IDEAS
ACTION
RESULTS

Artificial Intelligence Policy and the European Union

A Look Across the Atlantic

AUGUST 2022

Bipartisan Policy Center

AUTHORS

Sabine Neschke
Policy Analyst

Jeremy Pesner
Senior Policy Analyst

John Soroushian
Senior Assoicate Director

ACKNOWLEDGMENTS

BPC thanks all experts from industry, academia, and civil society who offered their expertise and feedback as part of the report writing process. The authors are grateful to Neeraj Chandra and Andrew Fung for their research assistance.

DISCLAIMER

The findings and conclusions expressed herein do not necessarily reflect the views or opinions of our partners, convening participants, BPC's founders, its funders, or its board of directors.

Table of Contents

Introduction

In late 2019, then newly elected European Commission President Ursula von der Leyen announced her intent to make regulating the use of artificial intelligence (AI) a top priority for Europe. She promised to "put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence" within her first 100 days in office.[1] Following this announcement, the European Union (EU) drove forward legislative efforts to address potential risks and harms with AI systems. However, designing government policy and regulation for AI systems and their use is no small feat; at the end of those 100 days, the European Commission had produced only a white paper exploring policy options.[2] In 2021, the Commission put forward draft legislation around AI that EU bodies and stakeholders actively debate today. Creating AI policy is difficult; it requires thoughtful consideration of the many perspectives involving this complex technology and ongoing conversations to aid future decisions and compromise solutions. This paper will present experts' and stakeholders' points of views and considerations for AI policy.

AI has become central to everyday life, transforming society in many ways. It is used in product recommendation systems for online marketplaces, voice recognition technology, and tools to help direct street traffic. Many lifesaving technologies rely on AI, from informing health care decisions to assisting rescue aid efforts. While the application and benefits of AI are numerous, there are also many challenges and risks. For instance, harmful bias in AI systems can perpetuate or exacerbate historical inequities in areas such as employment, health care, finance, and housing, and malicious actors can use AI tools to manipulate people.

The European Commission has made it a priority to create a regulatory framework that would prevent and minimize AI's negative effects. The United States, by contrast, has focused less on regulation and more on "soft law" approaches, such as guidelines, standards, and frameworks, complemented by tort and other existing laws (such as civil rights laws) to help hold people liable when harm occurs. Experts and policymakers, however, disagree with each other about how to design AI policy and what balance it should strike between different values, such as proactively working to prevent harm through government intervention and taking a more permissive approach to encourage experimentation and innovation.

The Bipartisan Policy Center is committed to finding common-ground solutions to establish trust, reduce harm, and promote innovation in the field of AI. In producing this paper, BPC worked with stakeholders from academia, industry, civil society, and others from the European Union and United States. Our goal was to better understand European regulatory approaches to AI, their influence on U.S. politics and society, and the challenges and opportunities of AI policymaking. Our efforts included in-depth conversations and survey responses by a wide range of stakeholders from diverse backgrounds, summarized in this report on AI policy in the EU.

Artificial Intelligence and Comparisons Between the U.S. and EU

AI and machine learning are not new, but they are becoming more powerful and influential with the increasing availability of large data sets, improved computing power, and greater storage capacity. AI and data are inextricably linked; a large volume of data is needed for training and testing AI systems, which can then analyze large amounts of additional data. AI systems require intensive computational power, and recent exponential improvements in computing power have enabled many modern AI systems.[3] Some examples of AI applications include autonomous vehicles and human-like text generation (such as GPT-3). Improvements in AI can lead to more uses and greater influence on how we work, live, and experience the world. Additionally, as developers make significant strides advancing AI, it is important to consider the implications of policies made today on future advancements and applications of technology.

