ICDPPC declaration on ethics and data protection in artificial intelligence

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

Executive summary

The American Chamber of Commerce to the European Union (AmCham EU) welcomes the International Conference of Data Protection and Privacy Commissioners' (ICDPPC) declaration on Ethics and Data Protection in Artificial Intelligence (AI)[1], and the opportunity to respond to the related public consultation. To advance global discussions on these topics, following areas are of particular importance:

- Common governance principles on AI as called for by ICDPPC, including the creation of a permanent working group to which AmCham EU stands ready to provide input;

- Role models for accountability approaches to make AI more transparent and intelligible and minimise harm to individuals and unintended societal consequences;

- Standardisation activities on algorithm explainability as well as research and development (R&D) in this area;

- Commitment to responsible technology design upon which AmCham EU members stand ready to further discuss 'ethics-by-design' approaches;

- Foster automated decision-making (considering all legal bases available under the GDPR in addition to consent) in concert with substantive citizens' rights (ie, access, correction, deletion) and the obligations of organisations (security safeguards and accountability approaches); and

- Investment in R&D to detect biases and discrimination and commitment to well defined internal processes that ensure data quality and individuals' protection.

---

[1] https://icdppc.org/public-consultation-ethics-and-data-protection-in-artificial-intelligence-continuing-the-debate/

Introduction

The declaration rightly acknowledges the positive impacts AI will have on our society are undeniable, with the innovation pace across AI ecosystems unprecedented. Autonomous technologies are already deployed for life-enhancing and potentially life-saving applications, such as disease detection, driving assistance and smart agriculture. AI systems are enhancing efficiency and productivity, preventing fraud and crime, enabling better access to education and improving safety at work. While these developments are important and exciting, advances are not sustainable if potential unintended consequences are not adequately addressed by public and private organisations. Hence, it is critical to create a public policy and regulatory environment that fosters innovation and citizens' protection in parallel. **AmCham EU members which are at the forefront of AI research and are investing in the uptake of AI in Europe, welcome the opportunity to provide comments and ideas on the ICDPPC declaration.**

The resolution adopted by Data Protection and Privacy Commissioners at their 40th International Conference in Brussels gives a comprehensive overview of ethical, legal and social issues related to the development and deployment of AI-based products and services. Privacy and data protection today represent intrinsic and foundational concepts for our modern society, enabling individual freedom of choice and user control. Implementing data protection is also relevant to the discussions on digital ethics, which entails societal values such as dignity, freedom, equality and justice among many others. Therefore, **we encourage a greater collaboration between data protection authorities, national authorities and international organisations to address more broadly ethical data processing as well as needs and challenges of AI use and development.**

International principles for AI governance

ICDPPC rightly calls for establishing global principles for ushering in responsible AI technology development based on an international, cross-sectoral and multi-stakeholder approach. We acknowledge also the increasing relevance of involving regulatory authorities from other domains like consumer protection and competition for the purpose of creating a more comprehensive assessment.

Additionally, AmCham EU members stand ready to support the activities of the Working Group on Ethics and Data Protection and to share technical expertise to address the complexity of the current digital landscape and better understand the functioning of AI and machine learning technologies.

Safeguards for individuals without blanket limitations

The principle of fairness, as part of the OECD Fair Information Practice Principles[2] published in 1980, has inspired privacy legislation for the past four decades. Those principles still reflect internationally accepted values but need to be adapted to modern technology advancements in order to provide valuable guidance. Autonomous technologies make determinations that, in some cases, may affect individuals, their private lives and their interaction with the rest of society. The potential for harm – discrimination or restriction of choices and possibilities, for example – will create a number of situations that public and private organisations will have to address.

The ICDPPC declaration focuses on limits to automated decision-making to minimise risks for individuals and society. Solutions should be explored to foster appropriate data processing and to increase protection for citizens without limiting *a priori* autonomous technologies. In particular, safeguards for individuals could include control and judgment by humans for well-defined and specific AI-uses. Policy-makers and regulators should make that delineation in continuous dialogue with stakeholders and with industry advising on

---

technical feasibility. These protections should be reflected in organisations' data governance policies and documentation, as well as in training for developers.

Role model accountability

Protecting individuals and their data goes beyond legal compliance requirements: it means embracing societal values and working to build much-needed trust in technology and its positive impact on people. Responsible organisations take technical and organisational actions to minimise risks linked to their business and to monitor, redress and remediate harm.

