UCLA
AI PULSE Papers

Title
Technocultural Pluralism

Permalink

Author
Osoba, Osonde A.

Publication Date

by: Osonde A. Osoba

A "Clash of Civilizations" in Technology?

Preamble

At the end of the Cold War, the renowned political scientist, Samuel Huntington, argued that future conflicts were more likely to stem from cultural frictions– ideologies, social norms, and political systems– rather than political or economic frictions.[1] Huntington focused his concern on the future of geopolitics in a rapidly shrinking world. But his argument applies as forcefully (if not more) to the interaction of *technocultures*.

By *technocultures*, I mean the stitched global patchwork of interacting technological ecosystems we currently live in. For an intuitive illustration of these distinct ecosystems, observe variations in these popular platform choices circa 2017 (Figure 1.). Given the proliferation of global tech platforms (e.g. Facebook, WhatsApp, LINE, etc.), these variations can give noisy hints about where technocultural fault-lines lie. I argue that ecosystems are characterized not just by local consensus or concordance in tech adoption, but also in culture, policies, tech innovation, and deployment priorities.
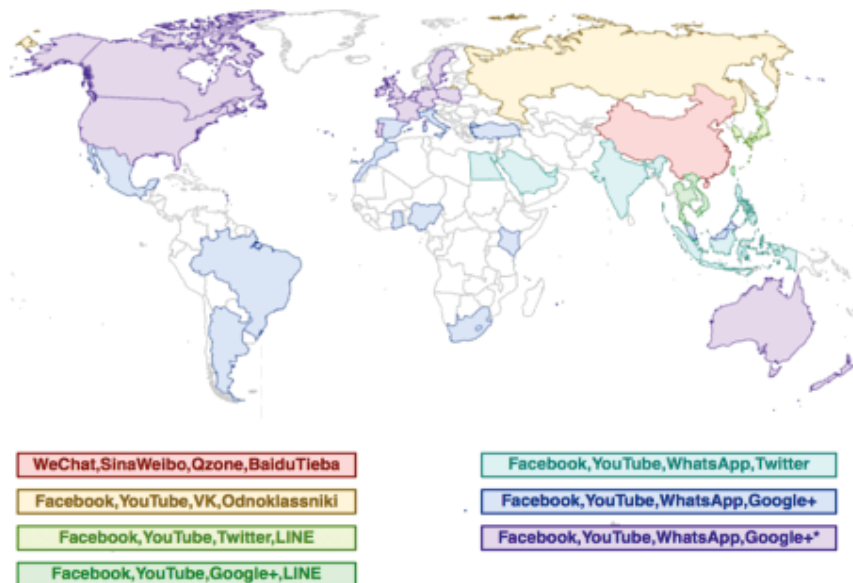
AI PULSE

by: Osonde A. Osoba

Figure 1: Mapping Out Dominant Social Media Platform Popularity Across the Globe as of 2017. Interestingly, observed platform-choice clusterings or signatures align quite closely to the cultural fault-lines Huntington outlined almost 30 years ago. We can roughly make out Western-Europe-and-USA-and-Australia, China, Eastern Europe, Japan, and Islamic-Hindu spheres of influence. (Data Courtesy of GlobalWebIndex.net, Cluster Analysis Courtesy of Joshua S. Mendelsohn)

The main hypothesis is two-fold.

- [Technocultural Frictions]: an AI "technocultural cold war" is more likely if not already in progress. This refers to a state of ongoing regulatory friction among multiple technocultures or governance regimes, forced to interact because effective geographic proximity, political necessity, and/or economic advantage. The focus here is on competitive or adversarial frictions.[2] Put differently, technocultural friction refers to friction due to the necessary interaction between technology

by: Osonde A. Osoba

policy spheres of influence.[3]

- [Technocultural Pluralism]: the prospect of a global monolithic AI technoculture emerging in the near-future is implausible. Persistent pluralism is more likely. By pluralism, I mean a persistent diversity in the global technoculture. These hypotheses are not necessarily AI-specific. But the current efflorescence of data-hungry machine learning innovation in AI heightens the salience of cultural differences.

