Digital Surveillance and Digitally-disadvantaged Language Communities

Isabelle A. Zaugg, PhD
Postdoctoral Research Scientist, Data Science Institute, Columbia University
Northwest Corner, 550 W 120th St #1401, New York, NY 10027, United States
iz2153@columbia.edu

Abstract

The issue of digital surveillance often falls outside urgent discussions regarding the need to build digital supports for under-resourced languages. While the benefits of these supports for digitally-disadvantaged language communities are clear, the reality is that standardized script use, standardized spelling, and NLP systems in particular increase a language community's legibility for digital surveillance. As we build digital supports for Indigenous and minority language communities, we must consider how these tools might be used against them through digital surveillance, and how to combat these risks.

Keywords: digital surveillance, language diversity, Indigenous communities

ፅንሰ ሀሳብ

ይህ ጥናታዊ ፅሁፍ በድጅታል ድጋፍና በቋዋንቋዋ ብዝሐነት ዙሪያ በሚደረጉ ውይይቶች ውስጥ አዝወትሮ ስለ ማይነሳው ስለዲጅታል ክትትልና ስለላ ጉዳይ ያትታል። የቋንቋዎች ዲጅታይዜሽን ጥቅሞች መጠነሰፊ ቢሆኑም በሌላ በኩል ደግሞ የነዚህን ቋንቋ ተናጋሪዎች ላልተጠበቀ አደጋ ሊያጋልጣቸው ይችላል:: በዚህ ፅሁፍ እኒህ አደጋዎች እንዴት ሊከሰቱ እንደሚችሉና እንዴት ልንከላከላቸው እንደምንችል ሀሳቦች ይቀርባሉ።

1. Introduction

This paper shines a light on an issue that lingers just outside many discussions on topics of digital supports for language diversity, digital surveillance. This is an issue that has increasingly caused me concern as a scholar and advocate for improved supports for digitally-disadvantaged languages, in particular the Ethiopian and Eritrean languages written in the Ethiopic script. In this text I raise issues and questions arising out of the field of critical data studies to pose what I hope will be a productive challenge to the participants of this conference as we focus on serving the digital needs of speakers of diverse global languages. While our work is done under the banner of equity and appreciation for the rich history and culture contained within each language tradition and its community of speakers, we should not fall prey to a blind techno-optimism that contends that we can find purely technical solutions to entrenched and troubling problems of social inequality and injustice. We must consider the way in which the very tools that can bring important benefits to language communities can also be turned against them/us. This paper explores a number of issues, and poses a series of questions, at the intersection of digital surveillance and digital tools focused on the under-resourced languages of minority and Indigenous communities.

2. Context

Many minority and Indigenous language communities, as well as the speakers of regionally-dominant and national languages that have not been target markets for global tech companies, are eager to see the development of digital tools that support their languages. The reasons are crystal clear. Without these tools, when using digital tech to read, write, and edit text, users' options are highly limited. They can choose to communicate in a globally dominant language that is well-supported, or transliterate their messages into a dominant script such as the A,B,C's of Latin. Alternatively, they can use workarounds like sending images of hand-written text or short audio "text messages." Or they may forego the use of digital tools, losing out on potential benefits, a language-induced digital divide. Or perhaps they may become motivated to develop their own digital supports such as a proposed Unicode encoding of their script, an easily accessible and well-designed keyboard, a font, spellchecker, a translated social media interface, etc… (Zaugg, 2019).

Many advocates and designers of such digital tools for under-resourced languages are motivated by the hopes of keeping their language and language community vibrant in the face of linguists' predictions that 50-90% of languages face extinction this century (Harrison, 2007; Kraus, 1992). If a language can achieve a digital foothold, the hope is that young "digital natives" will not forego their mother tongue under the impression that other more dominant languages are cooler, more modern, and more convenient for the digital sphere and wider life (Rehm, 2014).

The stakes are high and the benefits of digital inclusion clear. And considering that under-resourced languages have never been and are unlikely to become a major focus of large tech corporations, there is a lot of work for volunteers and passion-driven advocates and technologists to do. But what are the risks and drawbacks, if any, of bringing a language, particularly minority and Indigenous languages, into the digital sphere? This paper focuses on the issue of digital surveillance, and the role it may play in complicating this picture of digital solutionism for language communities that often face unique and complex vulnerabilities, as well as unique resilience.