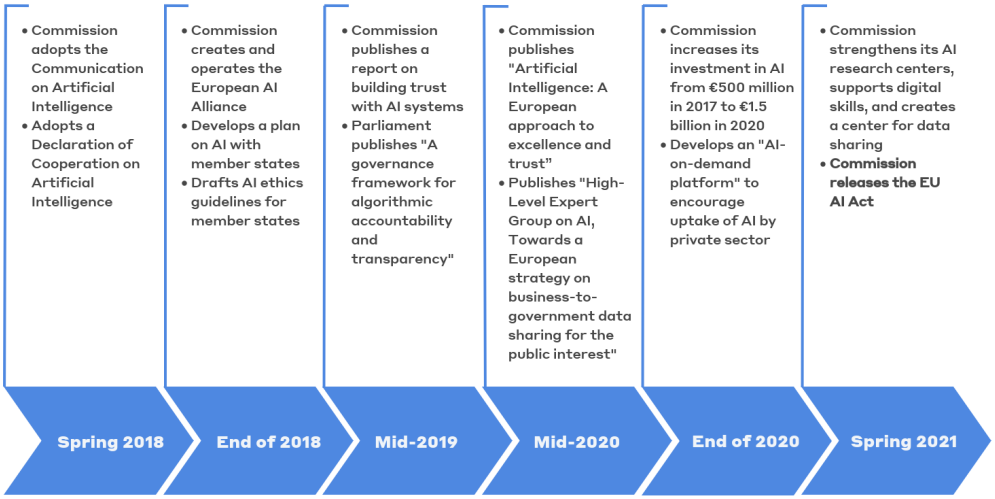
Because AI policies abroad affect the development and use of AI in the United States, thoughtful international discussion is necessary. EU regulations have often effectively set or shaped global standards – a phenomenon referred to as the "Brussels Effect."[4] For instance, many websites follow the General Data Protection Regulation (GDPR) internationally, even though they are regulations specific to the EU. Both national interest and some level of international cooperation will likely drive technology policy in the 21st century. The United States and the EU, for example, have a shared commitment to implement responsible stewardship of trustworthy AI,[5] centered on the OECD Principles on Artificial Intelligence of inclusion, fairness, transparency, robustness, and accountability.[6]

The United States and the EU have prioritized developing and using trustworthy AI, but their domestic political strategies differ. The United States is focusing on harmonizing standards through the National Institute of Standards and Technology (NIST), a federal agency, and has released its first draft of an AI Risk Management Framework to provide guidelines for developing AI.[7] In the EU, the European Commission proposed a broader regulatory framework for harmonizing AI policy across member states, known as the Artificial Intelligence Act (AI Act), which goes beyond just standards to create legal and technical obligations for potentially harmful AI. Many U.S. states are looking to pass their own laws and regulations around AI in place of a federal law.

Figure 1 shows a timeline of EU initiatives that have led to the development of the EU AI Act.

Figure 1

Timeline of European Commission Initiatives Leading to the EU AI Act



Sources: European Commission[8] [9]; European Parliament[10]; Reuters[11]

Differences between the U.S. and EU approaches to regulating AI stem partly from key structural differences between the two regions. For instance, according to many experts, the U.S. legal system has evolved to have a tougher tort liability regime relative to the EU, which may in part be driven by the U.S.'s common law system. A tougher liability system has costs and benefits, but it likely reduces the need for stricter regulation relative to other places. Further, differences between the EU and U.S. governance structures can affect the regulatory regime that is most appropriate for each region: The EU is a union of 27 member states, while the United States has a federal system governed under the U.S. Constitution.

The United States and Europe compete globally for leadership in AI, both with each other and other countries such as China. The United States has invested heavily in AI research and development: According to Stanford University's Global AI Vibrancy Tool,[12] the nation leads globally in total AI private investment, AI patent grants, and AI repository citations. The EU's recent AI investments are part of its Coordinated Plan to become a world leader in developing and deploying cutting-edge technology through €1 billion investments and plans to attract other public and private contributions.[13] Stanford University's 2022 AI Index AI reports global private AI investments in 2021 totaled $93.5 billion, more than double from the previous year.[14] The United States led in investment amount, followed by China and the European Union.

