Telecommunications Policy xxx (xxxx) xxx

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

It's just distributed computing: Rethinking AI governance

Milton L. Mueller

Georgia Institute of Technology, School of Public Policy, 685 Cherry St, Atlanta, 30332, GA, USA

A B S T R A C T

What we now lump under the unitary label "artificial intelligence" is not a single technology, but a highly varied set of machine learning applications enabled and supported by a globally ubiquitous system of distributed computing. The paper introduces a 4 part conceptual framework for analyzing the structure of that system, which it labels the digital ecosystem. What we now call "AI" is then shown to be a general functionality of distributed computing. "AI" has been present in primitive forms from the origins of digital computing in the 1950s. Three short case studies show that large-scale machine learning applications have been present in the digital ecosystem ever since the rise of the Internet. and provoked the same public policy concerns that we now associate with "AI." The governance problems of "AI" are really caused by the development of this digital ecosystem, not by LLMs or other recent applications of machine learning. The paper then examines five recent proposals to "govern AI"and maps them to the constituent elements of the digital ecosystem model. This mapping shows that real-world attempts to assert governance authority over AI capabilities requires systemic control of all four elements of the digital ecosystem: data, computing power, networks and software. "Governing AI," in other words, means total control of distributed computing. A better alternative is to focus governance and regulation upon specific applications of machine learning. An application-specific approach to governance allows for a more decentralized, freer and more effective method of solving policy conflicts.

1. Introduction

In March 2023, more than 1000 technology business leaders, researchers and intellectuals signed an open letter urging a moratorium on the development of "artificial intelligence" systems, claiming that it posed "profound risks to society and humanity." Two months later, an open letter signed by more than 350 executives, researchers and engineers claimed that "artificial intelligence" posed a "risk of human extinction" and urged us to make "mitigating that risk a global priority." (Center for AI Safety, 2023).

In response, the world's governments and various global governance institutions leapt forward to meet the alleged threats. The G7 started its "Hiroshima" process (OECD, 2023); the US Congress held hearings[1]; Biden issued a Presidential Executive Order claiming to take "the most sweeping actions ever taken to protect Americans from the potential risks of AI systems" (Biden, 2023). State legislatures in the U.S. introduced around 200 AI-related bills in 2023, and over 400 in 2024. The European Union passed what it claimed was "the world's first comprehensive AI law." (European Parliament, 2023) Canada, the United Kingdom (UK, 2024), India (TRAI, 2023) and China (Sheehan, 2023) have proposed or implemented targeted AI governance or policy frameworks.

"Regulating AI" has become a profession. But what does it mean to regulate AI? What is it, exactly, we are regulating? The evidence suggests that the boom in legislative and regulatory initiatives rests on deeply flawed understandings of what they are trying to govern. As Gasser & Mayer-Schönberger, 2024 put it, we are in a race to regulate before we know what the object or goal of regulation is.

This paper aims to provide a more scientific definition of the object of governance. It argues that what we now lump under the

E-mail address: Milton@gatech.edu.

[1] An oversight hearing to examine artificial intelligence, focusing on principles for regulation. Senate Judiciary Subcommittee on Privacy, Technology, and the Law. July 25, 2023. "Oversight of A.I.: Legislating on Artificial Intelligence," Senate Judiciary Subcommittee on Privacy, Technology, and the Law, September 12, 2023.

https://doi.org/10.1016/j.telpol.2025.102917
Received 2 January 2025; Received in revised form 30 January 2025; Accepted 1 February 2025
0308-5961/© 2025 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

unitary label "artificial intelligence" is not a single technology, but a highly varied set of software applications enabled and supported by a globally ubiquitous digital ecosystem. It is not a new technology but at best an inflection point in computing capabilities that have been developing since the 1960s. From a public policy standpoint, the term "AI" covers applications of machine learning that are so numerous, so diverse, and so embedded in everyday manifestations of networked computing as to render the concept of "AI governance" practically meaningless. This paper argues that we must stop framing the problem as regulating or governing "AI" and instead focus attention on specific problems caused by individual machine learning applications. This shift in perspective clarifies the policy choices we face.

The paper proceeds along the following lines. Part 1 introduces the conceptual framework of the *digital ecosystem* and explains why it needs to be the starting point for discussions of ICT governance. Part 2 shows how "AI" is not a free-standing technology that can be isolated for regulation, but a systemic capability of the digital ecosystem. It identifies both the enormous variety of AI applications and their dependencies on the lower levels of the computing stack. Part 3 consists of three short case studies of machine learning applications that have been present within the digital ecosystem for the past 30 years. It shows how these successful applications depended upon progressive improvements in computing power, data sources, and network scope and speed. Part 4 shows how the gradual rise of Internet- and platform-enabled capabilities provoked the same policy concerns we now associate with "AI" (though without the apocalyptic fears of human extinction). Part 5 evaluates some of the current proposals to "govern AI" and maps them to the constituent elements of the digital ecosystem model proposed in Part 1. This exercise shows that any attempt to assert generic governance authority over all "AI" capability requires systemic interventions across all the components of the digital ecosystem: content, services, applications, hardware and software. "Governing AI," in other words, means governing everything in information and communications technology.

2. The digital ecosystem

The digital ecosystem is a distributed cybernetic system for the production and distribution of communication, information and control capabilities. It is composed of four basic technical components: computing devices, networks, data and software (Fig. 1). Computing devices process and generate information; networks transmit information from one place to another; data is a stored manifestation of the information outputs; and software provides the instructions that organize and control the parts. All four are reliant on digital representations of information. A key feature of this system, often overlooked in discussions of AI governance, is the multiplicity, diversity and autonomous management of its constituent parts. It consists of trillions of computing devices, hundreds of thousands of independently managed but interoperable networks, growing stores of digitized data distributed across a growing number of data centers, and a plethora of software programs, algorithms and models that can come from any of millions of individuals and firms. A more detailed description of each component follows.

2.1. Computing devices

Computing devices are digital information processing capabilities fixed in distinct hardware units. These hardware units take many forms: semiconductor chips, desktop and laptop computers, servers, robots and drones, mobile phones, digital cameras. Semiconductors, also known as integrated circuits (ICs), are the foundation of the computing device component. Electronic circuits inscribed on a small piece of semiconducting material, ICs are "integrated" because the circuit elements are so small, interconnected and closely associated that they must be produced and sold as a single material unit (Cavin et al., 2012). A major driver of our progressive immersion in the digital world has been six decades of reductions in the size and exponential improvement in the speed and capacity of chips (Mack, 2011). This is often called "Moore's Law,"[2] although it is not a law of nature but an inductive extrapolation of gains in the efficiency of production since the 1960s.

2.2. Networks

Networks provide the communication pathways between the nodes where devices, software, and data reside. Networks can be big, capital-intensive multinational telecom businesses, small, household WiFi networks, or anything in between. The contemporary marvel is how digitization made them all potentially interconnected and interoperable. The critical step toward the digitization of networking came with the development of the Internet protocols in the 1980s and their universal adoption in the 1990s. TCP/IP, a nonproprietary packet switching protocol, converged the entire ecosystem on common layer 3 and layer 4 protocols, and on a set of recognized registries for coordinating the assignment of globally unique identifiers for addressing and naming. The World Wide Web (HTTP) protocol supplemented Internet connectivity with a graphical user interface and a naming and linking structure for information resources. It, too, was open-source software and it, too, achieved global adoption. The Internet-Web combo paved the way for digital convergence – the unification of voice, video, text and imaging systems (Yoffie, 1996). It also facilitated the privatization and decentralization of telecommunications networking, fostering a complex network of networks that enabled greater innovation and competition in online services and applications (Greenstein, 2015).

