Dataset and object data tagging to improve trusted and flexible AI/ML and data utilization

Ian Wardell, MA, J.D. Candidate 2022, Seton Hall University School of Law, AI Policy Research Intern, Global Government Affairs, Intel Corporation, U.S.A.

Jun Takei, Ph.D., Principal Engineer, Global Government Affairs, Intel Corporation, U.S.A.

INTRODUCTION

Public trust is crucial to the development of AI because members of the general public, as both consumers and constituents of key governments, are critical stakeholders for technology adoption.[1] The media has a large impact on the way issues are framed in every field, including AI. Therefore, much of the way AI is depicted in the media can change public opinion and influence what kind of AI is developed in the future and how AI is regulated. In a 2019 poll Mozilla found that people are divided on whether AI will make society better or worse.[2] A Pew study on the public opinion of AI and automation showed dramatic differences in public opinion on AI and robotics by region. In this poll, 60% of respondents in the Asia Pacific region believed AI and robotics were good for society, while less than half the respondents in Europe and the United States held a positive view of AI.[3] However, with the exception of Russia and India, the Pew study found countries with higher education were more likely than countries without to support AI development. Based on the varying levels of public mistrust in AI, the regulatory environment values trustworthy and robust AI, which focuses on the public good.

EXISTING POLICIES SUMMARY

There are numerous legal uncertainties concerning AI across the regulatory landscape. There is a clear need for technical process, procedure and policy frameworks to bridge the gap between policy and technical implementation. This need is highlighted by a notable increase in technical regulation discussion and working groups as countries begin implementing "AI and ethics" policies. Further, data privacy laws continue to evolve and complicate the transfer of datasets from country to country, highlighting a need to develop

[1] Ouchchy, L., Coin, A., & Dubljević, V. (2020, March 29). Ai in the headlines. SpringerLink. Retrieved August 20, 2021, from https://link.springer.com/article/10.1007/s00146-020-00965-5

[2] *How people feel about artificial Intelligence*. Mozilla Foundation. (2019, November 7). Retrieved August 20, 2021, from https://foundation.mozilla.org/en/blog/we-asked-people-around-the-world-how-they-feel-about-artificial-intelligence-heres-what-we-learned/

[3] Johnson, C., & Tyson, A. (2020, December 15). *Are ai and job automation good for society? globally, views are mixed*. Pew Research Center. Retrieved August 20, 2021, from https://www.pewresearch.org/fact-tank/2020/12/15/people-globally-offer-mixed-views-of-the-impact-of-artificial-intelligence-job-automation-on-society/

enabling policies and accompanying technical tools to facilitate continued AI and machine learning development.

International. International law focuses on ethical use guidelines which are generally non-binding. UN groups such as UNESCO and the ITU started AI and ethics studies and published high-level recommendations. International policy on AI does, however, provide insight into widely accepted ideas and uncodified standards within the AI regulatory space. International standards bodies such as the International Standards Organization, ITU, and IEEE have either published or are near publication on ethical standards revolving around approaches to establishing trust in AI systems through transparency, explainability, and controllability. Further, these organizations look at engineering pitfalls and typically associated threats and risks to AI systems, along with possible mitigation techniques and methods.[4] Internationally there is no indication that unified and strict international regulations will be applied in 5 years.

Industry. Due to a lack of harmonized ethical and technical international regulation, Industry is generally self-regulated outside of specific fields on a country-by-country basis. Corporate self-regulation in the AI space is an example of horizontal self-regulation, where large companies' commitment to developing responsible AI creates incentives for others to join, similar to international regulation. Corporate self-regulation often enhances corporations' opportunity to shape future legislation as it creates a de-facto standard.[5]

PUBLIC CONCERNS

Public trust significantly impacts sales and the pace and severity of law and policy in the regulatory sphere. The core public concerns in AI center around Fairness, Privacy, Transparency, Controllability, and Transportability.[6] In 2019 the Edelman public relations and marketing consultancy firm published a special report compiling the impact of consumer trust, in this report 81% of consumers said "trust" is a dealbreaker or deciding factor in purchasing products. The special report highlighted that 62% of consumers had concerns about the pace of product innovation and increased automation, 55% were concerned about the use of customers personal data, tracking, and use of AI for service, and 69% worried about social impacts.[7] Consumer concerns and increased media attention to high-profile