Recent research and development in AI have greatly influenced the global economy and societies and are expected to continue to affect growth worldwide. Development in AI is anticipated to significantly impact several industries, from retail to manufacturing to health care.[15] AI can improve supply chain decisions, increase efficiency in production lines, and help health care providers diagnose illnesses. The technology could be implemented in a variety of ways, focusing on risk management, predictive analytics, customer services, or R&D support, among others. The wide-

ranging versatility of AI applications underscores the financial implications that accompany them.

Despite the many positive contributions, AI has attracted some negative public attention and raised many important concerns in recent years. AI has brought challenges of algorithmic bias, which can foster inequities and harm many underrepresented groups and marginalized communities. For instance, Scientific American reported, "Algorithms trained with gender-imbalanced data do worse at reading chest X-rays for an underrepresented gender, and researchers are already concerned that skin-cancer detection algorithms, many of which are trained primarily on light-skinned individuals, do worse at detecting skin cancer affecting darker skin."[16] The combination of workplace surveillance and data collection with the increased use of AI brings issues of privacy and power asymmetries to the forefront. A piece by BPC reported, "Nontraditional employee monitoring tools that analyze emails or gather biometric data, have become more popular in the workplace over the years – a study by Gartner found more than half of companies surveyed in 2018 deployed some form of employee monitoring tool, a 30% increase since 2015."[17]

All of this has led to more awareness by policymakers about AI and a greater sense of urgency for them to address AI's ethical issues. Research shows an uptick in AI-related laws globally,[18] alongside increased mentions of AI in legislative proceedings and policy papers. For instance, the United States, Spain, Belgium, France, Italy, and Germany all passed AI-related laws in 2021. The upward trend may continue as governments and legislative bodies worldwide consider how to address AI's ethical and societal challenges while promoting responsible innovation.

To help guide well-informed policy decisions, we prioritize educating policymakers and stakeholders on important concepts in AI governance. Throughout this paper, we discuss learnings from recent policy developments in the United States and EU. As drivers of AI development, economic growth, and legislative action, these two governing bodies will be very influential in the future of AI. In the next section, we examine important broad-based issues present in many policy debates today.

Broad-Based Issues Relevant in EU AI Policy

BPC conducted a series of interviews with representatives from academia, industry, and civil society in the EU and United States who have expertise in the EU policy efforts around AI. We paid particular attention to the EU AI Act, currently in markup. This section will review several relevant issues discussed with experts and learnings from further research. These issues are non-exhaustive but provide important insights into ongoing debates around AI for close consideration by policymakers and stakeholders in the United States and the EU.

DEFINING ARTIFICIAL INTELLIGENCE SYSTEMS

There is no universally agreed-upon definition of AI. Coined by computer scientist John McCarthy, the term originated in 1956. The term often refers to intelligent technologies with capabilities that mimic human-like cognitive abilities. Some government bodies have attempted to define AI,[19] but industry, academics, and civil society groups often use very different definitions to suit their needs. AI often includes software that ranges from understanding human speech (such as Alexa and Siri) to predicting which pictures or content you want to see (such as the Facebook News Feed) to processing medical X-rays to help detect diseases.

Defining what constitutes an AI system is a pivotal point of the AI ACT. Many stakeholders providing feedback on the initial draft of the AI Act raised concerns that the definition of AI in the proposal (containing the complete list of techniques and approaches listed in Annex I,[20] including software-based "machine learning" technologies, "logic- and knowledge-based" systems, and "statistical approaches")[21] comprises too many systems and may lead to some uncertainty.[22] Stakeholders continue debating the definition of AI. Generally, advocates for a narrower definition consider simple algorithms or sorting technology to be outside the scope of AI and would therefore face unwarranted regulatory burdens under this legislation.[23] Advocates for a broader definition argue it should encompass any "software-based automated system" that "might have an impact on fundamental rights."[24]