This piece has two aims. The first task is descriptive (like most of Huntington's original 1993 discussion). I aim to describe underlying factors and dynamics that foster the development of differentiated technocultures. I build up key concepts (not least of which is a clearer depiction of *technoculture*). This descriptive exploration also serves persuasive function. Technocultures are easier to track once we observe how the warp and weft of technology innovation, deployment, culture-specific norms, and regulation "conspire" to differentiate our global technology environment. The second task aims to go beyond description to highlight dynamics and implications of technocultural pluralism. It is worth highlighting specifically the important implications of data privacy policies, data localization, and population size as mechanisms for differentiation in the evolution of technocultures around the world.

Part of the motivation for this discussion is to counter a specific perspective (admittedly a strawman perspective and often an inchoate one when held). This tempting perspective anticipates a future regulatory scenario featuring a monolithic global technology ecosystem with little to no geographic cultural variation. Although this is a strawman position, elements of this position arise in some technology policy conversations. What can we say about the prospects of such a monolithic

by: Osonde A. Osoba

technocultural world? If this homogeneous outcome is unlikely, what are the regulatory and governance implications? Hopefully this exploration starts us off with basic tools to gain more insight into these types of questions.

Technoculture… What is that?

First there is a question of what we mean by a *technoculture*.

The term technoculture here refers specifically to the combination of a *technology*[4] *regime* and the *culture*[5] in which it is embedded. The concept of a technoculture forces an engagement with questions of how cultural contexts affect, influence, or determine the evolution, deployment, and adoption of technological artifacts. This will include questions about the controlling innovation culture, the prioritization of problems for technological innovation, expected modes of deployment, etc.

Is this (or any) conception of technoculture useful?

At first blush, the concept of technoculture may seem paradoxical; technology is often supposed to be this objective or value-neutral fruit of dispassionate scientific analysis and design. But even under the debatable assumption of a perfectly value-neutral design process, the choice of problems on which to apply technological innovation is subject to cultural influence. As a recent anecdotal[6] illustration, take the polarized response to the demonstration of the use of machine learning models to infer criminality from face images.[7] The authors (of Chinese origin) maintain that this is perfectly acceptable while many American tech commentators strenuously objected.

Even the assumption of value-neutral scientific design wilts under light scrutiny. The constraints of ML development processes mean that designers make myriad non-

by: Osonde A. Osoba

negotiable design choices that will affect users,[8] including users with unexpected characteristics. Some of these design choices include impositions of norms and values (e.g. concerning fairness/equity, transparency). The Nymwars of 2012 gives a concrete case in point:[9] social media platform designers decided to impose and enforce the norm of only allowing profiles with real names. That decision stood in opposition to prior established norms of online pseudonymy in certain communities.

It is now less controversial to assert that technology is inherently cultural given these observations. Technological artifacts are not free of cultural or ethical values (implicit or explicit).[10] Cultural values infuse the innovation, design, and use of technology. Winner[11] recounts numerous examples of conscious and unconscious deployment of technology artifacts that either imposed or fostered political preferences (e.g. decisions in town-planning and bridge architecture in Long Island, NY explicitly designed to enforce extralegal segregationist preferences).

This is especially true of modern AI. Modern AI depends primarily on data. Data ecosystems are comprehensive records of cultural values and norms – neutral, good, or bad. Current conversations about data-diet vulnerabilities in AI and biases in algorithms highlights this point more emphatically.[12] Modern data-driven ML systems learn patterns (e.g. language behaviors and biases) present in their training data.

Furthermore, the contours of existing and future data ecosystems are strongly determined by operating data privacy regulations. Questions of privacy are (at least) as cultural as they are technological. On the cultural dimension, cross-national survey studies of attitudes towards privacy and cultural influences on privacy show significant relationships between privacy behaviors and quantified cultural factors[13]

by: Osonde A. Osoba

especially pragmatism, individualism, and country.[14] These relationships are found to hold even after controlling for population experience with/exposure to technology.