[2] Gordon Moore, the co-founder and former CEO of Intel, projected in 1965 that, given the scaling properties of chip technology, the number of transistors on an IC would double every 2 years for the next 10 years. As it happens, Moore was way off; this rate of progress continued for the next 50 years, and improvements are still happening.

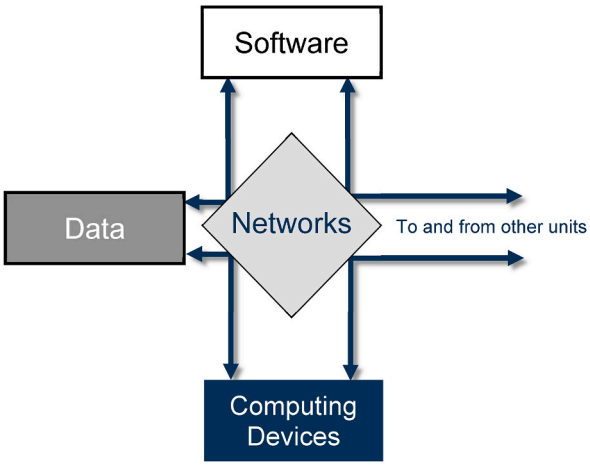


Fig. 1. Diagram of components of the digital ecosystem.

2.3. Data

Digital data is simply a stored record of an interaction with a digital system. Data is not found in nature, nor is it "extracted" from people; it is *generated* by interactions among people, digital devices, networks and services. Every interaction with the digital ecosystem, whether machine-machine or machine-human, generates digital data that can be stored, aggregated, shared, sold, processed and analyzed (Yaqoob, Hashem et al., 2016). The smart phone, because of its close attachment to individual human beings, is the ultimate data generator. Most of the population in nearly every country has one, so it generates data at a scale and level of behavioral granularity that no other communications medium has provided before. Online services and networks also generate vast amounts of data about user identity, traffic, location, transactions and other user and system activity. In short, the digital ecosystem is a gigantic, always-on data generator, and because it captures behavioral and operational patterns, this data becomes a valuable input to applications and services, including those applications that we now group under the term "artificial intelligence."

2.4. Software

Software is a set of instructions instantiated in code that enables humans to control the behavior of devices, data, networks and other software programs. Its key feature is that it exerts control via symbolic methods rather than physical rearrangements of material. Software is virtual, not physical. It replaces physical manipulation with control through signaling. Mahoney (1988) accurately summed up the central place of software in this way: "Between the mathematics that makes the device theoretically possible and the electronics that makes it practically feasible lies the programming that makes it intellectually, economically, and socially useful."

Of the four components of the digital ecosystem, software is the most complex and interesting. Software production is similar in many ways to writing; it is creative output from decentralized sources, and while its distribution may be constrained, there is no central gatekeeping entity controlling its production. Computer scientists who study the Internet often refer to what protocols do "in the wild" (Gopstein et al., 2018; Rouse, 2016). Like a natural ecosystem, code is not always predictable due to the many interactions and interdependencies involved. Like any form of human communication, code can be malicious and deceptive as well as informative and productive. It can be designed to exploit vulnerabilities to transfer control of information systems to an adversary, and, thanks to interoperable networks, these attacks can be conducted remotely from anywhere in the world. Adding to its complexity and diversity, the software environment is constantly under revision; there are updates, patches and many different versions of the "same" programs floating about.[3] Unanticipated compatibility and security problems are an inherent part of the distributed, open ecosystem.

2.5. Systems and ecosystems

The breakdown of the digital ecosystem into these four components is analytically useful. From an economic standpoint, we can readily distinguish between markets for devices, data, software and networking services, and we can see how any information-communications product or service combines these elements in their design and supply chain. From a technical standpoint, it allows us to see how specific manifestations of computing, such as platforms or machine learning applications, can be broken down into combinations of these components. From a political or policy standpoint, it helps us to see how public control of each component

[3] While computer scientists panicked about AI often warn us that we don't know why a large language model arrives at the answers it does (Heaven, 2024), the same could be said for almost any widely used, complex program released into cyberspace, as the massive outage caused by an update to CrowdStrike's cybersecurity application revealed recently.

requires different regulatory or governance tools (see Part 5).

The term "ecosystem" originated in biological studies, where it connotes systemic interdependencies among different lifeforms interacting with each other in a specific environment (Bogers et al., 2019; Blew, 1996).[4] While the digital environment is human made, once produced and put into operation it is external to humans and not fully under any individual's or organization's control. The actors producing and using digital information systems are autonomous and multifarious; the information systems within it are competitive and complementary, open and bordered, independent and interdependent. In that respect, it is like a biological ecosystem.

The digital ecosystem approach provides a richer basis for analysis of ICT-related governance problems. Other labels with which the author is familiar seem inadequate by comparison. "Digital economy" emphasizes only online commerce for priced goods and services and does not capture the distinctive ways in which institutions adapt to technological change. Theories of "platforms" and "platformization" (Van Dijck, Poell, & De Waal, 2018; Nieborg, Poel & van Dijk, 2022) highlight intermediary platforms, an important outgrowth of the digital ecosystem, but focus only on large-scale aggregation of online capabilities into multi-sided markets. The development and viability of platforms, however – like machine learning applications – depend on the broader digital ecosystem; i.e., on the long tail of ubiquitous devices, accessible and affordable networks, the generation and commodification of digitized data, and constant innovations in software.

The most important rationale for an ecosystem approach is that it highlights processes of evolution, co-evolution, and selection that lead to survival or extinction, growth or decline, of the socio-technical systems built around digital technologies, providing a framework for addressing the dynamics of distributed control, evolving capabilities and decentralized decision-making. Taken together, this approach situates digital technologies in *political economy*, highlighting technological change and its dependence on markets, business operations, capital flows, legal, regulatory and political constraints, and conflict, competition and cooperation among users, businesses and the world's governments.

3. "AI" as a product of the digital ecosystem

The conceptual framework described above makes possible a more precise definition of the object of governance. What we now call "AI" is actually a large, diverse set of *machine learning applications*. Machine learning applications use feedback loops from digital data (and humans) to train complex software models (an algorithm or some derivative of a neural network) to recognize inputs and produce or predict desired outputs; they are configurations of innovative software architectures, powerful processors, high-speed networks and abundant sources of digitized data.

The only thing all machine learning applications have in common is their dependence on the four elements of the digital ecosystem. The data that trains the model shapes the neural network; i.e., the structures and weights of the model are statistical properties of the data and reinforcement process; hence, one cannot define a neural network without including the data and feedback used to train it. Machine learning applications also require large concentrations of computing power, often attained by networking powerful chips into clusters.[5] The power of models is a function of the number of adjustable values within the software, the size of its training data, and the computing power to which it is connected (Ma, Grandi, et al., 2024).

Going forward, this paper will use the term "machine learning applications" – not "AI" – to denote this broader and varied set of capabilities. Calling it "AI" gives it a false homogeneity and contributes to the fallacy that "AI" is a unitary thing that can be "regulated" or governed.