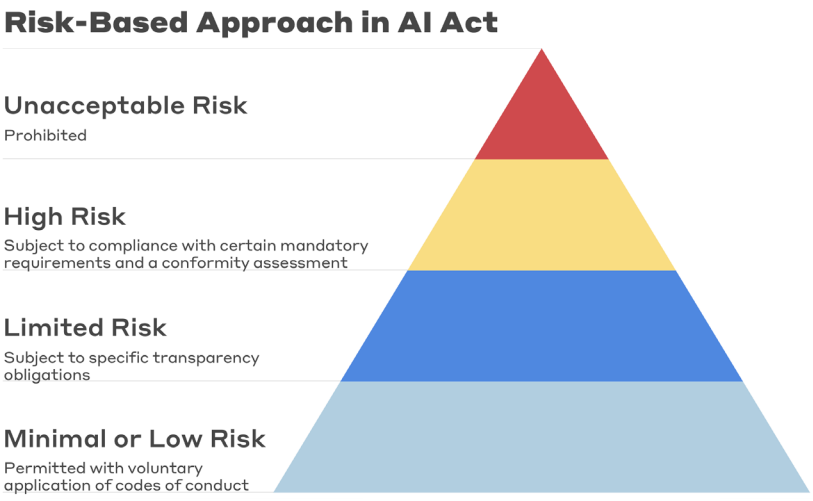
As the European Commission, and other policymakers in time, seek a compromise on a definition of AI systems, they should keep in mind the complexities of AI and the longevity of the legislation. AI technology will evolve and may not fit into the definitions carved out for AI systems today. Periodic reviews of the definitions and adaptability for technological advancements may help future-proof policies around AI.

RISK-BASED APPROACH

Generally, experts agree that a risk-based approach is necessary for regulating AI, but they disagree over the details and implementation. A risk-based approach involves categorizing AI systems or use cases based on the level of risk they pose and imposing different regulations and standards accordingly. Under this approach, policymakers and regulators can have stricter rules for preventing harm in high risk areas, and more permissive rules for low risk areas to reduce compliance burdens and promote experimentation.

A risk-based approach is reflected in proposals for regulations and guidelines in the EU and the United States. The EU AI Act differentiates regulatory obligations based on the risk an AI system poses, whether it creates an unacceptable risk, high risk, limited risk, or low or minimal risk (see Figure 2). As outlined in the AI Act, practices that fall under unacceptable risk are outright banned. They include AI systems that violate fundamental rights, subliminally manipulate people, exploit vulnerable groups such as children, likely cause psychological or physical harm, perform social scoring for use by public authorities, or collect real-time remote biometric identification data in public spaces for law enforcement purposes. AI systems classified under high risk face stringent obligations and enforcement under the AI Act, while limited, low, and minimal risk systems face less stringent or no obligations. In the United States, previous versions of proposed legislation, introduced by numerous democratic members, classified high-risk AI systems and proposed regulations specific to that category.[25] Additionally, NIST, the U.S. government agency responsible for developing an AI Risk Management Framework, is working to establish a risk-based framework to manage AI systems.[26]

Figure 2



Source: Europe fit for the Digital Age: Artificial Intelligence[27]

These efforts demonstrate the strong support for a risk-based approach to regulating AI, but experts debate how risks should be categorized and what should be in each category. Experts we spoke with focused the most on the categorization of high-risk AI systems. How the lines are drawn greatly affects accountability requirements and regulatory burdens for different AI systems. Additionally, because a risk-based approach requires assessment tools to determine risk levels, there is some debate about who should perform those assessments (whether by the developers themselves or by a third party).

HARD LAW VERSUS SOFT LAW

Hard law is a term used for government-enforced regulatory mechanisms like legislation and regulation, while soft law refers to policies, such as standards, best practices, and guidelines that are less enforceable by the government but more flexible. Each approach has benefits and drawbacks. Hard law can impose higher compliance burdens and be slower to adapt, but it has the benefit of the government's enforcement power. Soft law is more flexible and less burdensome but may be harder to enforce.

