifying-battle-for-africas-burgeoning-tech-landscape-2/>.

85. Fanikiso, *supra* note 74.

86. Xavier Harding, *Facebook Makes Money by Selling Your Data, But Why Can’t Users Just Pay for the Site Instead?*, MIC (Mar. 20, 2018), <https://mic.com/>

Much like chartered companies in the nineteenth century, who used limited trade competition to create monopolistic economic control within the colonies, these giant tech companies can control how the connectivity infrastructure is built, what apps and services users have access to, and what happens to the data due to the lack of competition. With Free Basics spanning sixty countries, reaching hundreds of millions of mobile phone users in Africa alone,⁸⁷ Facebook has the most data points about new users from emerging markets, and the best resources to synthesize this data into usable information—more than the majority of other companies in the market and most governments.⁸⁸ This makes Facebook the centerpiece of control for extremely valuable data sets, at no benefit to the users or the countries themselves.

III. LIMITATIONS OF DATA PROTECTION LAWS

Some scholars believe that the digital colonialism as described in Part II, is enhanced by scant data protection laws in Africa that leave users exposed.⁸⁹ However, the limits to data protection laws, which occur regardless of the relative strength or weakness of the laws, are overwhelming and fail to provide a panacea to digital colonialism. This Part describes these limitations and how they operate.

A. *The General Data Protection Regulation (GDPR) and Kenya's Data Protection Laws*

The General Data Protection Regulation (GDPR), which came into force on May 25, 2018, is now the world's strongest data protection law.⁹⁰ It applies to European companies broadly, as well as any company across the globe that collects data on its citizens. Designed to modernize

articles/188528/facebook-makes-money-by-selling-your-data-but-why-cant-users-just-pay-for-the-site-instead#.YxXwmlKa1.

87. Biddle, *supra* note 75.

88. Jon Russell, *Government Requests for Facebook User Data Continue to Increase Worldwide*, TECHCRUNCH (Dec. 18, 2017), <https://techcrunch.com/2017/12/18/government-requests-for-facebook-user-data-continue-to-increase-worldwide/>.

89. See generally, e.g., Maggie Fick & Alexis Akwagyiram, *In Africa, Scant Data Protection Leaves Internet Users Exposed*, REUTERS (Apr. 4, 2018), <https://www.reuters.com/article/us-facebook-africa/in-africa-scant-data-protection-leaves-internet-users-exposed-idUSKCN1HB1SZ>.

90. Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Jan. 21, 2019), <https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018>.

laws that protect sensitive and personal information of users,⁹¹ this law “reshape[s] how technology companies store, process, and profit from users’ personal information.”⁹² It also gives the user the “right to be forgotten,” as well as the right to withdraw their data from collection.⁹³

GDPR has elevated the standard for data protection laws globally, and yet in Africa, there is no continent-wide consensus of an approach to personal data protection, as some countries have little to no data protection laws or constitutional protections, while others have robust data protection laws.⁹⁴ Based on 2017 data, there are seventeen countries in Africa that have enacted comprehensive personal data protection legislation. Three more countries, Kenya, Uganda and Zimbabwe, have enacted personal data protection legislation that is currently moving through the lawmaking process. In addition, the African Union (AU) adopted the AU Convention on Cybersecurity and Data Protection (AU Convention) in June 2014,⁹⁵ which provides “a personal data protection framework which African countries may potentially transpose into their national legislation.”⁹⁶ However, the AU Convention has only been ratified by four of the fifty-four AU member jurisdictions and needs to be ratified by fifteen member jurisdictions in order to take effect.⁹⁷ Nevertheless, there are common themes and principles between the GDPR and comprehensive data protection legislation adopted by some African countries.⁹⁸ These themes comprise

- notice;
- choice and consent;
- data security;
- data access and correction;
- data quality and integrity;

91. *Id.*

92. Abdi Latif Dahir, *Africa Isn't Ready to Protect Its Citizens Personal Data Even as EU Champions Digital Privacy*, QUARTZ: AFRICA (May 8, 2018), <https://qz.com/africa/1271756/africa-isnt-ready-to-protect-its-citizens-personal-data-even-as-eu-champions-digital-privacy/>.