Besides the cultural dimension, both privacy enhancing technologies and privacy policies[15] determine how much and what kinds of data are available to train AI systems. Privacy enhancing technologies (PETs) highlight the outer physical limits of privacy preservation.[16] Privacy policies occupy a space between cultural factors and technology. These policies allocate rights and specify incentives to govern the behavior of data sources and sinks. Cultural and consensual norms influence the overall balance of such of rights and incentives. The EU's GDPR sets a precedent asserting the rights of users as primary individual controllers of their data (control but not necessarily rights to compensation for use). Chinese governance culture includes a current precedent of asserting communal control of individual data to address public welfare (e.g. to control public information consumption or to enable public reputation scoring). And technology deployment in lower income countries (e.g. Aadhar deployment in India) has been found to be less subject to privacy concerns.[17]

Why Do Technocultures Matter? Is a Universal Technoculture Plausible?

Back to Samuel Huntington's post-cold-war observation and its adaptation to technocultures. If the discussion in the previous section is compelling enough, then we are led to concede the following:

1. AI technology (and any technology) is subject to the influence of its cultural context.
2. There is a global diversity of technocultural contexts — even if the geopolitical boundaries or fault-lines are fuzzily defined at best.
3. Cultural values inform tech evolution, tech policy, and tech regulation — especially

by: Osonde A. Osoba

concerning data and AI.

Interaction between technocultures is unavoidable in our rapidly shrinking world. And differences in policy and regulation can lead to friction in interaction. This leads to the aforementioned two-fold hypothesis about technocultural pluralism and frictions. The interplay of the highlighted technocultural factors hint at the idea that the global AI technology ecosystem is likely to fracture along the culture-specific lines telegraphed in these data ecosystems. And AI's intense data dependence means privacy policy[18] is likely a key lever in technocultural divergence.

The technocultural friction point is somewhat supportable given:

- recent discussions of "AI arms races,"

- the flurry of AI strategy statements from different countries[19], and

- recent geopolitical squabbles over commercial data localization[20] and/or foreign investment in sensitive tech sectors.

The technocultural pluralism point is harder to support fully since it is a statement about the future evolution of technocultures.[21] In the context of data-driven AI tech, the cultural-specificity of available or accessible training data (either due to local norms in data behavior or due to local data privacy policies), may lead to persistent fracturing the evolution of AI tech. In the more general technology context, observable cultural differences in tech use, innovation, and regulation suggests persistent differentiation.

The pluralism hypothesis is admittedly a less-than-ironclad forecast. But it is a forecast based on the observation that we have yet to see global cultural convergence in the long (short?) history of civilization. Cultural differences (e.g. in

by: Osonde A. Osoba

language use) persist in spite of long interaction. A technocultural monolithic future is as unlikely as a culturally monolithic future. Sure, this is a conservative prediction. But it is likely a more reasonable one given the historical record.

Pluralism... Now what?

What are the strategic implications of these hypotheses? A persistently pluralist technocultural future raises some hard questions like: Are technocultural differences truly unresolvable in the long-term? If they are not resolvable, what are the possible equilibria in the long-run? Can a multipolar technocultural world be stable? Are technocultures inherently "winner take all"? Is there an alternative to technocultural dominance? In the short run, how do we understand the space of potential

technocultural frictions and conflicts? What are the evolutionarily stable strategies[22] for playing the game of technocultural thrones?

All useful questions. Probably. Rather than give definite answers to these

questions,[23] I instead explore a characterization of features of an inhomogeneous tech ecosystem and an examination of plausible future scenarios that arise under the pluralism hypothesis.

It is worth highlighting that pluralism is not necessarily a negative. The ability of local domains to determine local technoculture can be very empowering e.g. the ability of poorer nations to adopt technologies and deploy them to solve pressing local problems.

A Pluralist World: Useful Levers & Interesting Dynamics

It is useful to explore how the actions of aggregate agents (government, populations,

AI PULSE

by: Osonde A. Osoba

commercial entities) can influence the evolution of AI technology and the global technoculture more generally. Here is a non-exhaustive exploration in broad-strokes:

Data Localization Policies

Data localization is an emerging trend in data privacy and technology regulation. Data localization refers to restrictions or prohibitions on exporting data about local citizens or data originating from local sources. Notable examples of such regulations include EU's GDPR Article #45,[24] China's Cybersecurity Law Article #37[25] and Russia's Federal Law no.242-FZ.[26] GDPR's Article #45.2(a), for example, requires an assessment of the normative "adequacy" of foreign jurisdictions before certifying the outward transfer of EU data. Article #37 of China's Cybersecurity Law articulates similar constraints on outward data flows. Exceptions would require extensive security vetting.

