JSL THE JOURNAL OF SCIENCE & LAW

OPINION
published: March 12, 2021
doi: 10.35005/q8t1-ek30

Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends

Brian Higgins[1], Anastasia Dodd[1]

[1]Blank Rome LLP

Access to data is an essential part of artificial intelligence (AI) technology development efforts. Government and corporate actors have increasingly imposed localized and hyper-localized restrictions on data due to rising mistrust—the fear and uncertainty about what countries and companies are doing with data, including perceived and real efforts to exploit user data or create more powerful and possibly dangerous AI systems that could threaten civil rights and national security. If the trend is not reversed, over-restriction could impede AI development to the detriment of all. Solutions are offered to improve trust through the adoption of legal and social policies that ensure transparency in data collection and use, and explainability of decisions made by AI systems that affect people's lives.

Keywords: artificial intelligence, data collection, Executive Order, explainability, transparency

Introduction

The unprecedented proliferation and access to data has produced all sorts of benefits. Data has enabled development of artificial intelligence (AI) systems that improve public health, enhance delivery of public municipal services, and make consumer products work better, faster, and more efficiently.[1] This trove of available data has also revealed how people interact with one another and even how aspects of society works.[2] It is no wonder that "big data" has received so much attention, and why some technology companies and governments place a premium on getting their hands on more of it.[3]

Indeed, when it comes to creating newer, better, and more complex AI systems,[4] developers point to data as their most valuable commodity. To them, data is more precious than gold; it is *the* essential resource for creating advanced AI technologies.[5] Many popular AI-driven applications, for example, are designed not just for in-app purchases and advertising revenues, but also to datamine users' interactions, creating a data-generating machine for the app's creators.[6] The TikTok app is a notable example. Ostensibly, it is an ad-based revenue tool for ByteDance, its current owner.[7] But running in the app's background is a data juggernaut: TikTok users interact with the app and upload billions of audio-video files to the company's data servers every year, data that can be used to refine existing AI algorithms and create altogether new ones.[8]

Data's importance to the AI industry has also led some world leaders to view it, and AI technologies more broadly, as part of national security and economic imperatives.[9,10,11] When Donald Trump accused TikTok's owner of operating a system that "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage,"[12] he underscored not only the White House's broader national security concerns about China, but also the high value U.S. leaders place on data, especially data needed by AI developers.[13] This aligns with the White House's goal of "protecting the American AI technology base from attempted acquisition by strategic competitors and adversarial nations,"[14] and its larger effort to lead the world in AI innovation.[15, 16]

Other countries, especially India and Australia, have imposed their own restrictions on TikTok, as well as on

OPEN ACCESS | Edited by: David Eagleman **Reviewed by:** Sasha Davenport **Correspondence:** Anastasia Dodd, adodd@blankrome.com
Received: December 16, 2020 **Accepted:** December 17, 2020 **Published:** March 12, 2021.

other Chinese apps and data. After those countries' clashes with China, they banned TikTok, WeChat, and hundreds of other apps within their respective borders, cutting off users' access to the apps and, by extension, stemming the flow of app data to the app's owners.[17] Other government leaders, including those in Russia, China, and the European Union (EU) Commission, have adopted other forms of data restrictions. Russia, for example, employs data censorship to restrict access and block data exports. The EU issued regulations governing handling and storage of personal data and has initiated efforts to protect what it believes is its unique industrial data, going so far as to articulate goals that differentiate its member countries' data, and the so-called "European AI" built from it, from other countries' data and AI.[18]

State actors are not the only ones placing restrictions on data and AI. In the absence of regulations in the U.S., companies in the AI industry have themselves placed barriers and silos around data and data sharing, ostensibly to dominate the AI market through the control and monetization of useful raw data, especially user-generated data.[19] Combined with government measures, those business strategies threaten to lessen competition in the AI technology market, impede some AI developers' access to world markets, and potentially limit the benefits of AI.[20, 21, 22]

In Parts II and III of this paper, we refer to these government- and corporate-led actions around data and AI as localized or hyper-localized restrictions[23], and argue that rising mistrust—the fear and uncertainty about what countries and companies are doing with data, including perceived and real efforts to exploit user data or create more powerful and possibly dangerous AI systems that could threaten national security—could lead to excess restrictions and impede AI development.[24] In Part IV, we suggest ways to enhance trust through adoption of policies for improving transparency around the collection and use of user and other types of data, and explanations about how AI systems make decisions that affect users.[25]

From Data Globalization to Data Localization

From an historical perspective, actions by governments and industry leaders to restrict data are antithetical to decades-long efforts by scientists to globalize technology for scale across borders, which began in earnest with the development of the Internet and the World Wide Web.[26] At the time Tim Berners-Lee developed the Web at CERN in 1990, the principle of universality underscored the vision he and many other scientists held for the global Internet:

> "For anyone to be able to publish anything on the web, all the computers involved have to speak the same languages to each other, no matter what different hardware individual users have access to or what cultural and political beliefs they have. In this way, the web breaks down silos while still allowing diversity to flourish."[27]

