weizenbaum journal OF THE DIGITAL SOCIETY

SPECIAL ISSUE 03

WEIZENBAUM JOURNAL OF THE DIGITAL SOCIETY
Volume 3 \ Issue 3 \ w3.3.8 \ 12-31-2023
ISSN 2748-5625 \ DOI 10.34669/WI.WJDS/3.3.8

Information on this journal and its funding can be found on its website:
https://wjds.weizenbaum-institut.de

KEYWORDS

AI regulation
artificial intelligence
European Union
technology ethics

VOICES FOR THE NETWORKED SOCIETY

Human Experience and AI Regulation

What European Union Law Brings to Digital Technology Ethics

Joanna J. Bryson

Hertie School of Governance
jjb@alum.mit.edu

ABSTRACT

Although nearly all artificial intelligence (AI) regulatory documents now reference the importance of human-centering digital systems, we frequently see AI ethics itself reduced to limited concerns, such as bias and, sometimes, power consumption. Although their impacts on human lives and our ecosystem render both of these absolutely critical, the ethical and regulatory challenges and obligations relating to AI do not stop there. Joseph Weizenbaum described the potential abuse of intelligent systems to make inhuman cruelty and acts of war more emotionally accessible to human operators. But more than this, he highlighted the need to solve the social issues that facilitate violent acts of war, and the immense potential the use of computers offers in this context. The present article reviews how the EU's digital regulatory legislation—well enforced—could help us address such concerns. I begin by reviewing why the EU leads in this area, considering the legitimacy of its actions both regionally and globally. I then review the legislation already protecting us—the General Data Protection Regulation, the Digital Services Act, and the Digital Markets

Act—and consider their roles in achieving Weizenbaum's goals. Finally, I consider the almost-promulgated AI Act before concluding with a brief discussion of the potential for future enforcement and global regulatory cooperation.

1 Introduction: The Present Technological Context

Almost a quarter of the way into the 21st century, we suddenly face the world of Joseph Weizenbaum's nightmares. Conversational agents built on artificial intelligence (AI) are seemingly everywhere, attributed all sorts of power—sincerely or insincerely—by people with varying degrees of knowledge of AI, let alone (prior) experience of it. Moreover, these attributions come from people with extremely varied motivations. Some are here to sell, others to buy, some to regulate, and others to evade regulatory constraint or taxation. Some are hoping for a new form of progeny, some are trying to end the phenomena of death, while others are looking to replace the human species. Of course, most are just looking for some combination of efficient productivity and personal entertainment, but this does not obliviate the hazards of moral confusion over AI.

These may be the least of our planet's problems, and were indeed only a fraction of Weizenbaum's concerns. We are suffering also mass civil displacements and deaths, including but not limited to wars both between and within countries, an escalating climate crisis, further ill health and biodiversity collapse deriving from many polluting and otherwise unsustainable industrial and consumption practices, and a geopolitical contraction of trust. The expansion of powers our innovation has afforded our species positions us in a seemingly endless cycle of needing to further augment our collective intelligence to address the problems we are newly able to cause.

Humanity and the rest of our ecosystem need us to enact substantial, radical, sustainable change as quickly as we can – and this time without further devastation. Such radical change requires the worldwide peace and equality that were Weizenbaum's principal concerns with respect to the moral application of AI. Going well beyond a simple ban due to the confusion of a chatbot for a friend, Weizenbaum (1986) describes extreme hazards of misuse of AI. Not only the abuse of computers to amplify our capacity for emotionless destruction via intelligent weapons systems, or their essential role in the complex task of designing nuclear weapons, but also the potential misuse that arises from neglecting AI's positive utility for resolving resource scarcity, and (separately) the inequities in distribution that Weizenbaum saw underlying armed conflict.

While we seek to understand the landscapes of both solutions and problems generated by our innovations, we must recognize that AI is not the only new source of intelligence. Much of the increasing pace of change might be attributed to our ever-wider access to fellow humans. During the period 1918–2018, half of humanity moved out of extreme poverty. Our overall proportion in that condition decreased from 60% to 10% at the same time that that our overall population quadrupled. Almost half the percentage drop in poverty came after 1995 (Roser, 2021). Simultaneously with this bettering of life chances and increase in numbers, we have also been widening access to both education and information communication technology (ICT.) As of 2023, over 65% of people have some access to the Internet (DataReportal et al., 2023). One powerful form of ICT is social media, some of which enable important new channels of communication and collaboration between peers (including experts) who might otherwise never have discovered one another. Further, those of us lucky enough to have sufficient bandwidth or local computation available now have access to startlingly accurate language translation. Physical transportation has also become increasingly affordable, affording direct communication. All this opens windows to insight never before imagined.