93. *Id.*

94. DELOITTE, *PRIVACY IS PARAMOUNT: PERSONAL DATA PROTECTION IN AFRICA 5* (2017), https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf [hereinafter *Privacy is Paramount*].

95. Cynthia Rich, *Privacy Laws in Africa and the Near East*, BNA 1 (Sept. 11, 2017), <https://media2.mofo.com/documents/170911-privacy-africa.pdf>.

96. *Privacy is Paramount supra* note 92, at 6.

97. African Union Convention on Cyber Security and Personal Data Protection, art. 36, June 27, 2014.

98. *Privacy is Paramount, supra* note 92, at 6.

- data retention and destruction;
- registration with a data protection authority (DPA);
- cross-border data transfers;
- personal data breach notification; and
- appointment of a data protection officer (DPO).⁹⁹

Many of these themes are incorporated in Kenya's 2018 Data Protection Bill (DPB), which is said to mirror the GDPR.¹⁰⁰ Once passed, it will give Kenyan citizens a series of rights including: 1) the right to ask companies to clearly explain, using accessible language, how their personal data is being collected, used, and stored; 2) the right to request that their personal data be deleted; and 3) the right to object to their personal data being used for specific purposes like targeted advertising.¹⁰¹ This will also require companies to gain consent from users before collecting their data.¹⁰² The DPB is all-encompassing, applying to "all data subjects, regardless if they reside in Kenya, whose data is, or has been, collected or processed by a data controller in Kenya."¹⁰³ However, this bill has received much scrutiny,¹⁰⁴ and many provisions, much like some in the GDPR, reflect the limits of data protection laws against digital colonialism.

Once enacted, the Bill will give effect to Article 31(c) and Article 31(d) of the 2010 Constitution of Kenya, which guarantees every person the right not to have "information relating to their family or private affairs unnecessarily required or revealed," and the right not to have "the privacy of their communications infringed."¹⁰⁵ This will directly tie this law to the Constitution of Kenya, the supreme law of the land, which is binding on all persons.

B. *Violation of Data Privacy Laws*

Unfortunately, big tech companies can violate (and have blatantly violated) these laws, since they have the time, money, and resources to fight for their desired outcomes, even if they stand in direct violation of pre-established laws. For example, Uber has flaunted its willingness to

99. *Id.*

100. Brian Obilo, *Kenya Data Protection Bill 2018*, INTERNET YETU (Aug. 25, 2018), <https://internetyetu.org/kenya-data-protection-bill-2018/>.

101. *Id.*

102. *Id.*

103. *Id.*

104. *See, e.g., Comments on the Proposed Regulation Data Protection Bill*, FSD KENYA (July 23, 2018), <http://fsdkenya.org/blog/regulation-data-protection-bill-public-comments/>.

105. *See* Obilo, *supra* note 89.

operate in clear violation of local laws, launching in cities where its operation violates city ordinances.¹⁰⁶ “The company’s non-compliance with city ordinances ranges from Uber drivers not having the required driving permits to refusing a request by California state regulators to provide information about their drivers.”¹⁰⁷ Uber’s violation of the law extends globally—a French Court in 2016 convicted Uber of violating French transport and privacy laws.¹⁰⁸

Additionally, Google Books made a clear and public move to violate copyright law.¹⁰⁹ The goal of Google Books was to scan millions of books into digital format to add to their search engine, despite the project’s clear violation of age-old copyright laws.¹¹⁰ At this legal battle’s inception, approximately 24 million titles were under copyright protection. The potential cost for Google infringing on each work totaled 3.6 trillion, and yet Google forged ahead.¹¹¹ After a nearly decade-long legal battle, Google prevailed, and the courts upheld their fair-use claims.¹¹²

These examples from the Global North indicate that the presence of a comprehensive data protection legislation does not mean that large tech companies will actually comply if the benefit of violation exceeds the burden of consequence. This also proves the limits to penalties, fines, and sanctions against large tech companies—digital colonialism’s most prominent purveyors.