Berners-Lee's exploration of ways to facilitate information sharing between computers and the creation of worldwide communication and information access fulfilled a vision held by scientists for decades. That vision promoted technology designed with globalization in mind: tech made in one location scaled for cross-border deployment and wide accessibility. His work eventually laid the foundation for the future digital age and a proliferation of data that came with it.[28]

To promote an open and universal web, CERN made the underlying code of the Internet available to all to use, royalty-free, in perpetuity.[29] The Internet's dot.com era, beginning in the middle to late 1990s, flourished as a result. Buying and selling products and services shifted from brick-and-mortar stores to online ones, and social networks allowed peers and family members to interact over the Internet for "free" (while operators in the background monitored every user click and page view to better target advertising). More recently, the Internet has facilitated the development of myriad new smart devices that operate at the edge of networks within private homes and cars, and powerful, compact computing devices small enough to carry in pockets, allowing anyone, anywhere (with Internet access) to find information on a computer half-way around the world. Downloadable apps for work and entertainment have become ubiquitous. This explosion of data creation and sharing by users, however, raised concerns about privacy and ultimately prompted the adoption of policies embodying principles of data localization.

Data localization is the collection, processing, and storage of data at a particular location or region, as well as restrictions on what data can be transferred away from the location or region and how.[30] At the state level, China and Russia, and more recently the European Union (EU) and United States, have adopted data localization policies (Table 1). In China and Russia,

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

access to the Web and the availability of data over the Internet is restricted (China's web restrictions are colloquially known as the "Great Firewall").[31] In both countries, data localization restrictions require that any data about Chinese and Russian citizens be stored in China and Russia, respectively. In effect, this creates a one-way valve on the Internet's global data pipeline: information outside of those countries' borders can flow in (though it may be censored), but data about their own citizens cannot flow out, with limited exceptions.[32]

Country/ Region	Data Localization Policy	Remarks
United States	Limited restrictions on the flow of data about citizens	Many restrictions are healthcare and medical data/information - specific
European Union	Conditional release of data about citizens out of the EU	User-centric focus allows the individual user to direct the flow of data
Russia	Mandatory local storage of data about citizens	Internet and media censorship
China	Mandatory local storage of data about citizens	Internet and media censorship (nicknamed "The Great Firewall")

Table 1: Summary of Data Localization Policies.

In Europe, the EU's General Data Protection Regulations (GDPR), which ushered in a new paradigm for how governments control their citizens' personal data, established requirements for storage and export of European data to computers outside the EU. Enforceable beginning in 2019, the Regulations were a direct result of a lack of trust in others' use of user's personal and identifying information. The Regulations do not restrict foreign companies from cross-border access to the EU, but do place conditions for the flow of data back to those companies. Unlike China and Russia's restrictions, the GDPR provides transparency and user control over data. Specifically, users can opt to open the valve allowing their data to flow out of the EU.

In addition to regulating personal data, the EU has also proposed a single market for EU-specific data and European AI.[33,34,35] Its regional solution is to build cooperation among EU members and harness the "enormous volume of new data yet to be generated" in the EU, data that will be less about people and more about processes, including industrial data from transportation, shipping, manufacturing, energy, and agriculture sectors.[36] This neo-protectionist approach to data leverages data for EU's competitive economic advantage.

In the U.S., the White House's Federal Data Strategy includes measures to prevent public release of confidential and private information in U.S.-specific data using, among other techniques, statistical disclosures in place of actual data.[37] The National Security Council for Artificial Intelligence (NSCAI) has raised concerns about sensitive U.S. data leaving the country, and has suggested limiting the ability of hostile actors to acquire such data.[38,39] In Congress, a bill offered in November 2019 (the "National Security and Personal Data Protection Act of 2019") would, if enacted, prohibit "the transfer of data to, and storage of data within, foreign countries that threaten U.S. national security."[40] At the state level, lawmakers in California, Illinois, and elsewhere have passed privacy-related restrictions around user data within their respective borders.[41,42]

Among other factors, mistrust underlies the trend toward imposing greater data localization restrictions and less unfettered communication of data over the Internet. As discussed below, AI technology companies' handling of user data has also led to a rise in distrust and an increased use of hyper-localized data restrictions, further restricting data.

From Data Globalization to Data Localization

Data hyper-localized restrictions target the conduct of one or more companies, technologies, or industry segments whose actions give rise to real user privacy and other data-centric concerns. Examples include state and local government restrictions on the use of facial and other biometric data collection technologies, Executive Orders targeting specific Chinese companies and their data-collection apps, and state laws restricting use of data-based algorithmic decisions

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

systems, among others. In contrast, lawmakers have so far largely allowed other controversial technologies, notably content promotion algorithms employed by social media companies, to operate unfettered, despite rising distrust in the face of controversial data practices.[43]

Facial and biometric data collection technologies are some of the most widespread and controversial technologies to emerge from the surge in AI development in recent years. Following documented instances of misidentification leading to false arrest, bias, and other serious problems with the technology, as well as rising concerns about surveillance privacy in general, local and state governments have passed dozens of ordinances and laws generally targeting uses of the technology in the wild. [44,45] In doing so, they have also indirectly restricted the data used to develop the AI models powering the technology and the data those systems collect. Interestingly, some of the same AI companies that commercialize facial recognition systems have called on lawmakers to regulate the technology,[46] an openness perhaps borne out of necessity more than anything, as the current legal landscape they operate in begins to resemble a patchwork of differing restrictions.

