Kai Hueske-Van Ceylon

8/28/2021

BSSP Seminar

A Smarter Future: EU Artificial Intelligence Policy

Artificial intelligence is the driving force behind one of the most significant revolutions in modern industry. Predicted to add $13 trillion to global GDP by 2030 (Bughin et al., 2018), it's an incredibly powerful driver of economic growth which the EU hopes to harness. However, the increasing utilization of AI raises two main policy problems: ensuring that the data used in training AI systems don't infringe on citizens' data privacy, and regulating the use of the technology to protect fundamental rights. Various policy frameworks have been proposed to address these, most recently the European Commission's 2021 draft Artificial Intelligence Act, but there are still inherent issues in these solutions. The EU is finding a good policy balance between protecting citizens' rights and leveraging AI as a tool for economic growth; in addition to maintaining this balance and staying true to its role as a global leader, it should utilize emerging technologies to address remaining issues in this field.

Training AI systems requires tremendous amounts of data - the more data available, the better these systems work. However, perhaps unsurprisingly, the data generally need to be relevant to the field in which the system is applied. Particularly, this means that data gathered from industrial settings are useful in training AI systems to be utilized in the same settings, but those same data will likely be less useful in consumer settings (Kak & Sacks, 2021). For the EU, and especially for those hoping to attract innovation and make Europe the location of the next Silicon Valley, this is a difficult prospect. AI systems in consumer-facing businesses need large quantities of consumer data, posing more of a threat to personal data privacy than systems built on non-personal industrial data. This makes policies to promote a consumer-focused AI boom much more difficult to work with. Additionally, data in all sectors can display bias against certain

social groups, which means systems trained on these data can discriminate against or negatively impact such groups.

The problems don't stop once these systems are trained. AI is still fraught with possible uses that violate fundamental rights. One of the most concerning applications is in surveillance. Facial recognition technology, for example, can be a huge help to law enforcement in public spaces, allowing authorities to detect and respond to threats like crime and terrorism much more efficiently. However, this constant public surveillance is a violation of the right of EU citizens to privacy. This focus on fundamental rights, while in line with the EU's role as a global leader in responsible AI use, hinders its development and global competitiveness. Chinese companies like Huawei, less concerned with protecting privacy, have begun developing "smart cities" in Serbia, implementing similar surveillance in the name of safety (Vasovic, 2020). In addition to providing a profitable service (albeit of dubious ethical value), this surveillance provides China with still more facial data which can be used to further develop their AI capabilities and global competitiveness.

The use of AI in making important decisions relating to citizens' lives also merits regulation. Applications that could control access to important resources and services like education, professional training, or credit scoring have a potentially huge impact on daily life for those the system affects; if these systems malfunction, or have been trained on data which are biased against certain groups of people, then end users can be negatively affected or unfairly barred from essential resources. Beyond this, it's often simply reassuring for citizens to know that important decisions about their lives are being made by a fellow human being, rather than an inscrutable and faceless robot.

The misapplications of AI mentioned thus far have been problematic largely because of their potential unintended negative consequences. However, there are also applications which, beyond being dangerous to end users, are simply malicious. Events like the Cambridge Analytica scandal, where Cambridge Analytica used illegally obtained data and artificial intelligence techniques to build voter profiles and influence the 2016 US elections, highlight the ways AI can be used to directly manipulate people. This has become even more pertinent with the spread of misinformation campaigns (Confessore, 2018).

However, AI is also an incredibly powerful tool. When properly implemented, it has the capability to directly counter many of these issues, such as reducing bias in important processes (Caprino, 2021) and fighting the spread of misinformation and fake news (Marr, 2021). Beyond this, it's also a powerful driver of economic growth. AI is projected to increase labor productivity by 40% by 2035, by increasing the efficiency of time management. It also has the potential to create a new "virtual workforce", capable of performing tasks that would otherwise take up human workers' time, as well as solving problems and learning from the process (Szczepański, 2019).

In light of this, the EU needs to find some way to strike a balance between leveraging the potential of AI and protecting the rights of its citizens. To this end, EU policy has focused on regulating both the data used to train these systems and the implementation of the systems themselves.

EU data regulation takes a bifurcated approach: data is dealt with differently depending on whether it is personal or non-personal (Kak & Sacks, 2021). The GDPR is the EU's most well-known and well-established piece of personal data legislation; it regulates the collection and use of the data of European citizens based on seven protection principles. These are lawfulness,

fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. Of key relevance to AI development are purpose limitation, data minimization, and storage limitation. Data minimization and purpose limitation means that companies can't simply apply the "collect everything" approach; they must be discerning, collect only the data that they need for their systems, and explicitly specify the purpose of these systems to the data subject. Storage limitation means that companies can only store data as long as is necessary for training their systems (respecting the "right to be forgotten"), so keeping the data around "just in case" as a general resource isn't in compliance with the GDPR. Noncompliance such as this is punishable by heavy fines of up to €10 million or 2% of the noncompliant firm's annual revenue (whichever is higher) for less severe infringements, or up to €20 million or 4% of revenue for more severe infringements (Wolford, 2019). In short, the GDPR carries significant weight.

Non-personal data are regulated under a different and much more lenient framework. The Regulation on the Free Flow of Non-personal Data is a 2018 policy framework aiming to increase the flow of non-personal data across member state borders and create a single EU data market. Rather than imposing restrictive conditions on the use of non-personal data, the Regulation prevents member states from restricting where this data can be stored and processed (DG-CONNECT, 2021). This goal of a single data market reflects a shift in EU policy towards building solidarity and supremacy in industrial rather than consumer-driven AI (Kak & Sacks, 2021), leveraging the EU's existing "strong position in digitised industry and business-to-business applications" (COM, 2020).