There are justifiable reasons for imposing localization regulations:

1. **[Security Constraints]** Data localization can help prevent foreign intelligence breaches. Information traffic about domestic affairs flowing in foreign jurisdictions is often easier to intercept both physically and legally. Forcing local processing and storage (sometimes even transmission) reduces the risk of interception.[27] Furthermore, data localization makes information relevant to domestic security and safety more readily accessible within the jurisdiction. Technocultures as different in values as the EU and China both agree on the occasional need to breach privacy in pursuit of security or safety.

2. **[Normative Constraints]** Data localization helps preserve the contextual integrity of citizen's data. Privacy norms are value- and culture-dependent. One conception of privacy is of privacy as a form of contextual integrity.[28] Under this conception,

by: Osonde A. Osoba

privacy preservation is tied to the (explicit or implicit) norms of the specific context and jurisdiction. Non-local data handling increases the exposure of subjects' data to inappropriate contexts with privacy norms that are insufficiently aligned with local norms. There is thus a higher risk of violating contextual integrity and/or locally-acceptable privacy norms.

3. **[Self-Interest]** Data localization helps foster the local technology ecosystem. This point is especially central for the pluralism hypothesis as related to AI. Localization will often foster the development of local technical competence with data technologies. This competence is foundational for enabling innovations in AI and developing AI solutions tailored to local problems.

The combination of these factors incentivizes the trend towards a more fractured global technoculture. Increased data localization fosters siloed technocultures.

"Attractive" Populations: Power in Numbers

Regulatory levers like data localization have the effect of placing a cognitive burden on interested multinational firms. They need some familiarity with local norms if they intend to operate *profitably* and *legally* within foreign jurisdictions.[29] Ideally there is a benefit for shouldering that burden. That benefit comes from the economic power of a population-base. We can use the term "attractiveness" to refer to the influence that populations can exert on technocultures just by being sizeable sources of profit. The magnitude of a target populations's influence is somewhat proportional to its size.

Large populations attract economic attention as markets or sinks for economic goods. Jurisdictions with large population bases present a large pool of potential consumers. Firms that are able to survive regulatory and operational challenges

by: Osonde A. Osoba

qualify to play for larger potential (or actual) profits. In this scenario, regulatory barriers may operate as mechanisms for depriving competitors who are unwilling/unable to satisfy local norms of market share. Regulation and policy-making can thus be construed as acts of collective bargaining on behalf of a jurisdiction's population.

The past demises of Apple, Google, Uber, and Facebook operations in China are useful illustrations. Recent Apple and Google overtures to resume some operations in China also illustrate the strength of the attractiveness of that user-base.

As a lever in technocultural evolution, population size has a couple of modes of use. Countries with large populations can use their influence to extract concessions or compromises. This can be an explicit interaction e.g. China sanctioning firms that do not provide state access to collected user data.[30] The opportunity cost for a multinational firm closing down operations because of some regulatory barrier is higher for larger countries than for smaller. Influence can also be exerted via implicit negotiation, e.g. the EU using the weight of its population-base to shift international data privacy discourse and practice via ambitious regulation.

Populations also attract attention as sources of technical expertise or human capital at advantageous price points. This is useful to highlight because human capital comes equipped with value systems that can sharply affect the evolution of tech innovation and deployment. The moral aversion to defense-related uses of AI recently expressed by significant portions of Silicon Valley technical work-force offers a case in point.

Winners and First-Movers

There has historically been a form of *first-mover's advantage* in technology

by: Osonde A. Osoba

innovation. Intellectual property (IP) rights actually aim to strengthen this advantage as a way of incentivizing innovation. In recent history, for instance, the USA enjoyed unparalleled technocultural dominance. Current Internet technology still bears some reminders of its US-centric early development (e.g. USA's network centrality in internet routing and other vestiges of US-led tech standards formation). The migration of talent to the USA during WW2 helped cultivate this advantage. As did the relative depression of Chinese and Russian innovation due to experiments with versions of Communism.