The TikTok and WeChat Executive Orders are the clearest recent examples of hyper-localized data restrictions targeting specific companies. Both Orders arose from perceived potential threats posed by foreign governments. The WeChat Executive Order raises concerns about "a Chinese database containing billions of WeChat messages sent from users in not only China but also the United States…."[47] Similarly, the TikTok Executive Order raises concerns about the app's automatic data capture abilities, which reportedly include the ability to track the location of Federal employees, the use of personal information for blackmail and corporate espionage, and the use of data for disinformation and misinformation campaigns, and more.[48] Notably, although the Executive Orders could have simply closed the valve on data flowing from American users to countries outside its borders, thereby alleviating users' and national security concerns about data and AI, the White House chose to instead prohibit transactions with TikTok and WeChat, whether between users or advertisers. TikTok has a narrow opportunity for reinstatement, if it sells its U.S. operations to an American company.[49] One consequence of this approach is that potential U.S. owners would not only gain control over user data generated by the apps in the U.S., but also potentially gain access to the proprietary algorithms and source code behind a foreign company's AI technology.[50]

Rising distrust in AI systems is a natural consequence of the opaque, black box nature of their algorithms and data use. One such technology that has so far escaped data hyper-localized restrictions is content promotion algorithms used by social media companies, despite being castigated by lawmakers, the media, and the public for its excessive data collection efforts, murky data usage policies, ways in which they handle users' data (including reselling it to others without notice), opaque algorithms, and creating "echo chambers," in which balanced viewpoints and content are scarce. More than others, Facebook's content promotion algorithms have been criticized for what some consider deleterious, unquantifiable influence and real harm.[51] The U.S. intelligence community has widely acknowledged Russia's extensive use of Facebook to interfere before and during the fall 2016 U.S. election.[52, 53] But even today, it is impossible to know how Facebook's content promotion algorithms recommended Russia's election propaganda, which users were targeted by the disinformation, or how much of an effect those interference efforts had on American voters. During the 2020 U.S. election, Facebook and other social media companies voluntarily altered their content promotion algorithms to identify and block certain election-related disinformation or claims. Even so, the rising distrust trend may not be successfully reversed absent data restrictions.

The industry giants, particularly the largest AI technology developers, have furthered the rise of distrust through their efforts to amass big datasets and acquire smaller AI companies. By deploying AI systems to collect user and other forms of personal and behavioral data while at the same time removing competition, accusations of anti-trust monopolies have begun echoing through the halls of Congress.[54] As a result, just in the last half of 2020, top AI technology company CEOs have been grilled on Capitol Hill about antitrust, disinformation, and data mishandling, and calls to break up Facebook and possibly other companies have gained much attention.[55,56,57]

Notably, the apparent uneven treatment between content promotion technologies in social media, which have escaped data hyper-localization restrictions, and facial recognition technologies in the biometric industry, which have been hit hard by restrictions, reflect how AI technologies in general may be governed.[58] Lawmakers seem willing to impose data and other restrictions on AI systems when actual and immediate harm is traceable directly to an AI technology, as in the case of facial recognition, but less so when an AI system's actions and perceived or actual harm appears to be causally attenuated, diffuse, not immediately felt, or not concretely actionable (at least, outside the political realm).

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

Although the reasons for and against imposing data localized and hyper-localized restrictions may differ, some data restrictions may nevertheless be needed to promote civil rights, create a level playing field in the AI industry, and address legitimate national security concerns, among other benefits.[59] Unless reforms specifically targeting trust are implemented, however, the current trajectory could lead to over-restricting data, resulting in more siloed data, a slowing of AI development for the benefit of all, and a fractured technology world. For example, lawmaker's responses to facial recognition could overly-restrict the technology to a point that technological progress in areas where facial recognition could benefit society is slowed, such as in the detection and prevention of human trafficking. Figuring out how best to curtail nefarious or undesirable use cases for AI technologies while allowing beneficial ones to operate will be a challenge for lawmakers and policymakers going forward.

Law-Based Policies for Rebuilding Trust

The place to start rebuilding trust is where mistrust and distrust originate: the interactions between users and AI technologies. This is where fear and uncertainty can arise, driven in large part by a lack of transparency about how user data is being handled and a general lack of available, understandable explanations about how data-based systems like AI work and make decisions. Both state and non-state actors have a role to play in rebuilding trust.

