

Comment:**Digital Monitoring as a Threat to Human Mobility****Mirna Wabi-Sabi***Abstract*

During the COVID-19 pandemic, a “privacy nutrition label” was introduced to the Apple applications store. Its aim was to simplify access that consumers have to the content of terms and conditions, specifically to its implications on individual privacy. Nevertheless, undocumented migrants in the United States and Europe were and still are subject to invasive digital monitoring, begging the question of how to handle unhinged uses of technological advances by government institutions. Artificial intelligence has been used to predict the geographical movements of migrants, and phone applications have been used as an alternative to incarceration and ankle bracelets. It seems that technological advances do not move parallel to improvements in the human condition, which is why keeping up with these advances is a challenge to those who are struggling to improve their living conditions. In the following article, Artificial Intelligence and Integration Contracts of asylum requests are discussed within the framework of immigration rights and modern tools of governmental abuse of power.

Keywords

Artificial Intelligence, Integration Contracts, asylum seekers, privacy, human mobility

To sign off on; phrasal verb meaning “give one’s approval to something.”

We all sign things nowadays, but not all of us get to sign off on things. The use of a signature as a way to grant approval is not the same as the more commonplace practice of signing things like “terms and conditions.” This distinction ought to be made because in identifying when a signature is not empowering or representative of consent, we can look for alternative tools of resistance against the established order—one which uses signatures to control and subjugate disenfranchised segments of the population.

Signatures earn significance through institutions of power by governments that establish order and have the resources to enforce this order. In any hierarchical structure, signing off on something is indicative of a status difference, as is the ability to make someone sign an unfavorable agreement.

A good example of this is our routine practice of downloading apps into our smartphones. Apple, for instance, signs off on the apps it allows on its app store, but the terms and conditions we agree to when we download them are certainly unfavorable to us as consumers. In an attempt to mitigate this issue, a “privacy nutrition label” was introduced to apps in the store during the covid pandemic, supposedly simplifying access consumers have to the content of these conditions.

The labels are probably a result of the GDPR, which Apple cites in its page detailing Privacy Policies (Apple Store 2022) and requires not only transparency over these policies but also for this information to be presented in a way people can easily understand. Unfortunately, these “nutrition labels” are neither effective nor accurate (Fowler 2021), exacerbating the issue of unfavorable agreements we consent to through digital signatures.

Earlier in 2022, in the wake of abortion bans in the United States, women encouraged each other to remove period-tracking apps from their phones for fear of potential privacy breaches and legal backlash. This is a way of not signing, not consenting, to personal data sharing. It is also a form of

a general strike, provoking a sharp turn in the industry. To be able to delete something from your smartphone is thus a privileged position to be in.

Nearly a quarter of a million immigrants in the United States are tracked by ICE with the use of an app that officials describe as more “humane” (del Rio 2022) than ankle bracelets or incarceration. Unsurprisingly, many do not agree with this description, which is why there is an ongoing court case against the Department of Homeland Security, claiming a violation of the Freedom of Information Act and concern over the “drastic increase in the Intensive Supervision Appearance Program (ISAP)” (US District Court Northern District Of California 2022). This program embodies how, nowadays, privacy policies of applications can quite literally become virtual prisons.

In Europe, due to the 2015 “refugee crisis,” data monitoring was considered by government institutions as a tool for predicting the “movements of migrants into Europe.” The European Space Agency pitched several EU organizations, including Frontex, on “commercially viable ‘disruptive smart technologies’” (Black 2020). In a report from 2019 on this subject, the ethical and practical limitations of this program were considered, but no guarantee is given that this tool has not been or is not being used. Even though the report acknowledges this technology can be and has been used for racial profiling—which they describe as an “overfocus on African countries” (IOM 2019)—and that machine-learning reliant on unpredictable data produces unreliable results, the conclusion describes this method as a “nascent workstream.” In other words, if this deeply flawed and unethical method of handling humanitarian crises is not yet widespread, it surely is about to become so.

Agreeing to dangerous terms and conditions of applications which track movement and seek to predict future movements of people like you infringes upon freedoms of whole segments of the world population. Considering that today it’s nearly impossible *to not produce data* (from the day we are born, documents and data are collected and stored about us), what can we do to disrupt data processing strategies, ensure a certain level of privacy, and allow for freedom of movement?

Integration Contracts

Asylum requests in Europe are signed off on by government officials, and seekers are made to sign several forms—including “integration contracts.”