3.1. Scientific foundations

Three colossal intellectual achievements came together in the 1940s to provide the scientific foundations for this capability: information theory, cybernetics and the stored-program computer. Each achievement is associated with mathematicians: Alan Turing (1947), John von Neumann (1945), Claude Shannon (1948; Gappmair, 1999), and Norbert Wiener (1950). Put Information theory, cybernetics and stored program computing together, and the developmental path towards what we now call AI applications is clear.

Turing's seminal contribution was to substitute a machine-executable algorithm for the computations done by human beings. Nevertheless, he aimed at more than merely automating static mathematical calculations. Turing said in 1947, "What we want is a machine that can learn from experience [and] the possibility of letting the machine alter its own instructions provides the mechanism for this" (Copeland, 2020; Turing, 1947 p. 393). Wiener wrote in 1950 that cybernetics and computing have made it possible to move

[4] The application of the ecosystem metaphor to socio-technical phenomena became popular among business analysts after Moore (1993) used it to describe the interaction of technologies, markets, and industrial organization. In Moore's words, "In a business ecosystem, companies coevolve capabilities around a new innovation: they work cooperatively and competitively to support new products, satisfy customer needs, and eventually incorporate the next round of innovations." See also Arenal et al. (2020) for a discussion of an "innovation ecosystem."

[5] For example, in December 2024 Amazon's cloud computing platform AWS announced a new AI server made up of 64 of its own Trainium chips. It combines four servers with 16 Trainium chips to train and run Anthropic's future AI models. The linkage enables 83.2 petaflops of compute and involves a proprietary networking technology among the servers.

from "the sporadic design of individual automatic mechanisms" to "a general policy for the construction of automatic mechanisms of the most varied type." (Wiener, 1950) Drawing on Turing's mathematical proof of computability, von Neumann (1945) worked out an architecture that could translate Turing's theory into a real-world machine that could follow a recorded program.[6] The socio-economic significance of stored program computing was that it substituted software instructions for costly and slow hardware re-configurations, setting in motion the decades-long shift from physical-mechanical control to control by human instructions instantiated in software.

Notably, these key figures in the foundation of the digital ecosystem were never comfortable with the term "artificial intelligence."[7] Von Neumann's preferred term was "automata." (von Neumann, 1966). Wiener preferred to speak of *cybernetic systems* and to analyze the way biological and human-made systems use feedback and communication to monitor and regulate their activities. In 1955 Claude Shannon opposed using the term "artificial intelligence" to describe the emerging field of computing; following von Neumann, he suggested that it be called *Automata Studies*. (Rajamaran, 2014).

Anything we think of as being challenging about "artificial intelligence" was already present, in embryonic form, in the 1950s. Time Magazine in 1950 asked whether computers would take over the management of people and rob them of their autonomy (Klein, 2015). Wiener and Shannon designed small robots and Wiener made sweeping (later, falsified) predictions about the massive levels of unemployment he thought would be caused by automation in manufacturing (Wiener, 1950). There were Cold War efforts to use computers to translate languages (Delipetrev, Tsinaraki, & Kostic, 2020) and to plan the economy (Lopes & Neder, 2017).[8] Of course, the tools of the early decades were still primitive, and effective applications of digital technology to real world problems were gradual.

3.2. Emerging or emerged?

We can now reinterpret the governance problems raised by machine learning applications. What we call artificial intelligence is not a "new technology" but the realization of the control and automation potential of a socially extended digital ecosystem. If one wants to call it an "emerging technology" one must recognize that it has been "emerging" since the origins of computing; i.e., for 80 years. Recent technical innovations such as transformers and LLMs played an important role in advancing those capabilities, but the promise of machine learning and intelligent applications was present in computing from the very beginning, and its practical applications evolved gradually over time. Today's LLMs, which seem like a radical new technology, are actually based on neural network or connectionist models that were first theorized in the 1940s (McCulloch and Pitts, 1943) and first implemented in the 1960s (Rosenblatt, 1961). These early neural networks, however, suffered from the weaker processing power of chips, constraints on networking and the primitive design of the software instructions (Minsky and Papert, 1969; Pollack, 1989). The evolution of machine learning required building more powerful chips, expanding the coverage and bandwidth of networks, making digital devices smaller and cheaper, building up stores of digitized data, and clever software innovations. In other words, "AI's" history is intricately tied to, and insuperable from, the techno-economic evolution of the digital ecosystem.

Fig. 2 shows the correlation between various measures of the growth of the digital ecosystem, and the progress of machine learning applications.[9] With available bandwidth expanding at 50% per year for the past 4 decades (Nielsen, 2023), the number of transistors (logic gates) on a single chip growing from 2300 in 1971 to 208,000,000,000 in 2024, and the amount of digitized data available growing at even faster rates (Hilbert, 2015), the gradual emergence of more powerful machine learning applications follows. The more powerful, sophisticated and "lifelike" the AI application, the more processing power, connectivity, data resources and advanced software architectures it demands.

4. Case studies in the evolution of machine learning

Three cases illustrate the dependence of machine learning capabilities on general growth in the capabilities and needs of the digital ecosystem. The cases cited here are 1) cybersecurity applications, 2) search applications and 3) the collection and sharing of digitized data.

4.1. Cybersecurity

Email, one of the killer apps of networked computers, led to massive increases in the scale of one-to-one messaging. Along with that

[6] Before the Von Neumann architecture, changing the types of calculations a computer could do required reengineering and rewiring the hardware and could take weeks. VN and others working at the Univ. of Pennsylvania's Moore School designed a digital computer that could solve complex mathematical problems but could be efficiently reconfigured to store and execute different programs. This made what had once been huge, expensive machines designed to solve a single problem into general-purpose computers.

[7] The term "artificial intelligence" can be tracked to a 1955 proposal from McCarthy and Minsky seeking funding for the seminal Dartmouth conference of computer scientists. (McCarthy, Minsky, & Shannon, 1955) According to Brockman (2019), they labelled the subject "artificial intelligence" to avoid calling it a conference on cybernetics, which would have necessitated inviting Norbert Wiener – and McCarthy and Minsky found Wiener insufferable and did not want him to be at the meeting. See Dick (2019).

[8] The only – very interesting - exception was the idea of digitized money, which doesn't appear until the mid-1970s.

[9] Sources for this data: 1) Internet users is the "number of people using the Internet" in the ITU/World Bank statistics. 2) Chips is the largest number of transistors on a single chip in a given year, according to the Wikipedia entry, "Transistor Count." 3) Bandwidth is a very rough estimate of total capacity in terrrabytes per second drawn from both Nielsen and Telegeography. 4) Data storage estimate is based on Hilbert, 2015.