C. Limitations of Penalties, Fines, and Sanctions

GDPR fines for offenses are the greater sum of up to 20 million euros or 4 percent of a firm’s global turnover.¹¹³ However, if Google was willing to risk paying 3.6 trillion for a clear violation of law, arguably it would be willing to risk paying the GDPR penalty. That is, if the violation is worth it for the company, or if they have the resources to defend the alleged violation in court, the company may go ahead with its ac-

106. Jordan Golson, *Uber Used an Elaborate Secret Program to Hide from Government Regulators*, THE VERGE (Mar. 3, 2017), <https://www.theverge.com/2017/3/3/14807472/uber-greyball-regulators-taxi-legal-vtos>.

107. Anjuan Simmons, *Technology Colonialism*, MODEL VIEW CULTURE (Sept. 18, 2018), <https://modelviewculture.com/pieces/technology-colonialism>.

108. Sam Schechner, Douglas MacMillan & Nick Kostov, *French Court Convicts Uber of Violating Transport, Privacy Laws*, WALL STREET J. (June 9, 2016), <https://www.wsj.com/articles/french-court-convicts-uber-of-violating-transport-privacy-laws-1465477861>.

109. Simmons, *supra* note 105.

110. *Id.*

111. Jonathan Band, *The Long and Winding Road to the Google Books Settlement*, 9 J. MARSHALL REV. INTELL. PROP. L. 227, 229 (2009).

112. Simmons, *supra* note 105.

113. Burgess, *supra* note 85.

tions, even if it knows they are likely to be in violation. Kenya's DBP on the other hand, is silent on penalties or fines against corporations found to be in violation of the data protection law, leaving it up to the complaints commission to decide the course of action.¹¹⁴ Although this is a better proposition considering that the complaint commission may be able to exercise more effective sanctions that would serve as greater deterrents for large tech companies than monetary fines, there is still a loophole. Large tech companies and data brokers could simply dissolve before they ever have to face any accountability measures. This is the current predicament of Cambridge Analytica.

Cambridge Analytica, a data firm, harvested the personal data of approximately 50 million Americans and at least one million Brits through Facebook.¹¹⁵ This data was ultimately used to influence the 2016 U.S. Presidential Election of Donald Trump, as demonstrated by Cambridge Analytica's CEO, who was caught via secret recording claiming direct credit for the election of Donald Trump.¹¹⁶ Additionally, senior executives were "filmed describing its dominant role in Kenyan President Uhuru Kenyatta's election campaigns in 2013 and 2017 and were caught boasting about psychological manipulation, entrapment techniques and fake news campaigns."¹¹⁷ The Information Commissioner's Office, a UK independent authority, is prosecuting SCL Elections, Cambridge Analytica's parent company, for failing to comply with an enforcement notice.¹¹⁸ However, SCL Elections filed bankruptcy in May and will be completely dissolved by the January 2019 trial date.¹¹⁹ The ICO is examining whether the SCL Elections directors can still be pursued; however, it seems that this major data firm will escape unscathed despite their clear violation of pre-GDPR protection laws.¹²⁰ All of this sets the foundation for the potential abuse of power by large tech companies who can blatantly violate

114. Frankline Sunday, *Data Protection Bill 2018*, STANDARD DIGITAL (June 24, 2018), <https://www.standardmedia.co.ke/business/article/2001285254/data-protection-bill-2018>.

115. Cat Contiguglia, *Cambridge Analytica Shutting Down*, POLITICO (May 3, 2018), <https://www.politico.eu/article/cambridge-analytica-shutting-down/>.

116. *Id.*

117. Justin Crabtree, *Here's How Cambridge Analytica Played a Dominant Role in Kenya's Chaotic 2017 Elections*, CNBC (Mar. 23, 2018), <https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html>.

118. Gareth Corfield, *Cambridge Analytica's Daddy Pleads Not Guilty to Ignoring Data Notice*, THE REGISTER (Oct. 4, 2018), https://www.theregister.co.uk/2018/10/04/scl_elections_pleads_not_guilty_data_notice_cambridge_analytica/.

119. See Alex Hern & David Pegg, *Facebook Fined for Data Breaches in Cambridge Analytica Scandal*, THE GUARDIAN (July 10, 2018), <https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal>.

120. *Id.*

laws and skirt fines, penalties and sanctions, leaving the local citizens whom they exploit for data extraction powerless, despite clear data protection laws.