Digital surveillance can take a number of forms, from the sometimes forced collection of biometric data (Wee, 2019), CCTV systems that monitor the behavior of a city or country's residents (Diamond, 2018), and the monitoring of verbal and written communication, which typically rely on the legibility of a language to computers. This means that the more advanced digital supports and NLP systems are for a language, the more transparent the community using that language becomes to powerful forces that wish to surveil them. This is of particular import for us to consider, as the minority and Indigenous languages that are least supported digitally are also disproportionately at odds with national governments and corporate powers, sometimes by virtue of their very existence. These communities may also be particularly vulnerable to target marketing promoting the most injurious aspects of global modernity, and are often spread globally in diasporic patterns that may increase their digital communication needs.

In one telling example, we see Chinese-speaking #metoo activists sending text messages containing hand-written characters photographed upside down in order to pass the censorship of OCR-based (optical character recognition) AI systems designed to stifle their dissent (Weerasekara, 2018) – the very opposite of the types of standardized and legible digital tools we are promoting here. Therefore, it is critical that we consider the extent to which digital tools represent a double-edged sword for the communities we hope to serve, and think actively about the ways in which to harvest digital benefits while guarding against their vulnerabilities.

3. Military-intelligence Surveillance

While the vast majority of the approximately 7000 languages of the world are digitally under-resourced, in some case tools to work with these languages exist in the private domains of military-intelligence projects. These tools are built in order to surveil and in some cases constrain the activities of groups that pose national security concerns, who in many cases are also members of minority and Indigenous language communities. These tools are often developed by resource-rich countries with a high focus on military-intelligence (European Commission, 2006; "IARPA MATERIAL Program," 2017). It stands to reason that in some cases these tools are developed by or have the potential to fall into the hands of authoritarian governments or corporate entities whose interests are at odds with the language communities in question.

It is important to recognize that some minority language communities contain groups that propose violent means to achieve separatist or supremacist aims, and surveillance of their activities is essential to saving lives. But in turn, other language communities pose a threat to oppressive regimes by their simple existence, such as entrenched plutocracies that wish to clear-cut rainforests populated by Indigenous peoples who have been the historical residents of these areas and are also guardians of their biodiversity (Muñoz Acebes, 2019). Unfortunately, it would be naïve to think that language tech "for all" is a simple good, untainted by the same power structures that have left these languages digitally under-resourced in the first place. I hope that a concern for the human consequences, both intended or unintended, of the technologies being promoted at this conference under the banner of equity will be a highlight of conversations throughout the conference.

A question worth posing is: To what degree are NLP innovations resulting from high-investment research on under-resourced languages carried out in the military-intelligence sector eventually made available to serve the needs of language communities (if any)? This would not be unprecedented – for example, consider DARPA building the backbone of the Internet, then making it available for public use (Cerf, n.d.). An additional question: To what degree does military-intelligence research feed off of open-source corpora and data sets provided by academics and language advocates in the hopes of pooling resources to build better tools for their communities? What is the direction of funding, data, and tools developed in this arena, and whose needs do they serve?

4. Surveillance Capitalism

Digital surveillance is no longer the exclusive purview of traditional agents of surveillance, such as governments. On the contrary, digital technologies make surveillance, or "big data analysis" as it is often euphemistically termed, an activity available to almost any actor that can pay. In her 2019 book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Shoshana Zuboff builds upon the work of many critical data scholars to propose the term "surveillance capitalism" as the defining economic structure of our era. Surveillance capitalism, she proposes, uses human experience, mediated by digital and "smart" technologies and often extracted without consent, as a free raw material that can be translated into behavioral data. This behavioral data is fed to machine learning systems that provide predictions about what people will do in the future. She documents how surveillance capitalists have gained immense wealth through the trading of "prediction products," as companies profit from laying accurate bets on people's future behaviors. These systems tend to reward the privileged while entrapping the underprivileged, whose choices are particularly constrained.