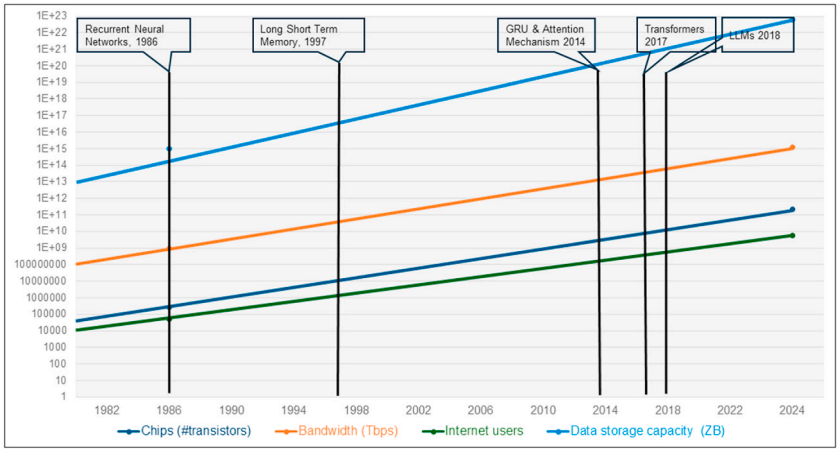


Fig. 2. Growth in the capacity of digital ecosystem components correlated in time with developments in machine learning software models.

growth came unsolicited bulk email (UBE), also known as spam. As the scale of messaging exceeded the ability of users and service providers to manually sort it, spam fighters in the late 1990s developed algorithms to detect and block UBE. (Delany et al., 2005; Drucker, Wu, & Vapnik, 1999). These were simple sets of rules for recognizing UBE messages. As information service providers acquired more processing power, they were able to sort incoming emails into categories based on these patterns. Email providers, particularly ones affiliated with large-scale platforms like Microsoft or Google, would use this method to keep junk mail out of their users' inboxes. Dealing as it does with semantics and context, spam sorting is still beset with false positives and false negatives (a problem that afflicts social media content moderation algorithms as well). Still, it involves the same capabilities as other machine learning applications: recognition of patterns in digital data based on training on large quantities of data, and triggering actions based on recognition.

In related developments, computer science researchers and network equipment vendors taught network appliances to inspect high-speed packet streams to recognize the signatures of malware as it passed through (Kolter & Maloof, 2004). Known as deep packet inspection, these enhanced recognition capabilities were soon able to trigger automated responses by Intrusion Detection and Prevention Systems.

These developments took place two decades before "AI" was recognized as an "emerging technology." Today, many endpoint cybersecurity applications use more complex machine learning models based on the analysis of vast amounts of data to identify patterns or anomalies that indicate malicious activity, and respond to these threats in real time, even when they are from unknown attackers.

4.2. Search

The growth of the Internet and the World Wide Web after 1992 meant that the number of Web pages exceeded the ability of humans to find the ones they wanted. This led to the development of automated web scanners that came to be called – appropriately enough – robots (Koster, 1994). The first known web robot, a Perl-based "WWW Wanderer" developed by Matthew Gray, generated an index of the web to measure its size.[10] The first search engines, Lycos (1994) and Alta Vista (1995), relied on robotic "crawlers" to identify and categorize web pages and send data back to a source. Google's category-killing innovation, PageRank (Page, Brin, et al., 1998), incorporated more intelligence into its crawler by collecting data on incoming and outgoing URL links to a web page, forming a graph that could perform automatic calculations of a web page's centrality in a network to guide recommendations (Rieder, 2012).

Intensifying the cybernetic process of learning and control through feedback, Google began to use search queries to train its search engine to do a better job. Tracking what users clicked on taught their systems which search results users thought best matched their intent, a feedback loop that progressively increased the precision and usefulness of its recommendations. After a while, Google's statistical models were able to anticipate search queries; the web interface instantly appended additional search terms to the user's typed-in query based on probabilities derived from massive amounts of data about users' queries. Aggregated user query and online behavior data became economically valuable when used to match users to advertisers. AdTech executed instant auctions for ad space on a user's Web browser. These, too, were "AI" (i.e., machine learning applications).

4.3. Data

One of the main weaknesses of earlier machine learning models was the paucity of digitized data. In 2006, computer scientists at

[10] Gray, Matthew. "Internet Growth and Statistics: Credit and Background". Retrieved February 3, 2014.

Stanford University hypothesized that more data will produce better predictive models. (Li, Fergus and Persona, 2006) This work took for granted something that the AI researchers of the 1980s and early 1990s could not: the presence of a global Internet that facilitated the generation of data and broadened its accessibility. The growth of bandwidth and the extension of connectivity to a growing portion of the world's population meant that users were sharing an endless torrent of digitized text, images, videos, and records of live interactions, and these Internet-generated datasets could be collected and shared with unprecedented ease. ImageNet, first published in 2009, contained 3.2 million humanly labelled images sorted into a human-constructed taxonomy. (Imagenet; Deng et al., 2009). The ability to make this data available to other researchers via the Internet accelerated progress in image recognition. In 2012, Google researchers built a neural network of 16,000 computer processors with one billion connections and used 10 million unlabeled images from YouTube videos to train it to recognize images of cats (Dean, Corrado et al., 2012). Here again, progress hinged on the lower costs and greater power of semiconductors, on high-speed networking, and on the ability to collect and share Internet-generated data.

As the number of digitized books and texts piled up, and platforms availed themselves of user feedback via networked devices, language translation programs became progressively better. The improved Natural Language Processing capability fueled the ability of chatbots to respond to queries in complete sentences and paragraphs. The progressive digitization of images and the lower price and ubiquity of image capture devices allowed programs to analyze and quantify human faces, leading to a wide range of facial recognition applications, as well as an enhanced ability to create convincing simulations of real or imagined people, objects and events.

These and many other machine-learning applications were taking place under our noses for three decades before the great AI panic of 2023.

5. Policy concerns

If machine-learning applications have been a growing presence in the digital ecosystem for the past 30 years, one would expect to find in those years the same policy and regulation problems now attributed to the rise of "AI." And this expectation is confirmed. With only one exception (addressed below) all of today's "AI" governance issues were anticipated, if not duplicated, by policy conflicts associated with the rise of the Internet. Misinformation, bias, fraud, cybersecurity, copyright, open vs closed source software, all preceded what we now think of as "AI."

In the 1990s, a chorus of voices claimed the Internet was spreading misinformation (Hernon, 1995; Ebbinghouse, 2000). Artists denounced image manipulation software as "digital robbery" and debated watermarks and other indicators of provenance (Garofalakis, Kappos et al., 1998). Search engines were accused of spreading misinformation, disinformation and fraud (Sheldon, 2010). Like AI and its training data sets, search engines were accused of biased outputs (Goldman, 2005; Mowshowitz & Kawaguchi, 2005). Platform recommendation algorithms produced outputs denounced as illegal (Liang & Mackey, 2009), immoral (Bouhnik & Deshen, 2013; Wright & Randall, 2012), fattening (Tamtomo & Cilmiaty, 2019), harmful to children (Richards, Caldwell, & Go, 2015; Strasburger et al., 2010), piratical (Padawer, 2003; Jeweler, 2005; Xalabarder, 2012), or violations of privacy (Zimmer, 2008; Korolova, 2010; Mayer-Schoenberger, 2011). To anyone with a historical memory that goes back more than 15 years, accusations about the dangers of generative AI are familiar refrains.