Lawmakers and government agencies, for their part, can introduce standards for data and AI with the goal of improving transparency and explainability. Some of these efforts are already underway. For example, the National Institutes of Standards and Technology (NIST) is currently exploring appropriate technical standards for AI systems, and has already issued standards for certain data-based technologies.[60]

In the absence of governmental technical standards, however, the AI technology industry itself should collaborate and establish open data collection and transparency standards, published for public comment. Each industry segment that employs user-centric AI technologies and collects user data may need their own unique standards, but consistency across industries will give users confidence in companies' purposeful engagement with them and the challenges and conflicting interests surrounding data privacy and data use. Standards should be developed whenever a new use for an AI technology is to be deployed.

Among the necessary industry standards that would improve trust, data privacy should be near the top on the list. The AI industry should change the way data privacy policies are developed and made available to persons affected by them. In a study of privacy policies by the New York Times, the longest policies took readers nearly 35 minutes to finish, with an average reading time of about 18 minutes. Many policies are written such that adequate comprehension is beyond most people's ability.[61] Standards for privacy policies should ensure none are "verbose and full of legal jargon."[62]

Data use and privacy policies could also include concrete examples to explain difficult legal issues and illustrate the effect of selecting one privacy option over another. Clear descriptions of what data is collected and why should be employed. The oft-used but vague "so we can improve our services" should be eliminated from privacy policies, unless companies are forthright and honest about their interest in user data. For example, if data are collected from users and about users to build new AI systems or improve existing ones that can be monetized, a privacy policy should clearly disclose that fact and offer users alternatives.

In the absence of good faith self-governance by the industry, lawmakers may need to enforce privacy policy requirements, for example by promulgating rules requiring companies that collect, store, and use a threshold amount of user information (based on monthly active users or data processed) to submit their privacy policies for government review and also to certify annually that actual operations were in compliance with those policies or explain any deviations from those policies. Knowing one's published policies are scrutinized by a regulatory authority, especially one with investigatory and law enforcement powers, could at least cause more companies to regularly question their own actions toward data. A federal agency like the U.S. Federal Trade Commission (FTC) could lead this effort as part of its enforcement of the anti-deceptive trade practices under the FTC Act.

Greater transparency could also be achieved by providing real-time indications to users when their interaction with an AI system generates data that may be mined by a company for its own purposes beyond the basic operation of its system. For example, if brief voice recordings uploaded to a company's server help it create and improve a machine learning automated speech recognition (ASR) model, a data policy could include an example to illustrate what actions by the user or the company trigger collection of the user's voice recordings and how much of the recordings are used. At the same time, a visual or audible indicator, text message, or email could provide users feedback

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

when their interaction with a company's AI system is or has generated data that the company mined for its own use. Surveillance notices are already imposed on businesses who use cameras in their facilities to monitor customers.

Data policies would also benefit from a straightforward explanation of how users' data can be used outside the companies that collect it. That is, who specifically the data can be sold to, what the third parties can do with it, and who the third parties can resell it to.[63] Companies, not users, should have the burden of evaluating the terms of service (TOS) of third parties who companies sell user data to, including evaluating what the third party can do with user data and what foreseeably could be done with the data. For example, if data is resold in an anonymized format but could be deanonymized by the third party, or if aggregation with other data by the third party could allow the data to be deanonymized, the company's privacy policy should include a clear explanation of that possibility. Consumers could be further reassured by descriptions of the company's review of third parties' data privacy policies and the company's enforcement mechanisms. Enforcement of the data collector's TOS restricting data usage should be a necessary and ongoing facet of data resale to downstream purchasers.

Even the most carefully scripted language in data privacy policies and TOS agreements, however, may leave users wondering if a company is living up to its words. The black box nature of many AI systems makes it impossible for users to know for sure how those systems make decisions that can affect them, which compounds mistrust. AI-powered content recommendation tools are notable examples. Recommender systems intake users' present and past viewing histories (passively-collected user data) and stated preferences (user-supplied data) and output content that the model believes would be of interest to the user. Yet, in most cases, a user has no idea what happens when he or she clicks on the "like" button, views a video, or clicks through pages on a website. By not explaining how an AI-based recommender system makes decisions, a user can feel a company is intruding on their private interactions through unnecessary monitoring.[64]

Moreover, there is an assumption that AI systems are always accurate in their decision-making roles, but an AI system may be employed to merely offer the best option among several choices given a set of input features. Thus, companies using AI systems to make decisions affecting people should provide a confidence bar along with the output to give insight into the AI model's "thought process."[65] For example, an AI model used to assess whether a person should receive pretrial release on bail (a yes/no classification model) should provide its decision along with a range of possible outcomes that are within a stated confidence for a human operators (e.g., an expert, judge, or jury) to evaluate. A classification decision with a wide confidence band (suggesting less confidence in the correctness of the result) may be less persuasive to a trier of fact than, say, a decision that is associated with a tighter confidence band.