Yet, while education, transport, and access to information are entangling and enhancing minds in ways we can barely conceive, swathes of humanity are losing familiar liberties. This is due not only to increasingly pervasive surveillance, but also perhaps worse to a concurrent hardening of governance styles. That many governments now seem ready to both acquire and express enhanced capacities to surveil is hazardous even if those currently in office presently use these abilities benignly. Domestic autocratic consolidation of political power can be achieved not only by eliminating or undermining political opposition figures, but also by disrupting even the potential for political organization. Leaders and intelligentsia no longer need to be conspicuously eliminated. Social-scoring type systems facilitate reducing the life chances of "wrong-thinking" individuals, such as academics studying topics considered dangerous to a regime. Internationally, long-used strategies of propaganda and other means of interfering in the affairs of competing (and even cooperating) states are being enhanced and escalated. Advances in AI make it easier to identify individuals in foreign countries or your own susceptible to your influence. AI also aids all parties in modelling expected outcomes of such interventions, including impacts on elections.

There is though also substantial cause for hope. Globally, both greenhouse gas emissions per person and the number of persons seem to be levelling off, and may even soon decline.[1] We have largely healed the hole in the ozone layer, we are increasingly able to treat diseases including cancer, and, as mentioned earlier, education and equity both show positive trajectories. The same tech-

[1] Note that there is no reason to take such successful regulation to indicate impending extinction (Roser, 2023).

nologies improving the capacity of governments (and other organizations) to surveil and repress could equally be used for any other applications of informing and control, including beneficial and consensual ones.

We could be and sometimes are already using AI's potential to increase justice, representation, and democratic expression. In many jurisdictions (including some we categorize as autocracies), digital technology has been used to simplify access to government services, including the reporting of problems. On a global scale, we have seen increasing innovation of and accessibility to commercial digital services, including email, video conferencing, and automated search. There ought to be discoverable means to better ensure that communication technology is used to create transparency—or, as some now call it, legibility (Pilling et al., 2023)—for ordinary citizens. Progressive application of AI should allow us all to better understand the world around us, or at least the actions of our governments, corporations, and indeed our AI systems themselves. We should not only be able to understand the intelligent technology we use but be able to use it to help ourselves to collectively, beneficially regulate our ecosystem, economies, and security more generally.

If we start from a functionalist position that ethics describes the set of behaviors that maintains a society, then we can see the problem of maintaining the ethical use of technology to be one of governance—a means by which a society deliberately regulates itself, producing public goods, and ensuring its own self-preservation, in contrast to regulation due to externalized forces, such as starvation or war. There is—at least by treaty—global agreement that ethical outcomes require each nation to not only respect but actively defend the fundamental rights of all humans within its borders. These obligations include positive rights such as employment and health care (United Nations, 1948). More recently, it has also been agreed (also at the UN level) that the universal defence of human rights both mandates and is mandated by the goal of achieving ecological sustainability (United Nations General Assembly, 2015).

The largest single—or at least harmonized—jurisdiction presently trying to legislate and enforce a rights-based digital technology ethics is the European Union (EU; Bradford, 2023). In this article, I have already established the basic motivation for the EU (or indeed, any polity) to regulate information technology. I will now discuss why and how the EU has arrived at this juncture. Subsequently, I will return to the Weizenbaum-esque inquiry into how people–under EU law–can understand their AI systems, and be defended against their misuse, including the deployment of anthropomorphic tactics of deception. I will, in particular, emphasize laws already enforced: the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Digital Markets Act (DMA); I will also examine briefly the contributions of the nascent AI Act (AIA). In short, Weizenbaum might be proud: the one requirement the AI Act makes of all AI is that it be clearly identified as such to users. However, the biggest question opened by Eliza–of whether users under-

stand the full implications of an intelligence being artifactual–is perhaps better addressed by the EU digital legislation already in force.