By the same token, political outrage about the influence of algorithms is incentivizing more, not less, reliance on machine learning. Apparently, scalable solutions to the problems of the digital ecosystem are more likely to come from enhancing automated, intelligent applications than by regulating or banning them. Faced with lawsuits or complaints about public sharing of copyrighted digital materials, for example, platforms developed registries of copyrighted materials and reduced uploaded content to machine-readable "fingerprints" that could be compared against that registry. The Content ID technology alerted the copyright owners when registered materials were matched by the content uploaded on servers.[11] (Edwards, 2018) Alarm about undesirable content, such as child sexual materials or hate speech, fueled the use of algorithms to take more responsibility for recognizing and controlling what people see and do online. Algorithms are also used to detect illegal or fraudulent forms of exchange on platforms or in financial transactions. Fear of machine-generated disinformation has led to the adoption of machine learning-based detection tools for content provenance (Kuerbis and Han, 2024). Plagiaristic uses of chatbots in the classroom are leading to the development of tools for detecting the output of generative chatbots, and they all use … "AI." This is because machine learning applications are technologies of regulation and control that can work at Internet scale and speed.

This is not to imply that technical evolution alone will solve all social problems; there is clearly a role for law and regulation. The existence of laws protecting copyright and the threat of litigation, for example, provided an incentive for platforms to deploy automated content recognition and alert technologies. Effective governance, however, occurred not by regulating some generic capability of the digital ecosystem ("AI"), but by legally recognizing certain rights and imposing constraints and liabilities on specific actors or behaviors for violating those rights. To use another example, machine learning capabilities can both help and hinder cybersecurity. We cannot improve cybersecurity by imposing ex ante regulations on the production of machine learning applications, because such regulations would constrain all kinds of legitimate and beneficial activities, and still allow criminals to find ways to use enhanced capabilities for bad purposes. We can better protect information systems from cybersecurity threats by letting private actors develop

[11] In the mid-2000s ISPs and online service providers such as Google claimed that it would be either technically impossible or prohibitively costly to prevent people from uploading copyrighted material to YouTube. By 2012, however, YouTube had implemented its Content ID system, which gave it the ability to detect and manage copyrighted videos. Participating content owners provided YouTube with audio or video files that were scanned and transformed into a smaller unique "fingerprint." YouTube then scanned every uploaded video to see if it matched a fingerprint, and if it did, it was able to automatically notify the owner and ask whether they wanted it blocked, allowed, tracked or monetized.

and use automated tools to protect themselves, and by encouraging governments to prosecute illegal forms of unauthorized access to information systems, whether they use machine learning or not.

In sum, it makes no sense to propose institutional changes or regulations targeting "AI" generically. Each application raises different policy issues. The use of facial recognition by police departments raises completely different policy issues than the use of machine learning for chatbots or health-monitoring devices. Policy and regulation will have to respond differently to different applications in different contexts, because the governance problems posed by each application will differ.

Are there no novel policy problems posed by AI? In the author's judgment, none of the problems posed by AI are truly novel, except for the claim that AI poses a threat of human extinction, a fear which has been debunked (Harisch, 2023; Mueller, 2024). All other problems have been confronted before in Internet, data, social media, and software governance.

6. Mapping "AI governance"

If, as evidenced above, machine learning applications are an endogenous capability of a socially extended digital ecosystem, the question, *how shall we govern AI?* is a deeply misleading one. There is no single object of governance, no isolatable new technology like the atomic bomb to "govern." There is, rather, a hugely diverse collection of machine learning applications serving different purposes.

Nevertheless, in many policymaking circles the answer to the first question, *how shall we govern AI?* bleeds inexorably into the question, *how shall we govern the entire digital ecosystem?* That is, proponents of AI regulation, often unwittingly, are trying to use the tail of machine learning applications to wag the dog of *all* information and communication technology. This mistake encourages policies that are at best unrealistic, at worst disproportionate or dangerously authoritarian.

Many descriptive-comparative papers have been published about the growing number of attempts to "govern" or "regulate" AI. (Corrêa et al., 2023; Dixon, 2023; Roberts et al., 2023; Sheehan, 2023; Zhang, 2024). These efforts, however, often generate more noise than signal. We can shed more light by mapping prominent "AI governance" efforts onto the digital ecosystem framework. Table 1 considers five such efforts: the AI "moratorium; " the "control compute" proposal; the "control the cloud" proposal; the EU AI Act; and China's AI regulations. We see that in all cases, any attempt to regulate or control "AI" as a general capability requires systemic control of other digital ecosystem components.

6.1. The moratorium

One of the most publicized global governance proposals was the Future of Life Institute's March 2023 call for a six-month moratorium in AI development. It was based on fears that out-of-control AI could destroy the world, and that we could be weeks or months away from such an eventuality. Signed by over 33,000 people, including technology entrepreneurs Elon Musk and Steve Wozniak, the proposal for a "pause" stated:

> **We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4**. This pause should be public and verifiable, and include all key actors. If such a pause cannot be enacted quickly, governments should step in and institute a moratorium. (Future of Life Institute, 2023)

The authors of this proposal clearly did not understand the embeddedness of "AI" in the wider digital ecosystem, nor did they grasp the institutional requirements and collective action problems associated with "pausing" technological development. A moratorium would require a very clear operational definition of an "AI lab" and "the training of AI systems" as well as a precise metric to decide whether an application was "more powerful than GPT-4." Monitoring and auditing procedures would have to be put into place to verify the presence or absence of such activities or powers anywhere in the world. Arriving at a consensual agreement among "all key actors" about these definitions and procedures would involve complex negotiations and binding commitments. The proposal does not specify what institution would facilitate this process. It does, however, call for "governments" to step in if necessary.

Yet an effective moratorium would require *every* government and *every* firm in the computer industry to abide by it. And not all businesses or governments really want to pause. It is unlikely that the U.S., Israel, China, the European Union, Russia and India would trust each other enough to stop unilaterally. Nor would they be eager to expose their advanced software and hardware capabilities to inspection by other states or foreign businesses. Given the (alleged) military and business advantages of being the leader in AI technology, each state and business would have a strong incentive to defect from a moratorium. Even if noncompliance could be detected reliably, there would be no way for complying governments to enforce the pause agreement upon recalcitrant governments of sufficient size and power. "Pause AI" just does not work. But if it did, it would involve systematic surveillance and control of ICT capabilities worldwide.

6.2. Controlling "compute"

Advocates of AI governance quickly realized that the search for leverage over AI development requires leverage over other parts of the digital ecosystem. This led to a search for control points that can affect the ecosystem as a whole. In early 2024, a 78-page white paper issued by Open AI and fifteen research centers and universities in the U.S., Canada and the UK thought they had found the solution to this problem (Sastry, Heim, et al., 2024). The paper argued that society could control AI by controlling computer processing power.

The paper "Computing Power and the Governance of AI" was authored by many of the same people and institutes who had earlier proposed a moratorium. Their argument:

Table 1
Governing AI? Mapping proposals to the digital ecosystem targeted system component.

Control Method	Computing Devices	Networking	Data	Software applications & models
Moratorium			Stop training	Stop building
Regulate Compute	Control access to semiconductors	Reporting requirements	Reporting requirements	Reporting requirements
Regulate Cloud	Control access to AI via cloud providers	Export controls on CSPs	Restrictions and reporting	Monitor via CSPs
EU AI Act		Block noncompliant applications	Data governance rules	Bans, ex ante risk classifications
China AI Regulations		Block external applications	Data accuracy; data localization	Regulate and label outputs; Register algorithms

> "Relative to other key inputs to AI (data and algorithms), AI-relevant compute is a particularly effective point of intervention: it is detectable, excludable, and quantifiable, and is produced via an extremely concentrated supply chain." (Sastry, Heim, et al., 2024)

To govern AI, in other words, these scientists want to subject the core of all ICT systems and applications – the information processing power of the semiconductor – to hierarchical, centrally-controlled allocation on a global basis. The authors recognize that effective intervention in AI development is only feasible insofar as there is a chokepoint in the digital ecosystem. Controlling "compute," however, would also require reporting requirements and comprehensive surveillance of the rest of the digital ecosystem to ascertain who is using how much. The proposal does not tell us which central authority would take on this task.