Similarly, companies should provide insight into which input features an AI system weighted more than others when making its decision or taking an action. As developers add more and more features to a system input to better model a real-world distribution, they may find that several features stand out as being weighted the most. Identifying those features helps developers understand their own model and how to improve it, but can also help those impacted by an AI systems' decision understand what stood out as being relatively more important to the model. This sort of insight can also help assess a model's potential inherent biases.

Finally, companies should also consider implementing tools to timely receive feedback from those directly impacted by a company's AI systems, and comments from other interested stakeholders about the company's data collection policies and its efforts to explain how its AI systems work. Feedback should be assessed relative to the aforementioned standards, both subjective and objective.[66] This underscores the need for companies to publish industry-wide and company-specific standards applicable to their AI systems, so that they remain accountable to users. While publicizing feedback might seem counterintuitive to risk management, it can showcase for consumers how well a company is following through on promises of improved transparency and explainability.

It may be naïve to expect every technology company will fully embrace transparency. Any company that opens their AI system to public scrutiny also risks the intellectual property driving it—hardly a sustainable business model. It would be equally naïve to expect all technology companies will effectively self-police their actions. Facebook's Oversight Board, which ostensibly was installed to be seen publicly doing something about the company's content moderation policies, was given limited powers and scope, raising doubts about its effectiveness as a self- enforcement mechanism.[67,68]

Instead, it falls to lawmakers and government agencies to meaningfully enforce any data and AI regulations and incorporate them into international treaties to enact a worldwide standard and enforcement policy. Lawmakers may benefit from careful review of the GDPR's enforcement mechanisms, including the European Data Protection Board, and learn from the

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

pitfalls and growing pains it observed over the past two years.[69]

Conclusion

The power of today's AI technologies to transform the world economy and improve people's lives has not been over-hyped. Getting the most out of AI, however, requires a meaningful degree of trust in data and AI technologies at user, local, and international levels. In this paper, we describe how data localization and hyper-localization restrictions are reactions to rising mistrust and distrust felt by users, government leaders, and technology companies around issues of data and AI, which breeds anti-globalization, nationalistic sentiments about data, isolation of AI technology development, and could lead to a fractured technology world. It will take a concerted, purposeful effort by stakeholders to counter these impulses and achieve the benefits that advanced AI systems can provide for all. Implementing policies to improve transparency and provide better explanations about how AI systems collect and use user and other types of data are suggested as means to rebuild trust. Companies that make and deploy AI systems are best positioned to lead the charge toward greater trust by adopting standards-based and comprehensible transparency and explainability policies for data and AI.

References

1. Kearns, M. & Roth, A. (2020). *The Ethical Algorithm*. Oxford University Press.
2. *Id*.
3. Apple, Inc. (2021, Jan. 28). *A Day in the Life of Your Data: A Father-Daughter Day at the Playground*. Available at https://www.apple.com/au/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf.
4. We use "AI" as shorthand for "AI technologies" or "AI systems," depending on the context. AI technologies are the software-implemented algorithms that use specific machine learning techniques and other approaches for analyzing large dataset to create digital models of the real world. "AI systems" are the software and related hardware deployed by AI developers to operationalize the digital models in a private or public enterprise.
5. Ng, A. (2017, December 15). *The State of Artificial Intelligence*. MIT Technology Review https://www.youtube.com/watch?v=NKpuX_yzdYs.
6. *Id*. Here, Dr. Ng describes a data-product-users-data feedback loop in the context of AI technology development.
7. At the time of writing, who owned the TikTok app was uncertain. McCabe, D., Swanson, A., & Merced, M. J. D. L. (2020, September 21). *TikTok Deal Trips Over U.S.-China Power Struggle*. https://www.nytimes.com/2020/09/21/technology/tiktok-bytedance-deal-walmart-oracle.html.
8. TikTok (2020, July 9). *TikTok Transparency Report 2019 H2: Enforcing Our Policies*. https://www.tiktok.com/safety/resources/transparency-report?lang=en. *See also* Johns, F. (2017). "Data Mining as Global Governance." Handbook of Law, Regulation and Technology. Brownsword, R. et al., editors. Chap. 32. Oxford University Press.
9. Executive Order 13943 (2020, August 6). *Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*. White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.
10. Sullivan, M. (2020, August 27). *Eric Schmidt: China could be AI's superpower if we don't act now*. Fast Company. https://www.fastcompany.com/90544259/eric-schmidt-china-could-be-ais-superpower-if-we-dont-act-now.
11. Chivot, E. and Castro, D. (2019, May 13). *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy*. Center for Data Innovation. https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/
12. Executive Order 13942 (2020, August 6). *Addressing the Threat Posed by TikTok*. White House. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.
13. TikTok said the White House's restrictions "were not motivated by a genuine national security concern, but rather by political considerations relating to the upcoming [U.S.] general election." Shepardson, D., & Stempel, J. (2020, September 24). *TikTok asks judge to block U.S. from barring app for download*. Reuters. https://www.reuters.com/article/usa-china-tiktok-lawsuit/tiktok-asks-judge-to-block-u-s-from-barring-app-for-download-idUSKCN26F07K.
14. Executive Order 13859 (2019, February 11). *Maintaining American Leadership in Artificial Intelligence, Section 1: Policy and Principles*. White House. https://www.whitehouse.gov/presidential-actio

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

ns/executive-order-maintaining-american-leadership-artificial-intelligence/.