There is also a strong bias towards survivors of technology arms-races: a winner-take-all dynamic or close to it. As a first approximation, effective tech innovations spread and drive less effective innovations to extinction (practical performance as the fitness metric). But the memetic resonance of modern information technology platforms may not be as fully determined by practical performance e.g. the geographic differences in adoption of international platforms like facebook and vKontakte is likely not just a function of differences in technical performance. But the dynamics of network effects and preferential attachment to popular platforms leads to cumulative survival advantages that approximate winner-take-all behavior.

These trends, first-mover's advantage and winner-take-all, may mediate local economic advantages as well as a technoculture's influence on future policy. But these trends are not "unchallenged laws of nature." MySpace gave way to Facebook in spite of precedence. As did Yahoo to Google in search technology. And the fracturing of the modern social media ecosystem suggests that network effects are not irreversible.

Paths of Evolution: Local Norms with Global Reach?

There is a deliberate analogy between ecology of technocultures and the ecology of

by: Osonde A. Osoba

biological ecosystem. Species in an ecosystem interact (cooperatively or competitively) and evolve in response to their environmental context. Similarly, technologies, platforms, firms, governments interact and co-evolve in response their specific cultural context.

The analogy suggests a vulnerability. Geographical distance may have served as a barrier against the transmission of technocultural cultural influence in the past. But distance is no longer a strong barrier. Technocultures now evolve in a crowded international space. One technoculture might foster a specific innovation in tech use, development, or regulation. Such innovative mutations may now be more easily transmitted across technocultures. And such mutations may find stronger resonance in non-native contexts. Such cross-technocultural transmissions may be beneficial or virulent.[31]

Examples of beneficial cross-technocultural transmissions[32] include:

- the transmission of key aspects of ICT innovations (outwards from the USA)
- the transmission of AI innovations (esp. facial recognition AI outwards from the USA to prominent use in China)
- The transmission of sericulture [outwards from China]
- In tech regulation, the spread of GDPR concepts from the EU into Californian privacy regulation

Examples of virulent cross-technocultural transmissions include:

- The repurposing of social media platforms for propaganda or psychometric targeting in political elections [outward from the UK or from Eastern Europe].

We can also play with the prospect of convergent evolution in technology e.g. the

by: Osonde A. Osoba

convergent evolution of printing technology in the East and the West, or the convergent evolution of flight and photography. Intense global interaction may mean it becomes easier to adopt foreign innovations rather than innovate locally (thus reducing the likelihood or opportunities for convergent evolution). The key theme here is of local norms and actions having unprecedented global reach.

Innovations in AI tech also change the balance of influence in international relations. Nation-states naturally develop the abilities necessary to pursue their interest in cyberspace. It is reasonable to expect this trend to continue. But the context is slightly shifted somewhat… Now smaller anti-social non-state actors with some AI expertise have an expanded ability to project influence and hold larger actors hostage. Especially if there are no trusted referees to mediate disputes.

Again, the theme: local norms, global reach.

Conclusion: The Fruits of a Pluralist Framing

The purpose of this piece was to encourage us to take seriously the prospect of unresolvable cultural schisms in the global technology landscape. Culturally-mediated fault-lines are particularly salient when dealing with data-driven AI technologies which make-up the bulk of modern AI technology. This is because culture-dependent privacy norms circumscribe what data is available/accessible/permissible for training AI systems. The general interaction of culture and technology is what we have termed a technoculture. The point of introducing this concept is to provide a fruitful lens for examining the evolution of technology.

I have referred to the fractured state of the global technology ecosystem as

by: Osonde A. Osoba

Technocultural Pluralism. In a sense, this pluralist conception has been the historic norm. Our multicultural history is not a history of globally uniform patterns in tech innovation and deployment. The key assertion in this piece is that pluralism is likely a more permanent state than one might perhaps think — globalization, disruptive AI innovation, and (potentially/supposedly?) impending singularity notwithstanding. We can take language use as an informative precedent. Language is one of humanity's oldest culture-infused tech innovations.[33] Yet it still retains a level of cultural specificity that is unlikely to fade away soon. Why expect anything else for AI on a shorter time-scale?