The criteria used by those with the power to sign off on asylum requests are kept from the segment of the public with the most stake in these immigration policies: asylum seekers. It could be said that it is in the interest of EU countries to maintain asylum seekers oblivious to the inner workings of its institutions and the decision-making processes. These government branches may not want asylum seekers to have information which can help them present their case more effectively.

This is exemplified in the 2014 court case *YS and others* (Wabi-Sabi 2022), where incoherent legal justifications were used to deny migrants the right to access their personal data, a right protected by European privacy laws. In some instances, it was claimed that the right to privacy of government staff and their line of reasoning trumps the plaintiffs’ rights, and that the applications did not contain the personal data of migrants. There is no doubt, however, that immigration request files contain the personal data of the applicant, and so does the written analysis of government staff about these applications.

Meanwhile, when an asylum request is approved, the migrant is required to sign contracts which, among other things, subject them to compulsory “civic training” (Ministère de l’intérieur 2020). The French Office for Immigration and Integration (OFII) calls this the “Republican Integration Contract (CIR)” (République Française 2020), where “newly arrived foreigners” (Ministère de l’intérieur 2022) are taught “the principles [and] values [...] of the Republic, the rights and duties associated with life in France and the organization of French Society.” The granting of the immigration request comes attached to the requirement to resign certain aspects of your cultural identity. Namely, robust integration efforts are not only about inserting immigrants into the workforce, but also a “shield against radicalization” (Rush 2018)—an umbrella term for extreme cultural differences.

The Netherlands has a similar program, where “knowledge of the Dutch society” (European Commission 2021) is mixed in with Dutch language skills. They go even further in requiring “voluntary” work in businesses and demanding health insurance from companies which refuse to provide information in any language other than Dutch. I have gone through this process—twice or three times a week when I “volunteered” to vacuum a video store. Here I learned about “black pete” (but not about the country’s colonial history) and had to sign up and pay for health services I could not use, because workers refused to give me information in English over the phone.

In Brazil, a parallel can be made with the integration efforts of Venezuelan refugees. In official reports there is no mention of civic training and values; instead, there is mention of opportunities for certification and work (The UN Refugee Agency 2021). The UN Refugee Agency report from 2021 describes Venezuelan refugees in Brazil to be more likely to have completed stages of education but they earn less and work more hours than their Brazilian counterparts. There is no compulsory integration program, therefore, this practice is not intrinsic to immigration policies everywhere.

A new “action plan” (European Commission 2020a) for the integration of migrants in Europe, released in 2020 and aiming to pan out between 2021 and 2027, lays out a clear connection between “inclusion” and “monitoring.” This monitoring is essentially digital surveillance, though it is described rosily as a follow-up on integration projects the European Union funds, to ensure its integrity and effectiveness, as well as an “anti-discrimination” initiative (European Commission 2020b). Researchers have quickly voiced their concerns over how these follow-ups on integration policies, paired with a new European Digital Agenda, can easily become “a mass surveillance framework” (Regina and Capitani 2022) and an infringement on the values of a democratic society.

The digitalization of public services goes much beyond the immigration sector, but the specific push towards the integration of migrants now involves digital training. Improving the digital skills of any segment of the population is, in theory, a good thing. But this can also hand over an immense amount

of power to the State, both of what information to share and how. Anyone nowadays sees new technologies marketed as helpful for the performance of a certain task, while crucial information about how your data are collected and shared is omitted. We are all susceptible to it, especially immigrants.

Artificial Intelligence and Action

A response analysis of a “public consultation” on the topic of migrant integration, done with mostly EU citizens, shows that nearly a quarter of those interviewed “reported adopting the local culture and customs [...] as factors for successful integration.” In this digital era, these integration efforts pose worrying questions about what Artificial Intelligence can do to track, predict, and manipulate people’s behavior. The more integrated people are, the easier it is for machine learning to spot abnormal behaviors within infinite pools of data. If we can not come back from that, we ought to move forward knowing what these technologies can do, and how to have control over them—as opposed to being controlled by them.

First, let us learn from people and groups which do not have a stake in promoting these integration policies and technologies. To trust tech companies and the government to teach us about their own tech innovations is like trusting McDonald’s to teach us about how their meat is produced; of course, they will describe themselves with unreal amounts of flattery. Though impartiality is nearly impossible to achieve, as are conflicts of interest difficult to completely eradicate, a democratic society has a duty to provide plurality of sources and diversity in access to information.