2 Why the EU?

I just stated that the EU is the largest jurisdiction presently trying to legislate and enforce rights-based digital technology ethics. There are reasons for all the caveats in that sentence. The EU is larger by population but not GDP than the US. However, the US is not trying to legislate or enforce technology ethics; instead, it is trying to encourage the digital sector to voluntarily conform to certain standards. The EU is (or has recently been) larger by GDP but not population than China, and China is working actively to legislate technology governance. However, China's focus on rights is limited by its larger focus on stability and security. Fundamental rights and government legitimacy are seen as essential only to the extent that they serve this primary goal. China's argument is structurally the same as "put your own oxygen mask on first." Without a state, there is no one to defend individual rights.

Europe's greater prioritization of individual human rights is at least partly an outcome of many horrific centuries of war. So far, these seemingly culminated in the 20th century, during which mass killings were more likely to be effected against you by your own state than by somebody else's (Rummel, 1995; Valentino, 2004). Here, I refer to not only death camps and death marches but also policy-driven starvation, often under the guise of collectivized farming. In absolute terms, Mao and Stalin both killed more people than Hitler, and still other countries killed a higher proportion of their own residents[2]. The EU, although established as a trade organization, not a security one,[3] was explicitly designed to bring an end to wars within Europe, particularly between member states. The EU has been viewed as sufficiently successful in this goal that it was awarded the Nobel Peace Prize in 2012.

However, the European focus on human rights may not be a simple consequence of collective trauma–which sadly is shared more globally–but rather also a reflection of strategy. The EU accounts for roughly 20% of the world's GDP[4] with less than 6% of its population. Investing relatively heavily in each individual may therefore be any combination of: a strategic necessity, a winning economic

---

[2] Following from the Universal Declaration of Human Rights (UDHR), I focus on residents here rather than citizens to avoid questions of which individuals "should" have citizenship. The UDHR creates a world wherein every individual is owed the protection of at least one state: whichever state they are standing in at a given moment. This assumes, of course, that there are no failed states–that all territory of the Earth has some responsible government.

[3] EU security is broadly though not entirely guaranteed by individual member states' belonging to NATO, a partnership that presently includes the US.

[4] Estimates vary; the International Monetary Fund reported 22% in 2019.

strategy, or the luxury of a very wealthy region. Investing in the well-being of even minority populations certainly seems to be an essential attribute of strong democracies, though the direction(s) of causality here may be complex (Rovny, 2023; Gibler and Owsiak, 2018).

Most people who question why or indeed whether the EU should be regulating global technologies focus not on the EU's internal motivations, nor on the mandates of international legal conventions. Rather, the question is why a region with no leading AI companies (where 'leading' is defined by size) should be the one that regulates AI. If we shift the question to ask instead whether the EU itself has competence in AI, then in fact it does. The EU not only produces more AI Ph.Ds. than any other comparable global region, but it also produces comparable numbers of WIPO-defended AI patents to China (Bryson and Malikova, 2021; Dorfs and Bryson, 2024). Further, the aggregate market capital of the companies that hold these patents is comparable to the aggregate market capital of the (more concentrated) Chinese companies. Interestingly, the rest of the world (excluding the US) outweighs the sum of the EU and Chinese capacities on both these metrics, and the US dominates all other countries combined. Given then this competence, and the EU's wealth and regulatory capacity, its obligations to its own citizens and residents–including under international treaty, but also under its own laws–demands that it regulates AI. The real question should be why other regions do not.

Bradford (2023) portrays China, the US, and the EU as three possibly overlapping empires of AI regulation, which she frames as hardware-driven, market-driven, and rights-driven respectively. Another framing of regulatory orientation in these regions might be surveillance autocracy, surveillance capitalism, and privacy. The problem with any form of surveillance is that information, once stored, can be accessed. Governance styles are not necessarily permanent, and indeed large, monopolization-prone power structures or resources have long been thought to encourage autocracy.

This brings us back to the question of why the EU does not feature large individual corporations generating AI. The reason is firstly that an early democracy, the US, innovated a legal practice called antitrust towards the end of its difficult first century. After much debate, the US came to the conclusion that too much concentration of commercial or economic power could undermine a democracy's capacity to govern (Wu, 2018). Antitrust law is intended to ensure that those with dominant positions in a market do not unfairly exploit those advantages to further undermine competition. Badly behaving (or perhaps just overly large) companies should be disaggregated, or "broken up." The ideal is that markets should be able to set fair prices and ensure good corporate governance through open competition. Where it better serves the public good to have a single organization operating at scale, then the market's capacity to regulate both prices and within-sector corruption has to be replaced by extra regulatory attention from the government. This is the case for utilities, such

as telephones and electricity, and probably also for some categories of digital services.