The EU AI Act uses hard law for riskier AI applications but soft law for less risky ones. The combination of the two approaches is due to the legislation's distinction between different risk levels and different enforcement power for each. Uses of AI that create unacceptable risks are prohibited. High-risk AI systems are mandated to comply with legal requirements, including conformity assessments, which is a risk analysis analogous to the process used by the Food and Drug Administration to authorize medical devices on the market. Limited-risk AI systems are subject to limited transparency obligations, such as disclosure of a video containing an artificially generated resemblance of a real person (or "deep-fake"). AI systems presenting low or minimal risk are not subject to legal obligations but may perform self-reviewed impact assessments and voluntary codes of conduct. While the distinction between hard and soft law is often vague, higher-risk AI systems are clearly subject to greater enforced obligations within the AI Act than lower-risk AI.

A debate exists over when to use hard and soft law to govern AI. Experts we spoke with often emphasized different concerns when discussing this issue. Some emphasized concerns that hard law may lock in regulatory requirements for incumbent technology, slowing technological advancements. Many others emphasized the need for prescriptive regulations to control AI systems that pose significant threats to users' health or safety, such as those used for medical devices. There is also great debate among experts as to whether and when policy should apply hard or soft law in instances where the risk level is unknown or uncertain.

PRECAUTIONARY PRINCIPLE VERSUS PERMISSIONLESS INNOVATION

Debate persists about whether and how much policymakers should take a precautionary versus permissive approach to AI technology. A precautionary approach seeks to achieve ex-ante protections, mitigating potential harms even before they are realized.[28] For instance, a government body can put requirements or guidelines in place for AI systems to meet specific standards before deployment, using either hard or soft law instruments. Given the potential for AI to seriously disrupt society in potentially negative ways, some experts recommend a precautionary approach over a permissive approach to discourage excessive risk-taking by developers when building systems. A permissive approach can give innovators more leeway to experiment and deploy AI systems without explicit government approval, but can still leave them open to lawsuits and large fines to discourage reckless risk taking. Due to the risk of stifling innovation through regulatory barriers, some experts advise against a precautionary approach and favor a permissive approach. A permissive approach, if well designed, can still mitigate and prevent many undesirable outcomes while allowing for greater experimentation and innovation.[29]

The EU often employs the precautionary principle when designing regulation and legislation, such as the AI Act.[30] The precautionary principle is most notably utilized in EU environmental law; The EU found precautionary regulations necessary to protect people from scientifically proven environmental risks and unpredictable consequences, such as aerosol sprays depleting the ozone layer or unsustainable use of fishery resources. Some believe many AI risks and uncertainties justify similar precautionary regulations in the digital environment.[31]

The United States generally embraces the notion of permissionless innovation, as exemplified in the 1990s when it developed rules around the internet and digital economy.[32] In the early 1990s, Congress expanded federal research funding and authorized the National Science Foundation to open NSFNET (what has evolved into the internet today) for commercial activities.[33] The United States maintained this strategy in 2019, when the Office of Management and Budget issued guidance following the executive order on Maintaining American Leadership in Artificial Intelligence.[34] The order stated, “Agencies must avoid a precautionary approach that holds AI systems to such an impossibly high standard that society cannot enjoy their benefits.”[35] Although the historical approaches to regulating AI are important to consider, today’s technology landscape differs considerably from decades ago, and even just a few years ago. Policymakers should weigh what they have learned from history with the information they learn today.

SECTOR-SPECIFIC VERSUS GENERAL APPROACH

A general regulation establishes obligations and policies that apply across industries or sectors, while a sector-specific approach focuses on a particular sector. For instance, a regulation that applies only to pharmaceutical drugs follows a sector-specific approach. In contrast, a tort law that applies in every sector of the economy follows a general approach.

The EU AI Act takes a general approach to regulating AI, but some argue that the framing of a risk-based approach shapes it into a sector-specific approach. The AI Act applies generally to the development, production, and use of AI systems across sectors. Despite its intended purpose, some experts are hesitant to say the AI Act indeed utilizes a general approach, suggesting some language targets specific sectoral use. For instance, some high risk classifications in the draft legislation may prescribe rules more relevant to some industries than others.