D. *Mass Concentration of Data and Lack of Competition Enforcement*

Another clear limit to data privacy laws is that the lack of protection against the mass concentration of data by dominant players is compounded by the lack of competition enforcement measures. Competition, data protection, and consumer protection law are inextricably related, and data privacy legislation often does not take this into account—Kenya’s DPB included. Without these protections, enormous amounts of data will be centrally held and owned by dominant players who have the resources to stomp out their competition, leaving the fate of millions and sometimes billions of people’s personal and sensitive data in the hands of a select few.

This was particularly visible in the merger decision for Facebook and WhatsApp. Facebook already had a lion’s share of the data market, with access to over 2 billion users’ data. The “main reason for Facebook’s interest in WhatsApp is believed to lie in the troves of data that came with the acquisition”¹²¹—namely, 500 million users. This was also a strategic acquisition to help Facebook fuel growth in developing markets, opening up data extraction opportunities for over 172 million WhatsApp users in Africa.¹²² The lack of protection against mass concentration of data and the lack of regulation of anti-competitive conduct by companies fuels the concentration of mass data, as there are no regulations within data privacy law that apply when a company has either 1) simply amassed too much data at the risk of users or 2) has amassed too much data at the risk of users through means of acquisitions, decreasing market competition.

Additionally, this hole creates a high barrier of entry for small, medium, and local tech companies who simply cannot compete with global tech companies. The cost for running centralized social networks is extremely expensive. A company must pay for costly cloud infrastructure, find and pay skilled programmers, and be able to pay for quality data col-

121. Inge Graef, *European Commission Approves Facebook/WhatsApp Deal: Data Concentration and Privacy as Competition Concerns?*, MEDIA POL’Y PROJECT BLOG (Oct. 17, 2014), <http://blogs.lse.ac.uk/mediapolicyproject/2014/10/17/european-commission-approves-facebookwhatsapp-deal-data-concentration-and-privacy-as-competition-concerns/>.

122. Abdi Latif Dahir, *Whatsapp is the Most Popular Messaging App in Africa*, QUARTZ (Feb. 14, 2018), <https://qz.com/africa/1206935/whatsapp-is-the-most-popular-messaging-app-in-africa/>.

lection and storage in a way that adheres to data privacy law standards.¹²³ A company must also think of a way to monetize their service in order to cover these costs.¹²⁴ Moreover, “competitors include multi-billion dollar corporations, who already dominate the market, enjoy the benefit of network effects, have accumulated brand equity and trade secrets, and have the power to acquire smaller companies.”¹²⁵ This leads to an overwhelming dynamic where “the largest sets of valuable data—such as social data” (Facebook, WhatsApp), and search (Google)—are concentrated and thereby controlled by a handful of “winners,” with no regulations within data privacy to promote and maintain market competition.¹²⁶

E. Consent

Lastly, this inextricably affects the notion of consent, as “it is often argued that strong competition enforcement could render data protection rules more effective by facilitating genuine consumer choice.”¹²⁷ Regardless of the requirements laid out by Kenya’s data protection privacy bill, when one combines a lack of genuine consumer choice (due to the extreme lack of market competition) with a strong desire and or need for the service, can true consent be granted for data extraction?

Many believe that user consent to the authorization of data extraction and user consent to sell data to third parties shifts the power dynamic to equality between large tech companies and data subjects; however, this is simply untrue. When the users’ desire for the service exceeds the threat of data misuse, consent will be freely given. The World Wide Web Foundation conducted a study in three countries, Kenya, Indonesia, and Philippines, on “Teenagers Use of Social Media and their Understanding of Privacy Issues in Developing Countries.”¹²⁸ Teenagers are the highest users of social media and thus at the highest risk for data misuse.¹²⁹ The results of this study concluded that “[m]ost surveyed teenagers are aware that social media companies collect their personal data, but are not

123. Kwet, *supra* note 28, at 12.

124. *Id.*

125. *Id.*

126. *Id.*

127. *Data Protection Through the Lens of Competition Law: Will Germany Lead the Way?*, MEDIA POL’Y PROJECT BLOG (Mar. 23, 2016), <http://blogs.lse.ac.uk/mediapolicyproject/2016/03/23/data-protection-through-the-lens-of-competition-law-will-germany-lead-the-way/>.