15. *Id.*, Subsection (f).
16. *Q2 Recommendations*, National Security Commission on Artificial Intelligence (NSCAI) (2020, July) at p. 58.
17. Mozur, P. (2017, August 1). *Joining Apple, Amazon's China Cloud Service Bows to Censors*. The New York Times. https://www.nytimes.com/2017/08/01/business/amazon-china-internet-censors-apple.html.
18. European Commission (2020, February 19). *On Artificial Intelligence - A European Approach to Excellence and Trust*. p. 2. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
19. Zuboff, S. (2020). The age of surveillance capitalism: the fight for a human future at the new frontier of power. Public Affairs. Prof. Zuboff explains how tech company collection and monetization of behavioral data is extracted from user's computer interactions.
20. Shivakumar, S. (2021, March). How Data-Sharing Partnerships Can Thwart Counterfeits on Online Marketplaces. Center for Data Innovation. https://www2.datainnovation.org/2021-data-sharing-counterfeits.pdf
21. New, J. (2019, September 18). *The Promise of Data-Driven Drug Development*. Center for Data Innovation. https://www2.datainnovation.org/2019-data-driven-drug-development.pdf
22. In contrast, some have argued that despite its drawbacks, data localization is inevitable and an effective tool against the data monopolies held by a few large technology companies. Thierry Breton, France's former Finance Minister, argues that an open internet is "naïve" and suggests that requiring EU data to be stored on EU servers would protect EU citizens from what he calls "abusive and unlawful" data requests from other countries. Edward Snowden's leak of classified intelligence revealing the extent of U.S. government surveillance into communications stored by U.S. technology companies on U.S. servers seems to weigh heavily on at least some EU policymakers.

    Claypoole, T. (2021, February 23). *Data Localization and the Limits of "Everything from Everywhere."* JDSupra. https://www.jdsupra.com/legalnews/data-localization-and-the-limits-of-5695264/
23. Here, we use the term "data localization" to indicate restrictions on the collection, processing, and storage of data at a particular location or region, as well as restrictions on what data can be transferred away from that location or region. For the most part, these restrictions are imposed by state actors on all data generators or data collectors where they reside or operate. We use the term "data hyper-localization" to refer to strict data regulations that are aimed at a particular company (e.g., Company XYZ) or industry segment (e.g., all facial recognition companies or all apps from a particular country or company) and are designed to protect not only citizens' privacy, but also to establish or maintain a competitive edge in the development of AI. These restrictions may be imposed by state actors or imposed by private companies offensively or defensively.
24. Here, we use "mistrust" to refer to a person's suspicion that others, including companies, state actors, and political groups, misuse and abuse data for economic or militaristic advantage, but where concrete and definitive evidence to validate those beliefs may not exist or be readily apparent. Where applicable, we use "distrust" to refer to concerns that others have been or are misusing or abusing data, especially user data, for any reason, where there is evidence to validate those concerns. The terms are not mutually exclusive, as a person may mistrust and distrust another actor when it comes to the collection, storage, and use of data related to operation of AI systems.
25. The notion of mistrust caused by fear and uncertainty about another's data practices is part of a broader area of study called "trustworthy AI," which invokes technology solutions addressing reliability, safety, security, privacy, availability, and usability. Wing, J. (2020, February 14). *Trustworthy AI*. Cornell University. https://arxiv.org/pdf/2002.06276.pdf.
26. Cailliau, R. (1995). *A Little History of the World Wide Web*. W3C. https://www.w3.org/History.html.
27. *History of the Web*. World Wide Web Foundation. https://webfoundation.org/about/vision/history-of-the-web/.
28. *Id.*
29. Cailliau, R. (1995). *A Little History of the World Wide Web*. "April 1993" W3C. https://www.w3.org/History.html.
30. Reinsch, W. A. (2018, July 11). *A Data Localization Free-for-All?* Center for Strategic and International Studies. https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all.