MITIGATING HARMFUL BIAS

The EU and United States both aim to combat harmful bias in algorithmic decisions. Biased data sets or algorithm design can perpetuate or exacerbate historical inequities and can cause significant harm to vulnerable populations and marginalized groups. Solutions to addressing this challenge have been a major focus of many stakeholders from government, civil society, academia, and industry. Leveraging people with a diversity of viewpoints and backgrounds when building and deploying AI tools or crafting AI policy can help cover blind spots and identify ways to counter harmful bias.

Addressing harmful AI bias requires a multipronged strategy using several approaches. However, the details of this strategy are still up for debate. Allowing industry to collect demographic data, such as age, race, or gender, to help detect, assess, and address algorithmic bias challenges is an approach that some have suggested for consideration. For example, demographic data can be used to understand and test for bias in an organization's recruitment algorithms. However, the highly personal nature of this data calls for further consideration when evaluating this approach. The stakeholders and experts we spoke with did not agree on whether and how to collect demographic data to detect and mitigate harmful bias. They generally expressed considerable reservations, but many were more open to the idea if policymakers could resolve certain important concerns. Two major concerns were about protecting data privacy and ensuring this data was used to mitigate harmful bias. Some ways to alleviate these concerns may include better data security, minimizing data collection to only what is necessary, privacy agreements to inform users about the information collected and its intended use, and mechanisms to hold companies accountable when they violate user trust.

Several other approaches were raised and discussed. One idea was creating regulatory "sandboxes" to study bias mitigation techniques and practices for certain AI systems

in a more limited real-world setting. Regulatory sandboxes would allow stakeholders to assess the feasibility of a practice in a controlled setting in the real world. Other techniques discussed included testing AI systems before they are deployed and exploring the use of anonymized or synthetic data to counter harmful bias.[36] A review of legal obligations in current legislation is also important to ensure they are the best approach to address harmful bias.

EU AI Act in Relation to Other Acts

The AI Act follows a series of other technology and data policies that the European Commission has proposed and passed in the past decade. The EU designed these laws to collectively regulate and guide some operations of technologies and technology companies, and all operate at the level of the entire European Union. Many of the acts affect the development of AI indirectly – AI depends on a high volume of data to work effectively, so any restrictions on the collection and use of data will invariably impact how AI systems operate. Furthermore, different laws and regulations interact with each other, so policymakers should be mindful of duplications, inconsistencies, and gaps in these laws and regulations. What follows is a brief summary of the relevant EU acts in data and technology, setting context for the environment in which the AI Act will be operating.

Policy	EU Act/Regulation	Summary
Artificial intelligence policy	Artificial Intelligence Act (AI Act)	The AI Act uses a risk-based approach through four risk categories, prohibiting the use of "unacceptable risk" AI systems and setting more strict requirements for "high-risk" AI systems that include a conformity assessment before market entry, a database that tracks standalone AI systems, and enforcement after market entry.
Regulation on data storage and privacy	General Data Privacy Regulation (GDPR)	The GDPR sets data privacy standards based on seven major principles: processing must be transparent, data use must be limited to specific purposes, no more data than needed should be collected, data should be accurate, data storage should be temporary, storage must be secure, and the collector must be accountable for all of this.
Regulation on digital platforms and services	Digital Services Act (DSA)	The DSA contains measures meant to help counter online illegal or harmful goods, services, or content, to assess and mitigate risks, and enhance supervision and enforcement by the Commission when it comes to very large online platforms.
Regulation on digital gatekeepers	Digital Markets Act (DMA)	Proposed in tandem with the DSA, the DMA explicitly gives the Commission the power to enforce certain behaviors of digital "gatekeepers," ensuring that other services and advertisers can interface with their platforms and conduct business outside the core platforms.
Regulation on data sharing	Data Governance Act	The Data Governance Act creates policy for data sharing in sectors such as health, environmental, mobility, agricultural, and public administration. The act's goals are to improve data availability, promote the reuse of data, ensure that data intermediaries can be trusted, and help data sharing across sectors and borders.
Regulation on data ownership, storage and transactions	Data Act	The Data Act, complementing the Data Governance Act, is designed to help users of connected devices to gain access to data from those devices, create protections for consumers from certain data sharing contracts, and enable users to switch cloud providers to access private sector data when necessary.