Unlike the pause proposal, the computer scientists responsible for this proposal made some attempt to think about what kind of governance institutions and procedures would be needed to implement their idea. They were even forced to admit that "naïve or poorly scoped approaches to compute governance carry significant risks in areas like privacy, economic impacts, and centralization of power." They imply that the need for regulation of AI is so dire, however, that these risks are worth taking.

Nevertheless, controlling compute in isolation also does not work. To monitor who is using computing power, regulators need to enlist networking intermediaries (cloud service providers - CSPs) and software developers, two other components of the digital ecosystem. The paper calls for mandatory reporting of "large-scale training compute usage from cloud providers and AI developers." It also calls for "an international AI chip registry." Who would the CSPs report to? Who would enforce reporting requirements upon all the world's cloud providers and software developers? Who would run the chip registry and require chip producers to register in it? The paper does not answer any of these questions.[12]

Another unanswered question is what this unnamed global central authority will *do* with its control of compute. If the authority has the power to gate-keep the use of computing power, how will the decision makers know in advance, before deployment, which demands for computing power will produce bad things and which will produce good things? Will the rival great powers (the U.S., China, Russia) trust any external institution to control their access to such a strategic technology? This kind of oversight typifies many proposals for public interest regulation, which rely on an assumption that the holder of centralized authority will be neutral, benign, possess perfect knowledge of the future, and have no self-interest in the outcome. This god-like entity will never erroneously stifle innovative new uses and will never be influenced by the lobbying by specific governments, incumbents or competitors seeking protection; it will always make error-free corrections of market failures. But this is not the world we live in.

6.3. *Controlling clouds*

The existing US sanctions on Chinese access to semiconductors provides a more realistic sense of what globally centralized power over compute would look like. But the very fact that only one nation-state is likely to hold that power means that its exercise would further the interests of that state alone; rival nation-states will constantly seek to evade or innovate around it. If achieving "AI supremacy" is the goal (Schmidt, Work, et al., 2019), then there are powerful incentives for other governments to promote AI development domestically while regulating its dissemination and use in ways designed to keep its military and economic benefits exclusive to the government of origin.

In keeping with this pattern, Washington DC think tanks overtly interested in promoting US power at the expense of adversary nations have proposed another method of governing AI: regulating cloud services (Dohman, Feldgoise, et al., 2023; Schare and Fist, 2023). They note that actors prohibited from buying AI chips can legally access the processing power of those chips through U.S. or foreign cloud services. Noting the leaky nature of export control regimes on devices, and the way bans on the export of U.S.-designed chips harm US economic and technological leadership and encourage China to develop its own chip industry, analysts at the Center for a New American Security (CNAS) and the Center for Security and Emerging Technologies (CSET) have proposed to:

[12] Relatedly, an October 2023 Executive Order (14110) from President Biden requires companies that "acquire, develop, or possess a potential large-scale computing cluster" to report "the existence and location of these clusters and the amount of total computing power available in each cluster" to the U.S. government (The White House 2023).

> Control cloud computing services that provide a China-located user with access to an advanced chip. … Make Infrastructure-as-a-Service (IaaS) directly controllable under the Export Administration Regulations (EAR) and implement "Know Your Customer" rules for CSPs.

This is another example of the way regulation of AI applications implicates the entire digital ecosystem. Hardware-based computing cannot be controlled without also pulling in transnational networked services that distribute hardware capabilities to networked devices. Once again, we see an attempt to make the tail of AI governance wag a much bigger digital dog: cloud computing, a US$ 500+ billion industry. The CNAS/CSET proposal would require regulating all clouds and impose surveillance and know-your-customer (KYC) regulations on its providers and users. To its credit, the CSET report flags a collective action problem inherent in the proposal, likely a fatal one. Unless these CSP regulations were global and uniformly enforced across countries, they could be easily bypassed. If the U.S. was the only authority to impose these requirements, for example, it would only disadvantage American CSPs relative to their Chinese or European counterparts.

6.4. Controlling applications: Europe

Among all regulatory authorities, the European Union seems to be the most bought in to the idea that "AI" is a new and distinct technology that requires a specialized regulatory regime. The European Union AI Act targets "AI systems," which it defines as

> … a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

The positive aspect of the EU AI Act is that it tries to take an application-specific approach. The Act bans some applications outright.[13] Non-banned applications are subject to a two-tier system of classification, high risk vs non-high risk. High risk applications pose a "significant risk of harm to the health, safety or fundamental rights of natural persons," or "materially influenc[e] the outcome of decision making." There is, however, no standard, no quantitative threshold for differentiating "high" from "low" risk, and no actuarial data that would make risk determinations scientific. Here the EU has been hampered by its insistence on taking an ex ante, anticipatory approach to regulation. Instead of responding to known problems posed by specific applications *ex post*, it posits preconceived categories of risk, which means its regulations can miss the target while blocking or retarding innocent innovations.

There is also a huge exception to the law: It does not apply to AI systems used exclusively for "military, defence or national security purposes, regardless of the type of entity carrying out those activities." Oddly, given the possibility of lethal autonomous weapons systems, the EU proposal exempts the most direct and serious risks to health, safety and fundamental rights from the law's consideration.

Following the logic of the digital ecosystem, the EU must extend its control to networking and data in order to maintain regulatory authority over AI applications. Noncompliant AI application providers located outside the EU cannot offer AI services in the EU jurisdiction via the Internet. The EU AI Act also tries to regulate data use by AI applications to ensure compliance with GDPR.

6.5. Controlling and labeling outputs: China

As noted by Sheehan (2023) and Zhang (2023), China viewed AI regulation as a form of content regulation. China recognized that social media recommendation algorithms were a form of AI, and instead of fearing human extinction, the Chinese Communist Party feared the extinction of their ability to control public discourse. Sheehan's analysis of the policy process indicates that the CCP Central Committee led the effort to control recommendation algorithms on social media because of their potential to expose Chinese users to news and messages not in accord with the Party line. They were also concerned about what we would call deep fakes and their potential to generate chaos. CCP guidance was implemented by the Cyberspace Administration of China, the specialized Internet regulator. The December 2021 "Provisions on the Management of Algorithmic Recommendations in Internet Information Services" includes many provisions for content control, protections for workers impacted by algorithms, and the creation of an "algorithm registry." The registry is an online database of algorithms that have "public opinion properties or… social mobilization capabilities." A November 2022 regulation prohibits the generation of "fake news" and requires synthetically generated content to be labelled. A subsequent regulation targeting chatbots extends control to data and requires both the training data and the generated content to be "true and accurate." So, chatbot hallucinations are illegal in China. China's other laws restricting the egress of "sensitive" data and requiring local storage also supports the regulatory regime affecting applications.