Taking pluralism seriously does not mean assuming a permanent Hobbesian state of "War of All Against All." There is certainly bound to be friction as technocultures negotiate their shared existence on a smaller global stage, under diverse, sometimes diametrically opposed value systems (technocultural clashes, to use Huntington's term). It also does not mean a constant arms-race or drive towards domination. The arms-race perspective is well-suited to discussions of defense in which the controlling objective was about survival and actions are centrally directed. In any given modern technoculture, there will be multiple preferences, utilities, or objectives in play. And the aggregate behavior of the technoculture is an impenetrable function of millions or billions of sub-agents' choices.

Taking pluralism seriously means spending more time exploring the features and dynamics of our global technocultural ecosystem. This piece represents one such exploration.

What strategic implications does a technoculturally pluralist framing highlight? One key implication would be the pivotal role of data localization and privacy policies in deepening schisms between technocultures in the age of AI since localization

by: Osonde A. Osoba

undermines uniformity in what data exists or is accessible in different jurisdictions for training local AI/ML solutions. There is a more positive take on this implication: data localization and local privacy policies can help foster more culturally-sensitive local deployment and innovation of AI technologies.

Questions remain. For example: What are the merits of a technocultural equivalent of the "Contact Hypothesis"? i.e. does more contact between technocultures lead to better long-term accommodation? Or to heated frictions and virulent cross-infections? What mechanisms are effective for improving the health and resistance of domestic technocultures from negative foreign infections? What are effective strategies and compromises in a technoculturally pluralist world?

Whatever insights remain, they will require a deeper engagement with the cultural foundations of our technologies and a clearer-eyed examination of the values/assumptions embedded within our technologies.

Acknowledgements

This discussion is a side-effect of numerous conversations. I am particularly grateful to Kathryn "Casey" Bouskill for many insightful discussions on the nuances of culture.

References

Allison, Graham. *Destined for War: Can America and China Escape Thucydides's Trap?*. Houghton Mifflin Harcourt, 2017.

Barocas, Solon, and Helen Nissenbaum. "Big Data's End Run Around Procedural

by: Osonde A. Osoba

Privacy Protections." *Communications of the ACM* 57, no. 11 (2014): 31-33.

Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104 (2016): 671.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* 20, no. 5 (2004): 313-324.

Boyd, Danah. "The Politics of Real Names." *Communications of the ACM* 55, no. 8 (2012): 29-31.

Caliskan, Aylin, Joanna J. Bryson, and Arvind Narayanan. "Semantics Derived Automatically from Language Corpora Contain Human-like Biases." *Science* 356, no. 6334 (2017): 183-186.

Chander, Anupam, and Uyên P. Lê. "Data Nationalism." *Emory Law Journal* 64 (2014): 677.

Cockburn, Iain M., Rebecca Henderson, and Scott Stern. *The Impact of Artificial Intelligence on Innovation*. No. w24449. National Bureau of Economic Research, 2018.

Dawkins, Richard. "The selfish gene: with a new introduction by the author." *UK: Oxford University Press.* (4th Ed.) 2016.

Standing Committee of the National People's Congress. *2016 Cybersecurity Law* (7 November 2016). Translated by China Law Translate. Accessed January 11, 2019. https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en.

Floridi, Luciano. "Infraethics–on the Conditions of Possibility of

by: Osonde A. Osoba

Morality." *Philosophy & Technology* 30, no. 4 (2017): 391-394.

G.D.P.R., 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union* (OJ), 59, pp.1-88.

Gershgorn, Dave. "A Harvard Professor Thinks That Tech's True Power Comes From Design." Quartz, February 24, 2018. *Quartz*. https://qz.com/1214645/latanya-sweeney-explains-why-tech-companies-are-so-powerful/.

Hofstede, Geert. "Dimensionalizing Cultures: The Hofstede Model in Context." *Online Readings in Psychology and Culture*, 2(1). https://doi.org/10.9707/2307-0919.1014.