In addition to policy solutions for data regulation, legislation is also being developed to regulate the actual *use* of AI. In early 2021, the European Commission published a draft of the

Artificial Intelligence Act, which aims to ensure the responsible development of AI in the European Union. Similarly to the GDPR, the AIA would apply to any entities within the EU market who utilize AI, and would impose fines for violation of its requirements. It defines AI broadly as "a suite of software development frameworks that encompass machine learning, expert and logic systems, and Bayesian or statistical approaches," meaning it deals with both technologies capable of learning from data and those based on logical and human-programmed rules.

It separates these systems into 3 categories based on their risk to human rights. The "prohibited" category includes systems that manipulate or exploit people (whether users or otherwise), enable governments to perform "social credit scoring," or provide real-time identification of individuals in public. Under the AIA, artificial intelligence can't be used for any of those purposes. Systems categorized as "high-risk" are those that form safety components of a product, fall under the coverage of any one of 19 particular pieces of EU market legislation, or are deployed in settings where the system could put lives or health at risk, or determine access to educational, financial, or justice services. High-risk systems must meet various requirements for safety, transparency, oversight, and absence of bias before being placed on the market. Finally, other uses of AI fall under the "limited-risk" category, and must only meet requirements for transparency (Mueller, 2021).

These policy solutions address many of the problems with AI related to fundamental rights. The GDPR deals with the collection of training data, covering many of the possible issues of privacy infringement and security. The AIA will complement this approach by preempting possible rights infringement in the utilization of AI tools by businesses with EU market exposure.

However, these regulations also significantly complicate the process of innovation and growth for consumer-driven tech companies; the use of consumer data and AI in these settings now entails many more legal hurdles, which can be difficult for small/medium enterprises like startups to overcome. This in turn tends to stifle innovation and competitiveness in the consumer tech sector. The Framework for the Free Flow of Non-personal Data, and the associated promotion of industrial data-driven innovation and technology, helps to alleviate the loss of competitiveness here, but it may still have significant impact; for those in the EU who hope to emulate Silicon Valley's innovation and economic success, a decline in the feasibility of consumer tech startups comes as a difficult blow.

The EU still has powerful prospects for AI-driven innovation and economic growth, however. The existing policy focus on growth in industrial AI and data, for example, plays to its strengths, and will increase its overall global competitiveness. In addition to this, it's worth noting that while the GDPR and the draft AIA restrict the use of personal data and AI applications, they don't completely preclude them. Innovation in these sectors is still very possible, if more complicated than in other countries like the US and China.

Further policy solutions to increase the EU's competitiveness in AI also exist. In particular, emerging technical methods can help address many of the privacy issues inherent in the use of personal data. More and more research is being done on methods for fully and irreversibly anonymizing user data (Bourtoule et al., 2021); if successful, such methods could provide an alternative path towards the utilization of personal data in training consumer-facing AI systems. This could merit an amendment to the GDPR to allow more lenient personal data regulations in cases where such methods were responsibly and transparently applied. Technical methods for increasing AI systems' explainability are also the focus of development, which

could transform these systems from inscrutable “black boxes” to more transparent “white boxes” (COM, 2020) This could address concerns about AI decision making and oversight in important sectors like lending, education, health care, and justice, and merit consideration in policy work going forward.

Beyond primarily technical solutions, the EU should also continue to maintain and strengthen its own role as a global leader in rights-based regulation, even in non-AI fields. This role has been established through legislation like the GDPR, and has a major impact even on foreign entities through regulatory pressures. The EU can leverage the significant power of its market to incentivize foreign businesses towards building AI systems that respect fundamental rights, leveling the global playing field and encouraging the responsible use of these technologies.

Artificial intelligence is driving the world into a new era. As with any resource, from the Internet to oil to coal or steel, the potential for misuse is great, but the EU has since its early origins in the ECSC been about peace, cooperation, and responsibility in the use of such dangerous tools. Its policy response, responsibly focused on balancing economic growth with fundamental rights, is well-founded and contains room for expansion and development as new technologies come to light, and with it the EU is well-equipped to lead the world into a new - and smarter - future.

Works Cited

Bourtoule, L., Chandrasekaran, V., Choquette-Choo, C. A., Jia, H., Travers, A., Zhang, B., Lie, D., & Papernot, N. (2021). Machine Unlearning. *IEEE S&P*.

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018, September). *Notes from the AI Frontier: Modeling the Impact of AI on the World Economy*. McKinsey & Company.

Caprino, K. (2021, January 7). *How ai can remove bias from the hiring process and promote diversity and inclusion*. Forbes.

COM, On Artificial Intelligence - A European approach to excellence and trust (2020). Brussels, Belgium; European Commission.

Confessore, N. (2018, April 4). *Cambridge Analytica and Facebook: The scandal and the fallout so far*. The New York Times.

DG-CONNECT. (2021, June 23). *Non-personal data*. Shaping Europe's digital future.

European Parliamentary Research Service, & Szczepański, M., Economic impacts of artificial intelligence (AI) (2019). Brussels, Belgium; European Parliamentary Research Service.

Kak, A., & Sacks, S. (2021). Shifting Narratives and Emergent Trends in Data-Governance Policy. *AI Now*.

Marr, B. (2021, January 25). *Fake news is rampant, here is how artificial intelligence can help*. Forbes.

Mueller, B. (2021). *A Quick Explainer of the Artificial Intelligence Act*. Center for Data Innovation.

Vasovic, A. (2020, August 13). *Serbia chooses links with China to develop ECONOMY, TELECOMS Despite U.S. warning campaign*. Reuters.

Wolford, B. (2019, February 13). *What is GDPR, the EU's new data protection law?* GDPR.eu.