This section has mapped proposed forms of "AI regulation" to the digital ecosystem framework. By doing so, it clarifies the potentially dire consequences of misidentifying the object of governance. Controlling compute could mean an end to permissionless innovation in the digital economy, as access to powerful semiconductors would require some kind of prior approval by a central authority. Controlling access to data, networks and cloud services could further diminish the scope and freedom of a (formerly) globalized Internet. Controlling recommendation algorithms and AI outputs could curb or even end freedom of expression.

Does this mean that there is no beneficial role for public policy, law or regulation? The answer is both yes and no. If "regulate AI" means asserting hierarchical control over the digital ecosystem in order to achieve some generalized control over the ability to develop

[13] These are enumerated in general terms in Article 5, https://www.euaiact.com/article/5.

and distribute any and all machine learning applications, then No, there should be no regulation, and any attempt to do that would be a cure worse than the alleged disease. If "regulate AI" means responding individually to specific harms or property rights problems posed by specific machine learning applications, then Yes, it is possible and sometimes desirable for law, regulation or public policy to do so, as explained in Section 4.

7. Conclusion

This review of the "AI governance" problem illustrates how powerfully the initial framing and publicity surrounding tech developments can influence public policy. As generative AI applications burst onto the scene in 2022–2023, a small community of computer scientists, fearful that they were latter-day Oppenheimers unleashing a force of unprecedented destructive power, misled the world. They presented what was only an incremental extension of well-established digital capabilities as a "new technology" that was so frighteningly powerful that it required a distinct regulatory regime, if not an outright ban. (McMillan & Seetharaman, 2023) Since then, policy entrepreneurs in and out of government seized on the political opportunities created by this framing to entertain sweeping interventions into the digital ecosystem to protect us from what has turned out to be an imaginary threat.

This paper challenges that framing by showing that "AI" is not a new technology that creates its own distinctive governance problems, but a varied set of machine learning applications derived from a burgeoning digital ecosystem. These machine learning applications are already pervasive and have been manifest in the digital economy for three decades at least. The policy problems posed by the most recent applications of machine learning show a clear continuity with the policy problems posed by the rise of networked computing. Other than the "threat of human extinction" it is impossible to find a single policy problem attributed to "AI" that was not also posed by the rise of networked computing twenty to thirty years ago. Taking a systems approach to the problem, the paper shows how any attempt to govern generic "AI" capabilities implicates every element of the digital ecosystem. The approach of China, which correctly sees in AI governance an opportunity to maintain control over public communication, should serve as a warning about the risks and dangers – not of machine learning itself, but of our efforts to govern it.

The purpose of this paper was not to propose specific institutional changes or regulatory initiatives, but to introduce perspective and rationality into policy makers' responses to machine learning applications. Understanding "AI's" rootedness in the digital ecosystem and the way different machine learning applications pose different policy problems facilitates a more realistic assessment of the necessity and proportionality of regulatory interventions. It enhances awareness of the economic and social costs of ecosystem-wide restrictions, particularly regarding freedom of expression, open competition, and the ability to explore and innovate new applications of computing. Once we know that an attempt to govern some generic capability called "AI" implicates the entire digital ecosystem, we are in a much better position to identify feasible and beneficial public policy responses.

References

Arenal, A., Armuña, C., Feijoo, C., Ramos, S., Xu, Z., & Moreno, A. (2020). Innovation ecosystems theory revisited: The case of artificial intelligence in China. *Telecommunications Policy, 44*(6).
Biden, J. (2023). Executive order on the safe, secure, and trustworthy development and use of artificial intelligence. *Washington, DC: The White House*, (October 30).
Blew, R. D. (1996). On the definition of ecosystem. *The Bulletin of the Ecological Society of America, 77*(3), 171–173.
Bogers, M., Sims, J., & West, J. (2019). What is an ecosystem? Incorporating 25 years of ecosystem research. *SSRN*.
Bouhnik, D., & Deshen, M. (2013). Unethical behavior of youth in the internet environment. *International Journal of Technology, Knowledge and Society, 9*(2), 109.
Brockman, J. (Ed.). (2019). *Possible minds: 25 ways of looking at AI*. Penguin.
Cavin, R. K., Lugli, P., & Zhirnov, V. V. (2012). Science and engineering beyond Moore's law. *Proceedings of the IEEE, 100*(Special Centennial Issue), 1720–1749.
Corrêa, N. K., Galvão, C., Santos, J. W., Del Pino, C., Pinto, E. P., Barbosa, C., … de Oliveira, N. (2023). Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns, 4*(10).
Dean, J., Corrado, G., Monga, R., Chen, K., Devin, M., Mao, M., … Ng, A. (2012). Large scale distributed deep networks. *Advances in Neural Information Processing Systems, 25*.
Delany, S. J., Cunningham, P., & Coyle, L. (2005). An assessment of case-based reasoning for spam filtering. *Artificial Intelligence Review, 24*(3), 359–378.
Delipetrev, B., Tsinaraki, C., & Kostic, U. (2020). *Historical evolution of artificial intelligence*. Publications Office of the European Union. Technical Report.
Dick, S. (2019). *"Artificial intelligence." HDSR 1:1 (summer)*.
Dixon, R. B. L. (2023). A principled governance for emerging AI regimes: Lessons from China, the European union, and the United States. *AI and Ethics, 3*(3), 793–810.
Dohman, H., Feldgoise, J., Weinstein, E., & Fist, T. (2023). Controlling access to advanced compute via the cloud: Options for U.S. Policymakers. *Part I. Washington, DC: Center for Security and Emerging Technologies*. May https://cset.georgetown.edu/article/controlling-access-to-advanced-compute-via-the-cloud/.
Drucker, H., Wu, D., & Vapnik, V. N. (1999). Support vector machines for spam categorization. *IEEE Transactions on Neural Networks, 10*(5), 1048–1054.
Ebbinghouse, C. (2000). Deliberate misinformation on the internet!? Tell me it ain't so. *Searcher, 8*(5), 63, 63.
Edwards, D. W. (2018). Circulation gatekeepers: Unbundling the platform politics of YouTube's content ID. *Computers and Composition, 47*, 61–74.
European Parliament. (2023). EU AI Act: First regulation on artificial intelligence. *News release*. June 8 https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
Future of Life Institute. (2023). Pause giant AI experiments: An open letter, March 22. https://futureoflife.org/open-letter/pause-giant-ai-experiments/.
Gappmair, W. (1999). Claude E. Shannon: The 50th anniversary of information theory. *IEEE Communications Magazine, 37*(4), 102–105.
Garofalakis, J., Kappos, P., & Sirmakessis, S. (1998). Digital robbery; authors are not unprotected. In *Proceedings. Computer graphics international (cat. No. 98EX149)* (pp. 558–563). IEEE.
Gasser, U., & Mayer-Schönberger, V. (2024). *Guardrails: Guiding human decisions in the age of AI*. Princeton University Press.
Goldman, E. (2005). Search engine bias and the demise of search engine utopianism. *Yale JL & Tech., 8*, 188.
Gopstein, D., Zhou, H. H., Frankl, P., & Cappos, J. (2018). Prevalence of confusing code in software projects: Atoms of confusion in the wild. In *Proceedings of the 15th international conference on mining software repositories* (pp. 281–291).
Greenstein, S. (2015). *How the internet became commercial: Innovation, privatization, and the birth of a new network* (Vol. 16). Princeton University Press.
Harisch, K. (2023). Why artificial general intelligence is and remains a fiction. https://osf.io/preprints/osf/fjcns_v1.
Heaven, W. D. (2024). Large language models can do jaw-dropping things. But nobody knows exactly why. *Technology Review*, 477–486.
Hernon, P. (1995). Disinformation and misinformation through the internet: Findings of an exploratory study. *Government Information Quarterly, 12*(2), 133–139.
Hilbert, M. (2015). Quantifying the data deluge and the data drought. *Background Note for the World Development Report*, Article 2016.