[4] IEEE SA. (2020). *ISO/IEC tr 24028:2020 Ethically aligned design*. Retrieved August 20, 2021, from https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf

[5] OECD iLibrary . (2015). *Committee on Consumer Policy, Industry Self-Regulation*. Retrieved August 20, 2021, from https://www.oecd-ilibrary.org/industry-self-regulation_5js4k1fjqkwh.pdf

[6] Wardell, I. A. (2022). *Product liability applied to automated decisions*. eRepository @ Seton Hall. Retrieved August 20, 2021, from https://scholarship.shu.edu/student_scholarship/1214

[7] *PWC's Global Consumer Insights Survey 2021*. PwC. (2021). Retrieved August 20, 2021, from https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey.html

market sectors such as Autonomous Driving led to increase regulations and global policy positions.

Reduction of Public Concerns. Reducing public concerns is important because it reduces regulation which increases the supply of technologies on the market. Additional regulation, past a minimum baseline of consumer protection, restricts the supply of digital technologies by raising costs and reducing revenues for companies to invest in new products and services.[8] This is the Negative Trust Cycle.

RESEARCH SOLUTION: DATA TAGGING

Data tagging in AI allows for fine-grain control over object data sharing and helps reduce the growing resistance to AI tools. Data tagging to transfer permission with data objects can provide data transparency, fair and reasonable data collection and may assist in the development of bias detection in training data leading to a reduction of algorithmic bias. Overall, demonstrating technical implementations supporting AI regulation can lead to increased accountability and a reduction in liability.

Fairness. Data tagging assuages concerns related to fair and reasonable data collection through data disclosure because it allows for the transfer of permission with a data object. These permissions may include categorization, ownership, usage licenses, data deletion tags, and Sensitivity tags. Standardized models may provide test cases to ensure unbiased training data automatically. Fairness testing may track with data sets because accepted results may be added to the dataset as a whole. When changes are made, this result would change, as would the hash to ensure integrity.

Privacy. Compliance tags can be added and read to ensure data is used where the data provider consents to use for AI and training, reducing the risk of non-compliance. Not all data requires the consent of the data subject, such as data within the public domain. To verify that a dataset consists of public domain data objects, data objects may be tagged as public domain data. When a dataset consists of all public domain data, the dataset itself may also be tagged.

Transparency. Data tagging allows for the disclosure of the types of data used for training a machine learning model, how the datasets are stored and shared, and gives insight into how a data processor handles the data provided to them. Utilizing tagging allows for data tag visualization, showing a streamlined view of the types of data used in a dataset, demographics, legal obligations, bias statistics, and error rates. Because entire datasets can be

[8] Alan McQuinn, D. C. (2018, July 11). *Why stronger privacy regulations do not spur increased internet use*. Retrieved August 20, 2021, from https://itif.org/publications/2018/07/11/why-stronger-privacy-regulations-do-not-spur-increased-internet-use

tagged based on the individual objects within tagging future, developers can choose the right data for their training and testing.

Controllability. Data tagging brings significant benefits for controllability, both for individual data providers and the data processor. Where each data object is tagged with permissions such as ownership and permissions such as licensure and data deletion requests, the data provider can be given fine-grain control over where their data is being utilized and for which purposes. The process of data tagging also gives the data processor the ability to fully monitor compliance with different regulatory environments and allows for long-term data tracking, such as where the data was sold and what can be done with varying degrees of sensitive data.

Transportability. Transportability is an issue primarily for data processors and operators. Through the implementation of data tagging, the process of transferring datasets between multiple regulatory environments becomes easier. By providing an easy to utilize way to compare a given dataset and data objects to a set of regulatory standards, datasets can be pre-cleared for transfer, and where a dataset is not in compliance, the exact areas of non-compliance can be located. Because the issue of compliance can be narrowed down to specifically tagged non-compliant data objects, those objects may be removed, and a modified version of the dataset may be transferred as needed. Further, in the case that an individual removes their data from a dataset through some regulatory mechanism such as the GDPR, the dataset can be automatically updated to reflect these changes.