Besides the common sense of this, the second reason the EU has antitrust law is because it was imposed by the US on Germany (and Japan) following the Second World War. The wars were seen as having been caused at least in part by facilitation of dictators by overly-powerful single companies. Those monopolies were broken up under the direction of the Allied forces, and the constitutions of the offending countries altered to ensure that antitrust regulation would prevent the situation from recurring. The EU largely retains West German competition law, though with some adjustments, leading to occasional conflicts between Germany and the EU on antitrust matters.

This returns us to the real question, mentioned earlier: why the US does have such large digital technology companies. Or if something like network effects makes the scale of these companies essential, why they are not more carefully regulated like the (other) utilities. Although often attributed to something special or sudden about the digital "platforms" that have been evolving over the last thirty or forty years, there has in fact been a deliberate relaxation of rules regulating the scale of all corporations in the US. The "Chicago School" of antitrust or competition law was first popularized in the late 1970s, about the same time as the Soviet economy peaked (Hanson, 2014; though see Miller, 1962 on the origins of the Chicago School). This school of thought, which assumes that only consumer welfare–as measured through consumer prices–is a suitable concern of government, gradually assumed greater prominence. Its first conspicuous application was in the settlement phase of United States v. Microsoft Corp. 2001. The decision to not disaggregate Microsoft marked the triumph of the Chicago School in the US. The US has since even sought to block the EU from enforcing the merger laws that the US had initially demanded Germany implement (Patterson & Shapiro, 2001).

The result of all this is that the EU not only addresses Weizenbaum's concerns about peace, but it is also presently the best-positioned jurisdiction to address his concerns about the plausibility of the ethical production and use of AI, which includes but is not limited to making AI systems well-understood. Collectively, the EU has the scale required to contest the laws of the nations producing the most powerful AI services. It also has the institutions, values, and explicit intentions to focus on the well-being and understanding of ordinary humans, ensuring that we can protect ourselves through our participation in our economies and democracies. Whether these are enough to give the EU capacity particularly for enforcement is presently an ongoing empirical experiment.

3 How EU Legislation Works Towards Human-Centered AI

At one time, it was difficult to discuss AI regulation without encountering the suggestion that it is controversial or even wrong to focus AI ethics on human concerns without regard for the AI itself. As the top tiers of international relations, international law, and human rights have engaged with the problem, it has been more common to emphasize human-centering as opposed to centering on corporations or perhaps governments, but no longer on machines. If machines could be meaningfully said to have any interests at all, those interests would only exist due to product design decisions, such as failing to ensure that memory is backed up. Purported machine interests are therefore in the best case corporate design failures, and in the worst case deliberate evasion of liability or other legal responsibility for AI products or services that rely on them. For this reason, Bryson et al. (2017) advocate strongly against constructing any law recognizing AI interests.

As mentioned in the Introduction, human-centering in a UN context is now increasingly well-understood to also entail sustainability and concern for biodiversity. This makes sense because human well-being depends on a healthy environment—such as that which our ecosystem tends to stabilize—and living within our resource constraints. Resource conflict can lead to war and abhorrent violations of human interests. Our planetary ecology cannot be as readily redesigned as our artifacts. Similarly, our legal system has evolved from prehistoric times, with deep roots in culture and perhaps even biology (de Waal, 1996). As such, where possible, technology should be adjusted to facilitate law, not the other way around. This is why—in the first national-level AI "soft law"–the UK's second of five principles calls for AI to ". . . be designed and operated as far as is practicable to comply with existing laws and fundamental rights and freedoms, including privacy" (Boden et al., 2011; Bryson, 2017, 2018). This principle was adapted for the second (also of five) principles of the OECD (and G20): "AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards—for example, enabling human intervention where necessary—to ensure a fair and just society" (OECD, 2019).

Both sets of principles also include a principle dedicated to transparency. The fourth British principle insists that AI systems "should not be designed in a deceptive way to exploit vulnerable users; instead, their machine nature should be transparent." The OECD/G20 somewhat softened the language concerning exploitation, instead requiring not only transparency, but "responsible disclosure," and that users know that they can "challenge outcomes" of a system. Such recommendations and soft law have not proved adequate to date. Even widespread and horrific miscarriages of justice involving automated decisions have proven at least in some cases extremely difficult to challenge, being addressed

only after large-scale human suffering including lives lost to suicide and decades in jail (Wallis, 2021; Peeters and Widlak, 2023).