Imagenet. About imagenet (website) https://www.image-net.org/about.php. (Accessed 28 July 2024).
Jeweler, R. (2005). *The Google Book Search Project: Is online indexing a fair use under copyright law?* Congressional Research Service. the Library of Congress.
Klein, R. (2015). *The cybernetics moment: Or why we call our age the information age*. Baltimore: The Johns Hopkins University Press.
Kolter, J. Z., & Maloof, M. A. (2004). Learning to detect malicious executables in the wild. In *Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 470–478).
Korolova, A. (2010). Privacy violations using microtargeted ads: A case study. In *2010 IEEE international conference on data mining workshops* (pp. 474–482). IEEE.
Koster, M. (1994). A standard for robot exclusion. https://www.robotstxt.org/orig.html#status.
Li, F., Fergus, R., & Perona, P. (2006). One-shot learning of object categories. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 28*(4), 594–611.
Liang, B. A., & Mackey, T. (2009). Searching for safety: Addressing search engine, website, and provider accountability for illicit online drug sales. *American Journal of Law & Medicine, 35*(1), 125–184.
Lopes, T. C., & Neder, H. D. (2017). Sraffa, Leontief, Lange: The political economy of input–output economics. *EconomiA, 18*(2), 192–211.
Ma, K., Grandi, D., McComb, C., & Goucher-Lambert, K. (2024). Exploring the capabilities of large language models for generating diverse design solutions. *arXiv preprint arXiv:2405.02345*.
Mack, C. A. (2011). Fifty years of Moore's law. *IEEE Transactions on Semiconductor Manufacturing, 24*(2), 202–207.
Mahoney, M. S. (1988). The history of computing in the history of technology. *Annals of the History of Computing, 10*(2), 113–125.
Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.
McCarthy, J., Minsky, M., & Shannon, C. (1955). A proposal for the Dartmouth summer research project on artificial intelligence. August 31 http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.
McMillan, R., & Seetharaman, D. (2023). How a fervent belief split silicon valley—and fueled the blowup at OpenAI.". *Wall Street Journal, 22*(2023 2), 25. pm ET.
Moore, J. F. (1993). Predators and prey: A new ecology of competition. *Harvard Business Review, 71*(3), 75–86.
Mowshowitz, A., & Kawaguchi, A. (2005). Measuring search engine bias. *Information Processing & Management, 41*(5), 1193–1205.
Mueller, M. (2024). The myth of AGI. *Internet Governance Project*. https://www.internetgovernance.org/wp-content/uploads/MythofAGI.pdf.
Nieborg, D. B., Poell, T., & van Dijck, J. (2022). Platforms and platformization. *The SAGE handbook of the digital media economy* (pp. 29–49). London: Sage.
Nielsen, J.. Nielsen's law of Internet bandwidth. Webpage. https://www.nngroup.com/articles/law-of-bandwidth/.
OECD. (2023). G7 Hiroshima Process on generative artificial intelligence (AI): Towards a G7 common understanding on generative AI (September 7) https://doi.org/10.1787/bf3c0c60-en.
Padawer, H. S. (2003). Google this: Search engine results weave a web for trademark infringement actions on the internet. *Wash. ULQ, 81*, 1099.
Page, L., Brin, S., Motwani, R., & Winograd, T. (1998). *The Pagerank citation ranking: Bring order to the web*. Stanford University. Technical report.
Pollack, J. B. (1989). Connectionism: Past, present, and future. *Artificial Intelligence Review, 3*(1), 3–20.
Rajamaran, V. (2014). John McCarthy - father of artificial intelligence. *Resonance*, 198–207.
Richards, D., Caldwell, P. H., & Go, H. (2015). Impact of social media on the health of children and young people. *Journal of Paediatrics and Child Health, 51*(12), 1152–1157.
Rieder, B. (2012). What is in PageRank? A historical and conceptual investigation of a recursive status index. *Computational Culture, 2*. http://computationalculture.net/what_is_in_pagerank/.
Roberts, H., Cowls, J., Hine, E., Morley, J., Wang, V., Taddeo, M., et al. (2023). Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. *The Information Society, 39*(2), 79–97.
Rouse, M. (2016). "In the wild." technopedia TechDictionary. https://www.techopedia.com/definition/31669/in-the-wild.
Sastry, G., Heim, L., Belfield, H., Anderljung, M., Anderljung, M., Brundage, M., et al. (2024). Computing power and the governance of artificial intelligence. https://www.cser.ac.uk/media/uploads/files/Computing-Power-and-the-Governance-of-AI.pdf.
Schare, P., & Fist, T. (2023). The cloud can solve America's AI problem. *Washington, DC: Center for a New American Security*.
Schmidt, E., Work, R. O., Catz, S., Chien, S., Clyburn, M. L., Louie, G., & Moore, A. W. (2019). *National security commission on artificial intelligence: Interim report, november 2019*.
Shannon, C. E. (1948). A mathematical theory of communication. *The Bell system technical journal, 27*(3), 379–423.
Sheehan, M. (2023). *China's AI regulations and how they get made*. Carnegie Endowment for International Peace. Working Paper https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.
Sheldon, D. (2010). *Manipulation of PageRank and collective hidden markov models*. Cornell University thesis. https://hdl.handle.net/1813/14806.
Strasburger, V. C., Jordan, A. B., & Donnerstein, E. (2010). Health effects of media on children and adolescents. *Pediatrics, 125*(4), 756–767.
Tamtomo, D. G., & Cilmiaty, R. (2019). Nutritional booklet and social media: Their effects on adolescents' fattening-food knowledge and consumption. *IOP Conference Series: Materials Science and Engineering, 633*(1), Article 012057. IOP Publishing.
von Neumann, J. (1945). First draft of a report on the EDVAC. In N. Stern (Ed.), *From ENIAC to UNIVAC: An Appraisal of the eckert-mauchly computers bedford* (pp. 181–246). Mass: Digital Press, 1981.
von Neumann, J. (1966). Theory of self-reproducing automata. In *Completed by arthur burks)*. Urbana and London: University of Illinois Press.
Wiener, N. (1950). *The human use of human beings: Cybernetics and society*. New York: Houghton Mifflin.
Wright, P. J., & Randall, A. K. (2012). Internet pornography exposure and risky sexual behavior among adult males in the United States. *Computers in Human Behavior, 28*(4), 1410–1416.
Xalabarder, R. (2012). *Google and the law: Empirical approaches to legal aspects of knowledge-economy business models*. Springer.
Yoffie, D. B. (1996). Competing in the age of digital convergence. *California Management Review, 38*(4), 31.
Zhang, A. H. (2024). *The promise and perils of China's regulation of artificial intelligence*. Available at: SSRN.
Zimmer, M. (2008). Privacy on planet Google: Using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine. *J. Bus. & Tech. L., 3*, 109.