AmCham EU members hold themselves accountable to put in place appropriate measures that address privacy, security and ethics concerns of customers, business partners and society. This translates into several actions, including but not limited to:

- Creating internal tools and training to implement privacy protections and to promote ethical design and use of AI;

- Carrying out internal audit and impact assessments;

- Defining data management policies, namely risk-based data processing practices throughout an AI product's lifecycle (from algorithms' training to market launch);

- Adopting technical mitigations, such as data de-identification techniques, differential privacy and encryption; and

- Establishing ethical review boards or councils to assess new products and technologies from their development to their deployment;

It is important to note in this respect that not all AI systems would require the same level of vigilance and oversight. Therefore, in the practical implementation of accountability there needs to be appropriate and effective differentiation of AI systems based, for example, on the level of risk arising from the context or purposes of the AI system or the potential harm to individuals.

Transparency and intelligibility of IT systems

The complexity and abstraction of deep learning tasks lead to situations where factors driving the output of algorithms can be hard to understand and explain. The ability to provide clear and meaningful information on AI systems entails different levels of detail depending on: (a) technical feasibility; (b) applications: industry quality control mechanisms do not need the same degree of explainability as a job selection; (c) use context: business-to-business (B2B) or business-to-consumer (B2C); and (d) protection of IP and trade secrets.

Achieving explainability will require organisations to take proactive steps to improve their ability to demonstrate that right processes are in place to implement privacy and promote internal oversight. Transparency and trust can be fostered by tools such as 'fact sheets' and by explaining the basic principles of how a specific AI system works (eg, how information is gathered and recommendations are produced). Increased accountability can also play a role in addressing transparency concerns in the age of AI.

AmCham EU members are contributing to ongoing international efforts to define standards for AI, like algorithm explainability, and believe that increasing investments in private and public research combined with accountability approaches can help make AI more transparent and intelligible.

Design technology responsibly

AmCham EU members have a record of accomplishments in designing technology solutions with privacy in mind ('privacy-by-design' and 'privacy-by-default'). Data protection impact assessments are solidly embedded in the product development processes of our companies and practices such as de-identification, bias detection and encryption have proved effective and reliable. Risk-based approaches to AI-based products and services represent the right path to pursue innovation while protecting citizens.

AmCham EU members reiterate their commitment to responsible design of technology and stand ready to further discuss 'ethics-by-design' approaches. On the one hand, defining ethical requirements entails a truly global debate on societal values that should be driven by policy-makers and regulators to respect human dignity and cultural diversity. On the other hand, accountability of organisations remains a key element of such responsible approaches and can really be a long-lasting solution to minimise adverse impacts and unintended consequences.

Citizens' empowerment

In the current technology environment, the principle of individual participation might be more challenging to apply due to the multiple contexts for data creation and collection. Balancing legitimate interests of entities processing data with expectations of individuals can be a tool to empower citizens in a way that also supplements the traditional model of notice and consent. Restrictive interpretations of provisions prohibiting automated decision-making might negatively affect basic functions of autonomous technologies, with no benefit for citizens. Technical means to detect bias in data sets on various platforms are already in place to increase transparency and to mitigate potential discriminatory outcomes in AI.

The ICDPPC should look at the 'legitimate interest' of data controllers/processors as a valuable legal basis for data processing in well-identified cases, as well as to foster (and not limit) automated decision-making in concert with substantive citizens' rights (ie, access, correction, deletion) and the obligations of organisations (security safeguards and accountability approaches).

Tackle biases and discriminations

Access to data is of paramount importance to develop AI-based products and services. Greater diversity of data will reduce the risk of unintended bias, especially in those sectors (ie, healthcare) where the broadest spectrum possible of the population needs to be adequately represented to make AI autonomous determinations truly accurate. Not only availability but also quality of data used to input algorithms define the reliability of their output. The potential presence of bias in datasets or in the design of algorithms feed users' distrust in AI technology. For these reasons, the ability to access large datasets and move them across borders serves the purpose of reducing harm and discrimination to citizens.

Accessing and moving data across borders, promoting data quality and robust data governance are essential to improve accuracy of AI determinations and minimise bias and discrimination risks. To achieve these goals, our member companies invest in R&D and reiterate their commitment towards improved internal processes that ensure fairness in the development and use of AI and individuals' protection.

Conclusion

Public trust is crucial to reap the societal and economic benefits of AI. Fostering innovation while ensuring societal good and individuals' protection requires an open, continuous dialogue and collaboration among different stakeholders. Leveraging public-private partnerships as well as cross-sectoral and international cooperation can contribute to find timely and appropriate solutions to the hard questions raised by disruptive technologies, such as AI.