Key Takeaways

- The EU is taking a more precautionary and hard law approach to AI in comparison to the United States, as demonstrated by the European Commission's work on the proposed AI Act.
- Contextualizing the EU and U.S. approaches to AI requires consideration of other major differences between their legal and governance structures, such as their tort systems and regulatory capacities.
- The EU's AI Act may become a global standard and driver for other countries' policies, but the degree to which this could happen is uncertain.
- "AI" is not easily defined, nor is it a stagnant term. Policies should be mindful of AI's innovative potential and be prepared to evolve in the future.
- Stakeholders generally agree on a risk-based approach to AI policy but disagree on how to categorize the risks of AI systems and implement this in practice.
- The AI Act follows a hard law approach with enforcement measures for AI in higher-risk areas, while maintaining a soft law approach for lower-risk areas.
- A major debate exists around whether to take a precautionary or permissive approach to regulating AI, with the EU leaning towards the "precautionary principle" and the U.S. leaning towards "permissionless innovation." However, neither is entirely in one camp or the other.
- The EU takes a general approach to regulating AI, applying to the development, production, and use of AI systems across sectors, but a debate exists around how much the EU's categorization of high-risk AI systems follows a more sector-specific approach.
- Tackling harmful AI bias is critical, and a holistic and multipronged strategy to address this problem is necessary.
- The AI Act builds upon a broader context of existing EU regulatory measures, such as GDPR and DSA, as issues of AI are heavily interconnected with data and other areas of technology policy.

Endnotes

1. Ursula von der Leyen, *Political Guidelines for the Next European Commission 2019-2024*. Available at: https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf.

2. European Commission, *On Artificial Intelligence – A European approach to excellence and trust*, February 2020. Available at: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

3. Jaime Sevilla, Lennart Heim, et al., "Compute Trends Across Three Eras of Machine Learning," arXiv:2202.05924, March 9, 2022. Available at: http://arxiv.org/abs/2202.05924.

4. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

5. U.S. Department of Commerce, "U.S.-EU Joint Statement of the Trade and Technology Council," May 16, 2022. Available at: https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council.

6. OECD AI Policy Observatory, "OECD AI Principles overview," accessed July 14, 2022. Available at: https://oecd.ai/en/ai-principles.

7. National Institute of Science and Technology, *AI Risk Management Framework*, Draft, 2022. Available at: https://www.nist.gov/itl/ai-risk-management-framework.

8. European Commission, "A European approach to artificial intelligence." Available at: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

9. European Commission, Towards a European strategy on business-to-government data sharing for the public interest, 2020. Available at: https://www.euractiv.com/wp-content/uploads/sites/2/2020/02/B2GDataSharingExpertGroupReport-1.pdf.

10. European Parliamentary Research Service, A governance framework for algorithmic accountability and transparency, April 2019. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2019)624262.

11. Reuters, "EU to Invest 1.5 Billion Euros in AI to Catch up with US, Asia," April 25, 2018, sec. Technology News. Available at: https://www.reuters.com/article/us-eu-artificialintelligence-idUSKBN1HW1WL.

12. Stanford University Human-Centered Artificial Intelligence, "Global AI Vibrancy Tool – Artificial Intelligence Index," accessed July 14, 2022. Available at: https://aiindex.stanford.edu/vibrancy/.

13. European Commission, "Excellence and trust in artificial intelligence," accessed July 14, 2022. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_en.