Second, let’s promote the embracing of cultural differences over integration efforts. Social integration is marketed by government immigration offices in Europe as “anti-racist,” generous and empowering. It is none of those things. As part of my “integration” classes, I “volunteered” at a video store where I had to vacuum a closed section dedicated to porn. For a Muslim immigrant, which in 2015 made up the majority of people in my class, this would be mortifying. At the time, the secularism the Dutch always promoted as progressive turned into blatant bigotry (Bahceli 2015), and “integration”

meant the hostile pressure to learn the local language quickly and hide any non-Christian markers. It is no wonder that scholars (Regina and Capitani 2022) have pointed out the dangers of AI technology becoming a new tool to enact old fascistic European behaviors (Hayes 2018).

Certain counter-terrorism tactics which are considered acceptable in the United States are, in theory, not acceptable in Europe, at least anymore. As Paola Regina and Emilio de Capitani point out in a study published in March of this year (Regina and Capitani 2022), artificial intelligence is pushing, or needs to push Europeans to “re-evaluate” their antifascist efforts around government surveillance and the right to privacy. Technology has expanded the scope of data access (Bigo et al. 2013) by government institutions, and the terrorist attacks of 9/11 have for two decades served as a “recourse to insecurity, real or imagined” (Hayes 2018). This fuels a desire for “the securitization of international migration.”

The differences in ethical and historical perspectives between the US, UK, and EU have proven to not withstand this geopolitical paradigm and the lightspeed of technological advances. Studies on this issue tend to mention the Snowden revelations of 2013 with a sense of concern (Bigo et al. 2013) in the face of such massive pools of data paired with some of the most secretive government institutions. A *Public Intelligence* study (Bigo et al. 2013) goes further to question the extent to which this practice “can be tolerated in and between democracies” in particular. That is, as if the issue arose when Europeans became targets of mass surveillance, not when Arabs were targets of it, or peoples anywhere else in the world. “In and in between democracies” excludes anti-democratic attitudes “by” democracies towards everyone else.

Migration flow into Europe, due to propitious geography and Western-induced unrest in the Middle East and North Africa, led to disorganized digital profiling, or “mass surveillance activities carried out without clear objectives” (Bigo et al. 2013). It seems as if the second decade of the 2000s is marked by discoveries of how these digital technologies seeped into every little crack of our lives. And it is only now, in the third decade, that we are coming closer to defining, and labeling, what has been happening. How can

we get better at tracking and predicting the technological movements of Powerful institutions?

Preventing these technologies from being developed is virtually impossible, assuming democracy and freedom are the values supposedly being defended by those who are engaged in this debate. What is within our reach is understanding how these technologies work, how they have been used, and as a result, gain clarity as to how they might come to be used in the near future. For that, we need *independent networks of digital training*.

Many of us already know what Photoshop can do with images, so we are now learning what face-editing effects can do to videos. It's clear that this type of AI technology is already being used to track and racially profile people, and that it's not only immoral but also unreliable. It would be safe to assume that the direction the established order is going is one where much more effort is being put towards solving the issue of unreliability, than of immorality.

Deleting period-tracking apps only handles the issues of the past, when we thought we could still shy away from problematic digital hotspots. In a landscape where there are assumed to be no bad apples, there is just a very large rotten one upon which more than half the world's feasts (Chaffey 2022). Sometimes I think increasing data input, and so decreasing its predictability would be useful. Machine learning and algorithms cannot be effective in predicting human behavior, especially when we as humans resist the efforts being put towards turning us into machines. Encouraging difference and uniqueness can be a radical thing, because the pressure to "integrate" is more than a de-radicalization tool, it is an effort to predict and control our behaviors, even our most intimate ones.

References

- Apple Store. 2022. “App privacy details on the App Store.” *Developer*. Accessed [November 27, 2022]. <https://developer.apple.com/app-store/app-privacy-details/>.
- Bahceli, Yoruk. 2015. “Wilders tells Dutch parliament refugee crisis is ‘Islamic invasion.’” *Reuters*, September 10. Accessed [November 27, 2022]. <https://www.reuters.com/article/us-europe-migrants-netherlands-idUSKCN0RA0WY20150910>.
- Bigo, Didier, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer. 2013. “National Programmes For Mass Surveillance Of Personal Data In Eu Member States And Their Compatibility With Eu Law.” *Public Intelligence*, October. Accessed [November 27, 2022]. <https://info.publicintelligence.net/EU-MassSurveillance.pdf>.
- Black, Crofton. 2020. “EU agencies tested monitoring data on refugees.” *EU Observer*, April 28. Accessed [November 27, 2022]. <https://euobserver.com/health-and-society/148185>.
- Chaffey, Dave. 2022. “Global social media statistics research summary 2022.” *Smart Insights*, August 22. Accessed [November 27, 2022]. <https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/>.
- del Rio, Giulia McDonnell Nieto. 2022. “Meet SmartLINK, the App Tracking Nearly a Quarter Million Immigrants.” *The Markup*, June 27. Accessed [November 27, 2022]. <https://themarkup.org/the-breakdown/2022/06/27/meet-smartlink-the-app-tracking-nearly-a-quarter-million-immigrants>.