128. MICHAEL CANARES, WORLD WIDE WEB FOUND., *ONLINE PRIVACY: WILL THEY CARE?* (2018), http://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf.

129. *Id.* at 4.

knowledgeable or do not care about how these platforms use these [data].”¹³⁰ So, the largest users of social media in three major countries, including Kenya, are aware of data collection but do not register or care about data misuse. Thus, their consent for data extraction is given carelessly leaving the tech companies still in control of blind users.

Additionally, the requirement of consent has not shifted the power to users, as users are often uneducated on data sharing and misuse. Even when they are aware, users oftentimes cannot understand the policies and thus blindly consent.

A Deloitte survey of 2,000 consumers in the U.S found that 91 [percent] of people consent to legal terms and services conditions without reading them. For younger people, ages 18-34 the rate is even higher with 97 [percent] agreeing to conditions before reading. The language is too complex and long-winded for most.¹³¹

In Africa, “(p)rivacy advocacy groups say users of the Free Basics Service, who may be getting online for the first time, may have little or no understanding of what information is even being collected from them.”¹³² Furthermore, the World Wide Web Foundation study found that “[w]hile the teenagers were typically relaxed about sharing their personal information, they seemed to be unaware that, by using social media, they also share data they do not input directly, such as location data and browsing history.”¹³³ When users do not understand what they are consenting to, the concept of consent is null and void. The companies have no one to keep them accountable, and they remain in control by taking advantage of the ignorance of their large user base.

Even valid consent does not prevent data misuse. Large tech companies will still own personal and sensitive data after consent is given, and they can still sell this data to third parties without any accountability measures. Much like when Cambridge Analytica acquired millions of data and used it to manipulate presidential elections, “the company pointed out, this wasn’t a leak or data breach of any kind—it’s simply how Facebook works.”¹³⁴ “ ‘Everyone involved gave their consent,’ according to the company’s response on the matter.”¹³⁵

130. *Id.* at 7.

131. Caroline Cakebread, *You’re Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017), <https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11>.

132. Fick & Akwagyiram, *supra* note 84.

133. Michael Cañares, *Teenage Clicks: Can Teens Protect Their Privacy on Social Media?*, WORLD WIDE WEB FOUND. (Sept. 4, 2018), <https://webfoundation.org/2018/09/teenage-clicks-can-teens-protect-their-privacy-on-social-media/>.

134. Harding, *supra* note 82.

135. *Id.*

F. *Limits to Defined Nation-State Privacy Laws*

The limits presented above are based on the current state of technology. However, as technology continues to develop rapidly, and large tech companies invest in a variety of beta testing experiments, the limits of the current data protection laws will only become more prominent. Privacy laws are typically designed to “only be enforceable within defined nation-state borders.”¹³⁶ However, some speculate that large tech companies are seeking to exist outside of national borders entirely.¹³⁷ For example, in 2013, mystery Google barges were seen on the Western and Eastern coasts of the United States. They appeared to be floating data centers,¹³⁸ perhaps an early attempt at sea-steading.¹³⁹ Sea-steading “is the attempt to create non-governmental entities outside of recognized borders and gain freedom from legal control.”¹⁴⁰ If large tech companies could create sea-steads, they could operate in international waters, completely unregulated, while owning the data of billions of users, dodging data privacy laws all together.¹⁴¹

CONCLUSION

Digital colonialism is just as oppressive as the early colonialism from the nineteenth century. Large tech companies, typically owned and primarily operated by White men, are extracting data from uninformed users and controlling that data to profit via predictive analytics. Unfortunately, strong data protection laws will not prevent this domination. While modern data protection laws may constitute a step in the right direction, further reflection is required to answer the question of how society can protect user data in an increasingly digitally-dependent society.

136. Simmons, *supra* note 102.

137. *Id.*

138. Rory Carroll, *Google's Worst-Kept Secret: Floating Data Centers off US Coasts*, THE GUARDIAN (Oct. 30, 2013), <https://www.theguardian.com/technology/2013/oct/30/google-secret-floating-data-centers-california-maine>.

139. Simmons, *supra* note 102.

140. *Id.*

141. *Id.*