14. Stanford University Human-Centered Artificial Intelligence, "The AI Index Report – Artificial Intelligence Index," accessed July 14, 2022. Available at: https://aiindex.stanford.edu/report/.

15. The Economist Intelligence Unit, "Intelligent Economies: AI's transformation of industries and society," 2018. Available at: https://impact.economist.com/perspectives/technology-innovation/intelligent-economies-ais-transformation-industries-and-society/.

16. Amit Kaushal, Russ Altman, and Curt Langlotz, "Health Care AI Systems Are Biased," *Scientific American*, November 17, 2020. Available at: https://www.scientificamerican.com/article/health-care-ai-systems-are-biased/.

17. Babu Jackson, "Prevalence of Biometric Data and Security Concerns," Bipartisan Policy Center, September 20, 2021. Available at: https://bipartisanpolicy.org/blog/prevalence-of-biometric-data-and-security-concerns.

18. Stanford, "The AI Index Report," 2018. Available at: https://aiindex.stanford.edu/report/.

19. Institute of Electrical and Electronics Engineers, IEEE Position Statement of Artificial Intelligence, June 24, 2019. Available at: https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE18029.pdf.

20. European Commission, *Annexes to the Proposal for Regulation of the European Parliament and Council*, April 21, 2021. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

21. Nick Gondek, "Learning about Machine Learning," Bipartisan Policy Center, August 4, 2021. Available at: https://bipartisanpolicy.org/explainer/learning-about-machine-learning.

22. Big Data Value Association, *BDVA Position Paper: Response to the European Commission's proposal for AI Regulation*, August 4, 2021. Available at: https://www.bdva.eu/sites/default/files/BDVA_DAIRO%20response-feedback%20AI%20Regulation_Final.pdf.

23. Centre for Data Ethics and Innovation, United Kingdom Government, "The European Commission's Artificial Intelligence Act Highlights the Need for an Effective AI Assurance Ecosystem," May 11, 2021. Available at: https://cdei.blog.gov.uk/2021/05/11/the-european-commissions-artificial-intelligence-act-highlights-the-need-for-an-effective-ai-assurance-ecosystem.

24. AlgorithmWatch and Access Now, "EU Policy Makers: Protect People's Rights, Don't Narrow Down the Scope of the AI Act!" November 23, 2021. Available at: https://algorithmwatch.org/en/statement-scope-of-eu-ai-act/.

25. U.S. Congress,, *Algorithmic Accountability* Act of 2019, H.R.223, 116th Congress, introduced in House April 11, 2019. Available at: https://www.congress.gov/bill/116th-congress/house-bill/2231/text.

26. National Institute of Science and Technology, *AI Risk Management Framework*, 2022. Available at: https://www.nist.gov/itl/ai-risk-management-framework

27. European Commission, Press Corner, "Europe fit for the Digital Age: Artificial Intelligence," April 21, 2021. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682.

28. World Commission on the Ethics of Scientific Knowledge and Technology, UNESCO, *The Precautionary Principle*, 2005. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000139578.

29. Adam Thierer, "Embracing a Culture of Permissionless Innovation," Cato Institute, November 17, 2014. Available at: https://www.cato.org/cato-online-forum/embracing-culture-permissionless-innovation.

30. European Parliamentary Research Service, *The Precautionary Principle: Definitions, Applications, and Governance*, December 2015. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2015)573876.

Bipartisan Policy Center

1225 Eye St NW, Suite 1000
Washington, DC 20005

bipartisanpolicy.org

202 - 204 - 2400

The Bipartisan Policy Center (BPC) is a Washington, D.C.-based think tank that actively fosters bipartisanship by combining the best ideas from both parties to promote health, security, and opportunity for all Americans. Our policy solutions are the product of informed deliberations by former elected and appointed officials, business and labor leaders, and academics and advocates who represent both ends of the political spectrum.

BPC prioritizes one thing above all else: getting things done.

@BPC_Bipartisan
facebook.com/BipartisanPolicyCenter
instagram.com/BPC_Bipartisan