The EU has two pieces of legislation in place that address such problems already: the GDPR–fully in force since 2018–and the DSA, which began coming into force in 2023. The vast majority of commercial AI is best understood as an extension of the corporation that provides it, sometimes even at no explicit financial cost to the user. Our homes, laptops, and pockets contain microphones and cameras, the eyes and ears of corporations and sometimes of governments. Even in countries like the US, where the direct collection of data by the government is prohibited, the government may either purchase (Pasquale, 2015) or steal (Bauman et al., 2014) such data. The EU's GDPR recognizes that the relationship between personal data and the referenced persons is analogous to the relationship between air space and nations: new weapons technology makes its defense essential to security. Privacy is not 'only' essential for human well-being, personal growth, and a robust and creative society (Cohen, 2013; Bryson, 2020). Rather, personal data must be defended also because otherwise foreign and commercial agencies have undue access to and even potentially some control over what ought to be sovereign—the behavior of citizens and residents.

The GDPR addresses Weizenbaum-like concerns by defending privacy, but also by reifying and requiring explicit consent, and further by insisting on transparency about how data is collected and processed. EU citizens have the right to correct mistaken data, as well as the right to review any decisions made about themselves as a data subject in an "entirely automated" way. The GDPR also first demonstrated to the world the EU's capacity to govern and protect its residents from harm from foreign commercial entities. Although entities like Microsoft and Google attempted to disrupt the GDPR, threatening to withdraw their services from the EU, they ultimately preferred access to the 450,000,000 relatively wealthy individuals in the EEA, and have at least approximately complied (Bradford, 2020).

The GDPR though has not proven sufficient in itself to ensure EU citizens and residents are not being manipulated through AI. This has led to the DSA, and its provisions proactively obliging corporations to demonstrate a lack of harms created by their services. The DSA is designed specifically to handle the profiling of users, the targeting of advertising, and the making of recommendations more generally. In other words, we should be able to understand any individual customization of advertisements, social media posts, or search results. It would be impossible for the EU to play "cops and robbers," chasing down and inspecting every part of AI business processes. But what the Union does do is mandate a set of business practices that can be made subject to occasional inspection, not only after events that prompt calls for investigation but also proactively. For example, the DSA encourages corporations to consider and address the risks their services generate, leaving the EU to just

"check the work." The DSA also includes a series of reporting requirements, for example concerning content moderation practices, to ensure that these are compliant with EU law. Governance is a collaborative process. It is in the interest of everyone that regulation is successful–meaning the host society is secure and productive. It is also in the interest of all parties that commercially provided services are resilient, useful, and safe. Hopefully, experience of the benefits of the DSA will lead global organizations to advocate for similar laws in other jurisdictions, where they might otherwise have to compete against less ethical local opponents. This is a critical part of the "Brussels Effect" described by Bradford (2020).

Compared to the GDPR and the DSA, the AIA is almost an afterthought. I sometimes think it was designed as a decoy so that the Digital Services and Markets Acts—the DMA is discussed below—could be brought into force relatively unencumbered by lobbying. In my opinion, the AIA achieves only three interesting things:

\ The AIA finally clarifies that digital products are products and within the remit of product law. That is, corporations are required to perform due diligence, to avoid established bad practices, and to emulate best practices. Product law is a simple solution to the supposed problem of how to keep law governing complex products up to date. It is the sector that establishes due diligence and best and worst practice, though admittedly in cooperation with justice departments. Corporate competitors do not need to worry about a "race to the bottom". They can establish good practice and publish it, obliging their sector to improve with them. For those systems the AIA considers "high risk" (that is, likely to be used to make decisions that alter the course of human lives–concerning, for example, education, healthcare, or access to financial instruments), it also mandates the sorts of record keeping that need to be stored such that product liability can be more easily defended and enforced.

\ The AIA also determines which AI services are considered altogether incompatible with the EU's emphasis on human or fundamental rights. Generally, this again concerns privacy. For example, there is to be no database maintaining records of the location of every human being or their "social credit score." Nor should there be a means of localizing any individual arbitrarily, even if there may be surveillance for specific, named individuals, such as terrorism suspects or missing children.

\ Finally, the AIA has only one demand for all AI in the EU, namely, that it must be identified as such. No one in the EU should ever mistakenly believe that they are collaborating with a human when they are really interacting with an artifact.