European Commission. 2020a. “Watch: The EU Action Plan on

Integration and Inclusion (2021-2027) explained.” *European Website on Integration*. December 17. Accessed [November 27, 2022]. https://ec.europa.eu/migrant-integration/news/watch-eu-action-plan-integration-and-inclusion-2021-2027-explained_en.

European Commission. 2020b. “The EC reveals its new EU Action Plan on Integration and Inclusion (2021-2027).” *European Website on Integration*. November 24. Accessed [November 27, 2022]. https://ec.europa.eu/migrant-integration/news/ec-reveals-its-new-eu-action-plan-integration-and-inclusion-2021-2027_en.

European Commission. 2021. “Governance of migrant integration in the Netherlands.” *European Website on Integration*. Accessed [November 27, 2022]. https://ec.europa.eu/migrant-integration/country-governance/governance-migrant-integration-netherlands_en.

Fowler, Geoffrey A. 2021. “I checked Apple’s new privacy ‘nutrition labels.’ Many were false.” *The Washington Post*, January 29. Accessed [November 27, 2022]. <https://www.washingtonpost.com/technology/2021/01/29/apple-privacy-nutrition-label/>.

Hayes, Ben. 2018. “Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and ‘big data.’” *International Review*. Accessed [November 27, 2022]. https://international-review.icrc.org/sites/default/files/irrc_99_12.pdf.

IOM (International Organization for Migration). 2019. “Workshop Report on Forecasting Human Mobility in Contexts of Crises.” *ALNAP*, October 22–24. Accessed [November 27, 2022]. <https://www.alnap.org/system/files/content/resource/files/main/17022020%20FFO-IOM%20Workshop%20on%20Forecasting%20Human%20Mobility%20in%20Contexts%20of%20Crises.pdf>.

Ministère de l’intérieur. 2020. “Guide for asylum seekers in France.” September.

Ministère de l'intérieur. 2022. "The Republican Integration Program." January.

Regina, Paola, and Emilio de Capitani. 2022. "Digital Innovation and Migrants' Integration: Notes on EU Institutional and Legal Perspectives and Criticalities." *Mdpi*, March 23. Accessed [November 27, 2022]. <https://www.mdpi.com/2076-0760/11/4/144>.

République Française. 2020. "Republican Integration Contract (CIR)." *OFII*, July. Accessed [November 27, 2022]. https://www.ofii.fr/wp-content/uploads/2020/07/cir_contrat_en.pdf.

Rush, Nayla. 2018. "France: Integration of Migrants Begins with Shared Values." *Center for Immigration Studies*, June 6. Accessed [November 27, 2022]. <https://cis.org/Rush/France-Integration-Migrants-Begins-Shared-Values>.

The UN Refugee Agency. 2021. "Integration of Venezuelan Refugees and Migrants in Brazil." *ACNUR*, March. Accessed [November 27, 2022]. <https://www.acnur.org/portugues/wp-content/uploads/2021/05/5-pages-Integration-of-Venezuelan-Refugees-and-Migrants-in-Brazil-en.pdf>.

United States District Court Northern District Of California. 2022. "Complaint For Declaratory And Injunctive Relief For Violation Of The Freedom Of Information Act." *Just Futures Law, Community Justice Exchange, Just Futures Law, Mijente Support Committee v. U.S. Immigration and Customs Enforcement and U.S. Department Of Homeland Security*, April 14. Accessed [November 27, 2022]. <https://static1.squarespace.com/static/62c3198c117dd661bd99eb3a/t/635c0fe7ed5eab36eb46c47c/1666977767513/CJE+et+al+v+ICE+et+al.pdf>.

Wabi-Sabi, Mirna. 2022. "The Rule of Law and its Built-in Marginalizing Features." *A Beautiful Resistance*, June 30. Accessed [November 27, 2022]. <https://abeautifulresistance.org/site/2022/6/29/the-eu-court-of-justice-case-ys-and-others-and-built-in-marginalizing-features-of-the-rule-of-law>.