Huntington, Samuel P. "The Clash of Civilizations?." *Foreign Affairs* (1993): 22-49.

Huntington, Samuel P. *The Clash of Civilizations and the Remaking of World Order*. Penguin Books India, 1997.

Leon, P. G., Alfred Kobsa, and Carolyn Nguyen. "Contextual Determinants for Users' Acceptance of Personal Data Processing: A Multinational Analysis." *ISR Technical Reports* 16-5. (December 2016). https://isr.uci.edu/publications.

Li, Yao, Alfred Kobsa, Bart P. Knijnenburg, and MH Carolyn Nguyen. "Cross-cultural Privacy Prediction." *Proceedings on Privacy Enhancing Technologies* 2017, no. 2 (2017): 113-132.

Matthews, Luke J., Ryan Andrew Brown, and David P. Kennedy. *A Manual for Cultural Analysis*. Santa Monica, CA: RAND Corporation, 2018.

by: Osonde A. Osoba

https://www.rand.org/pubs/tools/TL275.html.

McSweeney, Brendan. "Hofstede's Model of National Cultural Differences and their Consequences: A Triumph of Faith-a Failure of Analysis." *Human Relations* 55, no. 1 (2002): 89-118. [Critique of Hofstede dimensions]

Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. "Information Privacy: Corporate Management and National Regulation." *Organization Science* 11, no. 1 (2000): 35-57.

Mumford, Lewis. "Authoritarian and Democratic Technics." *Technology and Culture* 5, no. 1 (1964): 1-8.

Nissenbaum, Helen, "Privacy as Contextual Integrity," *Washington Law Review*, Vol. 79, No. 1, 2004.

Ohm, Paul. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review 57* (2009): 1701.

Osoba, Osonde A., and William Welser IV. *An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence*. Santa Monica, CA: RAND Corporation, 2017.

Oulasvirta, Antti, Aurora Pihlajamaa, Jukka Perkiö, Debarshi Ray, Taneli Vähäkangas, Tero Hasu, Niklas Vainio, and Petri Myllymäki. "Long-term Effects of Ubiquitous Surveillance in the Home." *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012): 41-50.

Rho, Eugenia, Ha Rim, Alfred Kobsa, and Carolyn Nguyen. "Differences in Online Privacy and Security Attitudes Based on Economic Living Standards: A Global Study of 24 Countries." *Proceedings of the Twenty-Sixth European Conference on Information Systems* no. 95 (2018).

by: Osonde A. Osoba

Romney, A. Kimball, Susan C. Weller, and William H. Batchelder. "Culture as Consensus: A Theory of Culture and Informant Accuracy." *American Anthropologist* 88, no. 2 (1986): 313-338.

Selby, John. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?." *International Journal of Law and Information Technology* 25, no. 3 (2017): 213-232.

Winner, Langdon. "Do Artifacts Have Politics?." *Daedalus* (1980): 121-136.

Wu, Xiaolin, and Xi Zhang. "Automated Inference on Criminality Using Face Images." *arXiv preprint arXiv*:1611.04135(2016): 4038-4052.

Wu, Xiaolin, and Xi Zhang. "Responses to Critiques on Machine Learning of Criminality Perceptions (Addendum of arXiv: 1611.04135)." *arXiv preprint arXiv*:1611.04135 (2017).

By Osonde Osoba, Professor, Pardee RAND Graduate School, RAND Corporation

1. Huntington, 1993; Huntington, 1997.
2. We do not focus on military frictions in this discussion in spite of our use of the "cold war" metaphor.
3. Whereas Huntington wrote about "civilizations," we can think of the relevant units of analysis here as policy spheres of influence. These may be national (e.g. China), subnational (e.g. California, USA), or even supranational (e.g. the EU) aggregate entities that exert some form of regulatory control over their geographical jurisdictions.
4. Most of our conversation on technology will focus on data-driven AI/ML

by: Osonde A. Osoba

technologies.