In the context of this conference, we should consider how the social impacts of surveillance capitalism, will impact minority and Indigenous language communities, many of which already exist in economically and socially precarious positions. We know that online systems that market themselves as free and useful tools are designed to be addictive, through such strategies as "infinite scroll," and to promote superficial values and capitalistic consumption of advertised goods (Center for Human Technology, n.d.). And we know that platforms like Youtube push sensational content to keep users on their platforms, making them the perfect breeding ground for actors seeing to radicalize youth and divide communities (Fisher & Taub, 2019). Therefore, we need to think not only about building robust supports so under-resourced language communities can "join" these systems, but also how they can protect themselves once they are there. Or more radically, how can we dismantle the negative sides of these systems while preserving their benefits, to enhance the lives of all, so that as members of under-resourced language communities may choose to join these global domains, they find themselves in digital spaces that honor and enhance their lives?

5. Humanitarian Surveillance

A push for language technologies often takes on a sense of urgency during humanitarian crises. The need is clear - digital technologies can help connect displaced communities or spread life-saving information during ongoing disasters. Yet, we must also think about how to address long-term risks already vulnerable language communities may face in the context of tech solutions for humanitarian crises.

Mirca Madianou (2019) has demonstrated that digital innovation and data collection practices are increasingly core components of humanitarian response, yet in the long-term tend to further entrench discrimination and power asymmetries that disadvantage affected populations. This takes place, for example, when data first collected to identify, serve, and give voice to refugees, later, through "function creep" (Ajana, 2013), is used to monitor refugees' activities and limit their movements as their status shifts from objects of pity to national security threats (Madianou, 2019). Sensitive data is often collected through partnerships between humanitarian organizations, large corporations such as Accenture, Google, Microsoft, etc., and governments with whom the UN works hand and glove (Madianou, 2019).

These multi-faceted partnerships raise a number of questions about who owns, profits from, and can access this data in the long-term. For example, Rohingya refugees have expressed grave concerns that personal data collected by humanitarian organizations may be shared with the government of Myanmar, the same actor that perpetrated atrocities against them (Madianou, 2019). On the corporate side, too often the interests of vulnerable populations are forgotten when their data can be put to other uses, such as to improve facial recognition systems (Madianou, 2019) that may be sold back to governments seeking to keep refugees out. How might improving digital supports for the languages of humanitarian aid recipients potentially open their communities to further harms?

6. Positive Surveillance : Content Moderation

Paradoxically, when considering potential harms of digital surveillance, we must also consider the need for and persistence gaps in positive forms of surveillance and oversight. Content moderation, ideally community-led, is essential on open digital platforms in order to preserve the safety of these spaces, particularly for vulnerable communities. For example, Facebook serves around 1/3 of the world's population, with more and more language communities represented among its membership, yet its content moderation for all but the most globally dominant languages is close to non-existent (Koebler & Cox, 2018). As incidents of violence stemming from hate speech and fake news in Myanmar (Samet, 2018), Nigeria (Adegoke & BBC Africa Eye, 2018), and elsewhere demonstrate, this gap has life and death consequences.

Social media platforms like Facebook are ill-equipped to combat these trends as they simply have not invested the resources in personnel and AI systems that understand local languages and social tensions at play. Their business models raise questions as to whether this trend will be reversed without a major paradigm shift. Consider that the data generated by users in developed contexts like the U.S. is far more monetizable today than data generated by the company's huge and growing user base in the linguistically-diverse developing world. Furthermore, in a legal context in which even the U.S. government is struggling to hold Facebook, Google, and Twitter to account for their role in foul play perpetrated on their platforms (Bergen, Frier, & Wang, 2017), it seems unlikely that a developing country could succeed in this regard today.

Nigeria provides one stark example of how Facebook's gaps in language awareness and content mediation can lead to deadly violence and escalating tensions. After the June 2018 circulation of photos of graphic violence – viewed tens of thousands of times on Facebook - combined with false statements about an ongoing massacre in Plateau State, 11 people were killed in retribution in a town several hours north (Adegoke & BBC Africa Eye, 2018). In response, Facebook promised to strengthen its moderation of Nigerian content, a country with 24 million monthly Facebook users in 2018, and where 53 million Internet users are predicted to come online by 2025. But when BBC Africa Eye investigated Facebook's new "third-party fact-checking program," they found just four full-time employees in Nigeria to analyze and take-down fake news, and none of them speak Hausa, a language spoken by millions in Nigeria (Adegoke & BBC Africa Eye, 2018). For those of us promoting digital supports for digitally-disadvantaged languages, how might we also advocate for the human supports needed to make digital spaces safe for their speakers?