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

31. Borgen, C. (2019, May 23). *Internet Censorship in Russia and China*. The Borgen Project. https://borgenproject.org/internet-censorship-in-russia-and-china/.
32. Wei, Y. (2019, July 11). *Chinese Data Localization Law: Comprehensive but Ambiguous*. The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.
33. European Commission (2020, February 19). *A European Strategy for Data*. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
34. European Commission (2018, April 25). *Artificial Intelligence for Europe*. https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-237-F1-EN-MAIN-PART-1.pdf.
35. European Commission (2019, April 8). *Ethics Guidelines for Trustworthy AI*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.
36. European Commission (2020, February 19). *A European Strategy for Data*. https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
37. Office of Management and Budget (OMB). *2020 Action Plan*. Federal Data Strategy (2020, October 21). https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf.
38. *Initial Consensus Judgements*. Interim Report - Section IV, 4: Protect and Build Upon U.S. Technology Advantages. National Security Commission on Artificial Intelligence (2019 November). https://science.house.gov/imo/media/doc/Schmidt%20Testimony%20Attachment.pdf.
39. *Final Report*. National Security Commission on Artificial Intelligence (2021, Mar. 1). https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf
40. Hawley, J. (2019, November 18). *S.2889 - 116th Congress (2019-2020): National Security and Personal Data Protection Act of 2019*. Congress.gov. https://www.congress.gov/bill/116th-congress/senate-bill/2889.
41. California Consumer Privacy Act of 2018. http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
42. We observe that, at the same time data localization restrictions are being imposed in some circumstances, there is also a general belief in better openness when it comes to intra-agency and international data sharing (at least among allies) to improve trust and AI development. National Security Commission on Artificial Intelligence (NSCAI) (2021, March 1) (describing cross-border data sharing). *Final Report*, at p. 248; White House (2019, February 11), Unleashing AI Resources ("The [AI] initiative directs agencies to make Federal data, models, and computing resources more available to America's AI R&D experts, researchers, and industries to foster public trust and increase the value of these resources to AI R&D experts, while maintaining the safety, security, civil liberties, privacy, and confidentiality protections we all expect."). Office of Management and Budget (OMB). *2020 Action Plan*. Federal Data Strategy (2020, October 21). https://strategy.data.gov/assets/docs/2020-federal-data-strategy-action-plan.pdf. Organisation for Economic Co-operation and Development (OECD) (2019, May 21). *Recommendation of the Council on Artificial Intelligence*, Recommendation 2.2 (Fostering a digital ecosystem for AI) ("In this regard, governments should consider promoting mechanisms, such as data trusts, to support the safe, fair, legal and ethical sharing of data.").
43. Mitchell, M. J. & A. (2020, August 27). *Republicans and Democrats distrust social media sites for political and election news*. Pew Research Center's Journalism Project. https://www.journalism.org/2020/01/29/an-oasis-of-bipartisanship-republicans-and-democrats-distrust-social-media-sites-for-political-and-election-news/.
44. Fight for the Future. (2020). *Ban Facial Recognition* website map (graphically listing state and local restrictions on facial recognition). https://www.banfacialrecognition.com/map/.
45. WA Senate Bill 6280 (2019). http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729.
46. Smith, B. (2018, July 13). *Facial recognition technology: The need for public regulation and corporate responsibility. Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.
47. Executive Order 13943, *Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services*

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

Supply Chain. White House (2020, August 6). https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/.

48. Executive Order 13942, *Addressing the Threat Posed by TikTok*. White House (2020, August 6). https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/.
49. *Id*.
50. At the time of writing, federal courts had issued preliminary injunctions stopping the bans on WeChat and TikTok; the Justice Department has appealed both. McCabe, D. (2020, October 2). *U.S. Appeals Injunction Against WeChat Ban*. The New York Times. https://www.nytimes.com/2020/10/02/technology/wechat-ban-court.html.

    Isaac, M. (2020, October 8). *U.S. Appeals Injunction Against TikTok Ban*. The New York Times. https://www.nytimes.com/2020/10/08/technology/us-appeals-injunction-against-tiktok-ban.html.

    In response, China's leaders imposed their own restrictions on the sale of TikTok, citing the need to protect Chinese-made AI technologies.
51. Bessi, A., Zollo, F., Vicario, M. D., Puliga, M., Scala, A., Caldarelli, G., & Quattrociocchi, W. (2016, August 23). *Users Polarization on Facebook and Youtube*. PLOS ONE. https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0159641.
52. DiResta, R. et al. (2018, December 17). *The Tactics and Tropes of the Internet Research Agency*. Disinformation Report. https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf.
53. U.S. Senate. (2020, August 18). *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 5: Counterintelligence Threats and Vulnerabilities*. Report of the Senate Select Committee on Intelligence. https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf.
54. Holmes, A. (2020, October 6). *House lawmakers say Facebook, Google, Apple, and Amazon are monopolies that need to be more heavily regulated — and potentially broken up*. Business Insider. https://www.businessinsider.com/house-democrats-facebook-google-apple-amazon-are-monopolies-antitrust-report-2020-10.
55. U.S. House of Representatives (2020, July 29). *Online Platforms and Market Power, Part 6: Examining the Dominance of Amazon, Apple, Facebook, and Google*. Hearing of the Committee on the Judiciary, Subcommittee on Antitrust, Commercial, and Administrative Law.
56. U.S. Senate (2020, October 28). *Does Section 230's Sweeping Immunity Enable Big Tech Bad Behavior?* Hearing of the Committee on Commerce, Science, and Transportation.
57. *U.S. et al. v. Google LLC*, No. 20-cv-03010 (D.D.C., filed Oct. 20, 2020).
58. In a sign that Congress is willing to act when an AI technology threatens immediate and traceable harm to individuals, lawmakers may soon require hyper-localized restrictions on data collection and use in the field of generative adversarial networks (GANs) technologies, which can be used to convincingly superimpose a person's face and voice biometric data onto another's body, sometimes for entertainment purposes but also for nefarious one (e.g., so-called "deepfake" videos). S.2904—the *Identifying Outputs of Generative Adversarial Networks Act of 2020*—has passed both chambers of Congress and was sent to the President on December 11, 2020, to be signed into law. The law would require the National Science Foundation (NSF) and National Institutes of Standards and Technology (NIST) to "support merit-reviewed and competitively awarded research on manipulated or synthesized content and information authenticity, which may include fundamental research on digital forensic tools or other technologies for verifying the authenticity of information and detection of manipulated or synthesized content, including content generated by generative adversarial networks." The output of that research could form the foundation for specific regulations, including data restrictions, imposed on the underlying technology.
59. Adopting transparency and explainability policies around data and AI to improve trust among users in the U.S. may not dispel the mistrust held by government leaders toward each other unless companies outside the U.S. also adopt policies at least as strong as those in the U.S. Even then, geopolitical factors may continue to impose anti-globalization pressure on data and AI, providing justification for continued data localization and hyper-localization restrictions by government leaders. For example, efforts by the White House against TikTok likely had as much to do with ongoing political posturing by the countries' leaders involving disputes over trade, spying,