Implementation. Data tagging is a scalable way to handle data control. Utilizing widely available tools utilizing existing object metadata can allow for rapid implementation of data tagging practices. The process of tagging an object file or entire dataset may be done through the use of simple Exchangeable Image File Format (EXIF)[9] which is basic metadata created by a camera or image software whenever a photo is created. Similar metadata exists in most data formats and can be easily added when needed. Open sources tools such as ExifTool[10] allow developers to create programs to tag data in bulk. These programs may be either manually controlled or use machine learning to assist in tagging.

To update, view, and provide a 'drill down' for viewing data tags, databases can be created to interface with data objects and provide a view of the data relationships. This allows non-technical users to easily view where, when, and what each data object is, and what dataset or datasets a data object may be a member. This interface may also be utilized to

[9] *Metadata*. Merriam-Webster. Retrieved August 20, 2021, from https://www.merriam-webster.com/dictionary/metadata

[10] ExifTool is a Linux CLI tool, there are similar tools for Windows and OSX with and without a GUI. Exiftool by Phil Harvey. Retrieved August 20, 2021, from https://web.archive.org/web/20211122235924/https://exiftool.org

provide data deletion capabilities and track overall usage statistics. Ensuring that non-technical personnel, specifically policy specialists, can update data tagging relationships is paramount to the overall success of data tagging efforts.

Developing the data tagging tool itself is only one part of the solution. An up-to-date compliance database must be maintained to ensure that the correct data is tagged and adapted for current regulatory compliance. This database requires updating when new regulation is passed in a given region. From each regulation, the core compliance metrics, both ethical and technical, must be categorized and marked. To ease this process, premade categories can be developed to allow for a policy specialist to select which tag best fits or create a new tag for data tagging implementation.

Once the global policy database is completed and the tool to tag is developed, transparent testing methods can be implemented to integrate compliance assessment into the machine learning model testing and development process. These tests may be part of a continuous integration/continuous delivery (CI/CD) pipeline using either a DevOps or site reliability engineering (SRE) approach or implemented at the end of a model's creation in a traditional software development approach.[11]

Example Case. Tagging geographic data transfer for a country of origin can be done for images based on their geolocation tag within metadata. This case shows how tagging for a country code allows for a more efficient resolution of conflicts of law in dataset geo-transferability. Cameras commonly embed this metadata automatically as part of the saving process. To test country-level tagging a global sample dataset was utilized.[12] The data set contains more than 14 million geotagged photos crawled from Flickr with the corresponding metadata and provided for unrestricted use with citation. From this dataset, 40 images were selected for testing.

The tagging system intakes the media file, processes the metadata, and outputs a country code. If required, the system may be modified to include region, country code, state, county, and granular address data. For the purpose of international geographic data transfer, only the country code is necessary for processing. To process geographic metadata the system utilizes the OpenCage Geocoding API, which provides 2500 free geocodes.[13] There are two kinds of geocoding, reverse (latitude/longitude to text) and forward (text to latitude/longitude); this demonstration project utilizes reverse geocoding. An alternative to

[11] Red Hat. *What is Ci/CD?* Retrieved August 20, 2021, from https://www.redhat.com/en/topics/devops/what-is-ci-cd

[12] H. Mousselly-Sergieh, D. Watzinger, B. Huber, M. Döller, E. Egyed-Zsigmond, H. Kosch, World-wide scale geotagged image dataset for automatic image annotation and reverse geotagging, Proceedings of ACM MMSys 2014, March 19 - March 21, 2014.

[13] *Easy, open, worldwide, geocoding and Geosearch*. OpenCage. (n.d.). Retrieved August 20, 2021, from https://opencagedata.com/

OpenCage Geocoding is that each country code and region can be mapped in a database and looked up for each input. The OpenCage API requires an internet connection and API key to make API calls.

The output from the Tagging System resides on each media file which allows for transportability of tags between datasets. In this case, the tag is a country code. The country code is read by tag reader software which outputs the country and links to applicable law. Where finer detail is required, country codes may be accompanied by state/province codes that supply the applicable jurisdictional regulation.

CONCLUSION

The AI industry must be allowed to innovate in design, while allowing for consumer protection. The development of tools such as data tagging to support regulatory compliance allows for continued AI and industry standards development. Overall, supporting AI regulation solutions that assist in 'use' regulation, not development regulation, can lead to increased accountability and reduced liability without impeding technical development.