5. The word culture tends to raise intellectual hackles because of its supposedly nebulous or imprecise definition. However definitional imprecision is not sufficient reason for asserting non-existence. We use culture here to refer to persistent societal norms and values that circumscribe observed behavior. The social psychologist, Geert Hofstede, defines culture as "the collective programming of the mind that distinguishes [groups]." Less abstractly, a recent exploration on methodologies for research on culture [Matthews-Brown-Kennedy, 2018] defines cultures as "...the set of social influences that alter an individual's behaviors and beliefs..." There is significant body of work in anthropology that attempts to define and explore constructively valid models of culture including Hofstede's work on dimensions of culture [Hofstede, 2011] and Romney et al.'s work on identifying cultural groups via "high concordance" on social knowledge [Romney-Weller-Batchelder, 1986].

6. *Anecdotal* in the sense that it is unclear how representative the study authors' perspectives are of the cultural norms of their country of origin. Thus it is an unfair comparison.

7. Wu & Zhang, 2016; Wu & Zhang, 2017.

8. Latanya Sweeney (quoted in [Gershgorn, 2018]) calls this state of affairs a "technocracy." She argues that this is effectively a regime of rule-making, governance, or policy-making implemented by unelected technology designers. This is mildly reminiscent of Lessig's "code is law" thesis.

9. Boyd, 2012.

10. Floridi, 2017; Winner, 1980.

11. Winner, 1980.

12. Caliskan-et-al, 2017; Osoba & Welser, 2017; Barocas & Selbst, 2016.

13. There is a significant body of psychometrics literature on the relevant quantitative

by: Osonde A. Osoba

dimensions for a constructively valid signature of culture. Most of the cited studies on privacy attitudes rely on Hofstede's dimensions [Hofstede 2011]: *Individualism, Masculinity, Power Distance, and Uncertainty Avoidance*. A key critique of this signature framework is the issue of the level of aggregation [McSweeney, 2002]. This critique is highly relevant issue for a key question: how does one identify a geopolitically contiguous culturally cohesive unit?

14. Leon, Kobsa, Nguyen, 2016; Li-Kobsa-et-al., 2017; Bellman-Johnson-et-al 2004; Milberg-et-al., 2000.

15. The underlying and potentially contentious premise here is that policy is an imperfect crystallization of cultural values as expressed through laws, regulations, and social norms.

16. Barocas-Nissenbaum, 2014; Ohm, 2009.

17. Rho-Rim-Kobsa-Nguyen, 2018.

18. and to some extent privacy tech innovation.

19. The Future of Life lists no less than 25 "National AI Strategies," most released over the last couple of years. "National and International AI Strategies," Future of Life Institute, accessed January 11, 2019, https://futureoflife.org/national-international-ai-strategies/.

20. Data localization comes up mainly in privacy policies, specifically EU's GDPR and China Cybersecurity Law. Data localization refers to regulations that impose barriers on the free flow of data across geopolitical borders.

21. …And, as a useful piece of dogma, "all forecasts are wrong."

22. Dawkins, 2016.

23. Huntington's discussion argues against the feasibility of any form of global domination. His main policy response was developing a more culturally-informed understanding of local politics and learning "accommodation." Useful lessons here as well.

by: Osonde A. Osoba

24. GDPR, 2016.

25. Cybersecurity Law, 2016.

26. Chander-Le, 2014. Russia's 2014 Federal Law no. 242-FZ amends Russian Federal Law no. 152 ("On Personal Data") by introducing Article 18(5) which requires the use of local databases to process and store data on Russian citizens. The list of other countries with similar or related localization laws includes: Nigeria, South Korea, Vietnam, Indonesia, and Malaysia. Chander-Le, 2014.

27. Selby, 2017; Chander-Le, 2014.

28. Nissenbaum, 2004.

29. Arguably/historically, western exceptionalism encouraged avoiding this burden by nudging local norms closer to theirs (either by outright domination, persuasive attraction, or both).

30. As required by Article #28 of the Cybersecurity Law: "Network operators shall provide technical support and assistance to public security organs' and state security organs; lawful activities preserving national security and investigating crimes." Cybersecurity Law, 2016.

31. Beneficence or virulence are normative labels. But the suggested examples are arguably not controversial.

32. The operating analogy is that of a cross-species transmission event in epidemiology.

33. I will concede that the conception of "language as technology" is not uncontroversial...