7. Conclusion

How can we work with digitally-disadvantaged communities to balance both the goods and harms of digital supports? This paper, I acknowledge, offers more questions than answers. Certainly, infrastructure must be considered, as backdoors to data may be built into systems at the outset of digital infrastructure developments (Aglionby, Yang, & Feng, 2018). End-to-end encryption, trusted intermediaries, and community oversight and moderation are also essential. Community networks based on a commons model might also offer bespoke solutions for some language communities. I hope experts in data security and data sovereignty will weigh in on these questions, in conversation with language communities themselves and their digital advocates, spurred to thought by the questions raised here.

8. Bibliographical References

Adegoke, Y., & BBC Africa Eye. (2018, November 13). Like. Share. Kill. Nigerian police say "fake news" on Facebook is killing people. *BBC News*. Retrieved from https://www.bbc.co.uk/news/resources/idt-sh/nigeria_fake_news

Aglionby, J., Yang, Y., & Feng, E. (2018, January 29). African Union accuses China of hacking headquarters. *Financial Times*. Retrieved from https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5

Ajana, B. (2013). *Ajana: Governing through biometrics: The Biopolitics of Identity*. Retrieved from https://scholar.google.com/scholar_lookup?hl=en&publication_year=2013&author=B.+Ajana&title=Governing+through+biometrics

Bergen, M., Frier, S., & Wang, S. (2017, October 10). Google, Facebook, Twitter Scramble to Hold Washington at Bay. *Bloomberg*.

Center for Human Technology. (n.d.). The Problem. Retrieved November 30, 2019, from Center for Humane Technology website.

Cerf, V. (n.d.). A Brief History of the Internet & Related Networks: Introduction. *Internet Society*.

Diamond, A. M., Larry. (2018, February 2). China's Surveillance State Should Scare Everyone. *The Atlantic*.

European Commission. (2006). *Human Language Technologies for Europe*.

Fisher, M., & Taub, A. (2019, August 11). We Wanted to Know How Online Radicalization Was Changing the World. We Started With Brazil. - The New York Times. *The New York Times*.

Harrison, K. D. (2007). *When Languages Die: The Extinction of the World's Languages and the Erosion of Human Knowledge*.

IARPA MATERIAL Program. (2017, August 17). *National Institute of Standards and Technology, U.S. Department of Commerce*.

Koebler, J., & Cox, J. (2018, August 23). The Impossible Job: Inside Facebook's Struggle to Moderate Two Billion People. *Vice*.

Kraus, M. (1992). The World's Languages in Crisis. *Linguistic Society of America*, *68*(1), 4–10.

Loomis, S. R., Pandey, A., & Zaugg, I. (2017, June 6). Full Stack Language Enablement. Steven R. Loomis website: http://srl295.github.io/

Madianou, M. (2019). Technocolonialism: Digital Innovation and Data Practices in the Humanitarian Response to Refugee Crises. *Social Media + Society*, *5*(3).

Muñoz Acebes, C. (2019, November 14). The Amazon Rainforest's Defenders Are Under Attack in Brazil. *Foreign Policy*.

Rehm, G. (2014). Digital Language Extinction as a Challenge for the Multilingual Web. *Multilingual Web Workshop 2014: New Horizons for the Multilingual Web*. Presented at the Madrid, Spain. Madrid, Spain: META-NET.

Samet, O. (2018, April 20). Assessing Facebook's Role in the Violence Against the Rohingya. *Pacific Standard*.

Wee, S.-L. (2019, February 21). China Uses DNA to Track Its People, With the Help of American Expertise. *New York Times*.

Weerasekara, P. (2018, April 27). "Historic moment": China's #MeToo activists use blockchain to skirt censors. *Hong Kong Free Press HKFP*.

Zaugg, I. (2017). *Digitizing Ethiopic: Coding for Linguistic Continuity in the Face of Digital Extinction* (Doctor of Philosophy in Communication, American University).

Zaugg, I. (2019). Imagining a Multilingual Cyberspace. In *Next Generation Internet. Finding ctrl: Visions for the future Internet*. https://findingctrl.nesta.org.uk/