4 Peace, Equity, and Enforcement: Conclusions

Human justice only has the capacity to hold adult humans to account; its penalties only persuade living social organisms that can understand its language (Bryson et al., 2017). As such, having "value-aligned" AI (van den Hoven, 2007; van Wynsberghe, 2013) can only imply that the technology expresses not its own values, but the mutable values of those who own and operate it. To ensure those owners and operators comply with human interests (including keeping up with changing mores), we have the law. However, can laws be sufficient, given the power of the companies producing some—but nowhere near most (Bryson and Malikova, 2021)—AI products? I am persuaded by political philosophy—for example, the arguments of Gowder (2016) and Wu (2018)—which suggests that justice requires enough equity that obligations can be enforced. Handling the transnational infrastructure and public goods underlying large-platform AI is an enormous legal and diplomatic challenge that we will need to surmount if we are going to solve sustainability and limit warfare while defending freedom of thought.

Despite our progress against extreme poverty, we are presently experiencing grotesque levels of elite inequality such as we have not seen since the time of the First World War. Eventually, following that and another world war and an intervening global financial crisis of a scale far beyond the 2008 one, we came to do a decent job of addressing the situation. We achieved a long period of relative political-economic stability following the Bretton Woods agreement, due in part to increasing justice through equitable participation (Fraser, 2006; James, 2017) and in part to enforcing antitrust laws (Wu, 2018). More recently, not only have we succeeded in widespread vaccination in response to the COVID-19 pandemic but during that event we also reduced the influence of populism globally, with the exception of the US (Foa et al., 2022).

The US is not adequately enforcing one of its own innovations for maintaining democracy: antitrust law. This is part of the reason the EU has had to be bold in rising to the challenge of regulating a technology that stems more from the US than the rest of the world combined (Bryson and Malikova, 2021). It is also the purpose of the final piece of EU legislation I want to mention here, the DMA. I was originally concerned about why the EU was creating an alternative mechanism for ensuring competition law rather than strengthening support for its existing Directorate General of Competition. But the DMA is actually a very interesting piece of legislation. It allows for more agile enforcement than US law or even previous EU laws. Companies that behave anticompetitively can become subject to stronger sanctioning, eventually leading to their disaggregation. But equally, companies can become subject to weakening enforcement as they find ways to transparently demonstrate their trustworthiness and compliance. This is the legislation of a new age, one that embraces the potential for ICT to increase justice, agility, and cooperation between corporations

and their regulators. Again, the goal of regulation is to produce public goods that will strengthen a society as a whole. This must include the companies that produce its wealth and contribute to its residents' flourishing.

Ensuring the will and capital to enforce the EU's new digital legislation will be an ongoing challenge, one everyone should hope the EU is up to. The drain on resources represented by Russia's wars of aggression against not only Ukraine but also with it the ecosystem is obviously an enormous challenge for the EU and many other nations–particularly, of course, Ukraine. Nevertheless, the world is literally and quite explicitly watching to see what the EU can achieve with its Digital Services and Digital Markets acts. In the longer term, if the EU (or any other power) proves successful at regulating AI—including in making its "machine nature" adequately transparent to not infringe on human relationships and individual well-being—we can all be grateful. Further, we can hope that all nations will find ways to update their governance such that they, too, can defend and treasure the human experience.

References

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, 8(2), 121–144.

Boden, M., Bryson, J., Caldwell, D., Dautenhahn, K., Edwards, L., Kember, S., ... Winfield, A. (2011). *Principles of robotics*. The United Kingdom's Engineering and Physical Sciences Research Council (EPSRC).

Bradford, A. H. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bradford, A. H. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bryson, J. J. (2017). The meaning of the EPSRC Principles of Robotics. *Connection Science*, 29(2), 130–136.

Bryson, J. J. (2018). Patiency is not a virtue: The design of intelligent systems and systems of ethics. *Ethics and Information Technology*, 20(1), 15–26.

Bryson, J. J. (2020). The artificial intelligence of ethics of AI: An introductory overview. In M. D. Dubber, F. Pasquale, & S. Das (Eds.), *The Oxford Handbook of Ethics of AI* (Chapter 1, pp. 3–25). Oxford University Press.

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, 25(3), 273–291.

Bryson, J. J., & Malikova, H. (2021). Is there an AI Cold War? *Global Perspectives*, 2(1), 24803.

Cohen, J. E. (2013). What privacy is for. *Harvard Law Review*, 126, 1904–1933.