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30

and other matters, than they do about misuse of user data. Similarly, the U.S. Department of Commerce, Bureau of Industry and Security's imposition of export controls on certain foundational AI computer vision software was likely aimed more at protecting national security interests than addressing data privacy. Federal Register, Vol. 85, No. 3, pg. 459 (January 6, 2020). And the U.S. Federal Communications Commission's (FCC) resolution blocking China-based Huawei's roll-out and implementation of 5G wireless infrastructure in the U.S. was apparently as much about protecting U.S. technology industry interests and competitiveness as it was about national security concerns. *See* FCC 19-121, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*. (released Nov. 26, 2019). https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

60. Standards developed by NIST may lead to government agency policies or new regulations, including those for AI model accuracy testing, providing public notice of intent to use data-based systems to make decisions, ensuring meaningful human-in-the-loop requirements in data-driven decisions, and civil rights guardrails such as disparate impact assessments, among others. Others have suggested expanding property-type laws to user data, thus creating a sort of proprietary interest and ownership rights in one's own data, as a means to address privacy issues and improve trust. The suggestion is based on analogies to copyright, patent, and publicity rights laws: if copyrights arise at the moment a person embodies a creative work in tangible form, and patent rights arise upon a person's concept of a unique and nonobvious concrete idea, and publicity rights arise when a person's persona (name and likeness) achieves a degree of value, so too should rights arise in a person's personal data when that data is created by the user and has economic value to the user or others. We leave for others the task of assessing the feasibility of these and other legislative and regulatory approaches to improving trust.
61. Litman-Navarro, K. (2019, June 12). *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*. The New York Times. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.
62. *Id.*
63. Paul, K., & Hosenball, M. (2019, November 6). *Facebook executives planned 'switcharoo' on data policy change: court filings*. Reuters. https://www.reuters.com/article/us-facebook-antitrust-idUSKBN1XG1QP.
64. Smith, A. (2020, April 8). *Using Artificial Intelligence and Algorithms*. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.
65. Kang, M. O. A. D. (2018, January 31). *AI in the court: When algorithms rule on jail time*. Phys.org. https://phys.org/news/2018-01-ai-court-algorithms.html.
66. Smith, A. (2020, April 8). *Using Artificial Intelligence and Algorithms*. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.
67. The Oversight Board's decision in any appeal is binding only with respect to that particular piece of content. It is up to Facebook to decide whether it is "technically and operationally feasible" to extend that ruling to "identical content with parallel context." Oversight Board Charter, Art. 4, Bylaws r. 2.3.1
68. Douek, E. (2020, May 11). *What Kind of Oversight Board Have You Given Us?*. University of Chicago Law Review Blog. https://lawreviewblog.uchicago.edu/2020/05/11/fb-oversight-board-edouek/
69. Besides the suggestions offered here for improving trust, we acknowledge there are other technical and non-technical approaches that may be as good if not better at achieving the right degree of data localization restrictions that address data openness (to enhance existing AI systems and enable development of newer AI technologies), and concerns governments, companies, and individuals have about national security, public interests, competitiveness, and protection of private rights.

OPEN ACCESS | Correspondence: Anastasia Dodd, adodd@blankrome.com. Received:December 16, 2020 Accepted: December 17, 2020 Published: March 12, 2021 Citation: Higgins B., Dodd, A. (2021). "Artificial Intelligence and Trust: Improving Transparency and Explainability Policies to Reverse Data Hyper-Localization Trends". Journal of Science and Law, 8(1): 1-11. doi:10.35005/q8t1-ek30