DataReportal, We Are Social, & Meltwater. (2023). Worldwide internet user penetration from 2014 to October 2023. *Statista*. https://www.statista.com/statistics/325706/global-internet-user-penetration/

de Waal, F. B. M. (1996). *Good natured: The origins of right and wrong in humans and other animals*. Harvard University Press.

Dorfs, W., & Bryson, J. J. (2024). *Global artificial intelligence competition: Examining current state and drivers*. In preparation.

Foa, R. S., Romero-Vidal, X., Klassen, A. J., Concha, J. F., Quednau, M., & Fenner, L. S. (2022). *The great reset: Public opinion, populism, and the pandemic* [Technical report]. Centre for the Future of Democracy, Cambridge University, Cambridge, UK.

Fraser, N. (2006). Reframing justice in a globalizing world. In J. Goodman & P. James (Eds.), *Nationalism and global solidarities* (pp. 178–196). Routledge.

Gibler, D. M., & Owsiak, A. P. (2018). Democracy and the settlement of international borders, 1919 to 2001. *Journal of Conflict Resolution*, 62(9), 1847–1875.

Gowder, P. (2016). *The rule of law in the real world*. Cambridge University Press.

Hanson, P. (2014). *The rise and fall of the the soviet economy: An economic history of the USSR 1945-1991*. Routledge.

James, H. (2017). Bretton Woods to Brexit: The global economic cooperation that has held sway since the end of World War II is challenged by new political forces. *Finance & Development*, 54(3), A002.

Miller, H. L. (1962). On the "Chicago school of economics." *Journal of Political Economy*, 70(1), 64–69.

OECD. (2019). Recommendation of the council on artificial intelligence. Technical Report OECD/LEGAL/0449, *Organisation for Economic Co-operation and Development (OECD) Legal Instruments*, Paris. [Includes the OECD Principles of AI]

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Patterson, D. E., & Shapiro, C. (2001). Transatlantic divergence in GE/Honeywell: Causes and lessons. *Antitrust*, 16, 18-25.

Peeters, R., & Widlak, A. C. (2023). Administrative exclusion in the infrastructure-level bureaucracy: The case of the Dutch daycare benefits scandal. *Public Administration Review*, 83(4), 863–877.

Pilling, F., Akmal, H. A., Lindley, J., Gradinar, A., & Coulton, P. (2023). Making AI-infused products and services more legible. *Leonardo*, 56(2), 170–176.

Roser, M. (2021). Extreme poverty: How far have we come, and how far do we still have to go? Our World in Data. https://ourworldindata.org/extreme-poverty-in-brief

Roser, M. (2023). Demographic transition: Why is rapid population growth a temporary phenomenon? *Our World in Data*. https://ourworldindata.org/demographic-transition

Rovny, J. (2023). Antidote to backsliding: Ethnic politics and democratic resilience. *American Political Science Review*, 1–19.

Rummel, R. J. (1995). Democracy, power, genocide, and mass murder. *Journal of Conflict Resolution*, 39(1), 3–26.

United Nations. (1948). *Universal Declaration of Human Rights. Technical Report resolution 217 [A] ([III])*, UN General Assembly, Paris.

United Nations General Assembly. (2015). Transforming our world: The 2030 agenda for sustainable development. *Technical Report A/RES/70/1*, United Nations.

Valentino, B. A. (2004). *Final solutions: Mass killing and genocide in the 20th century*. Cornell University Press.

van den Hoven, J. (2007). ICT and value-sensitive design. In P. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.), *The information society: Innovation, legitimacy, ethics and democracy in honor of Professor Jacques Berleur* (pp. 67–72). Springer US.

van Wynsberghe, A. (2013). Designing robots for care: Care centered value-sensitive design. *Science and Engineering Ethics*, 19(2), 407–433.

Wallis, N. (2021). *The great post office scandal: The fight to expose a multi-million pound scandal which put innocent people in jail*. Bath Publishing Limited.

Weizenbaum, J. (1986). Not without us. *ACM Sigcas Computers and Society*, 16(2-3), 2–7.

Wu, T. (2018). The curse of bigness. *Columbia Global Reports*.

Acknowledgement

Thank you to the website projects *Our World in Data* and *Statista*. Thank you to Martin Krzywdzinski for the honor of this invitation and for your patience and persistence. Thank you to Helena Malikova for teaching me a great deal about antitrust and power.