#1599 Taming the Beast: AI Regulation Before Human Relegation

JAY TOMLINSON - HOST, BEST OF THE LEFT: [00:00:00] Welcome to this episode of the award winning *Best of the Left* podcast in which we shall look at why AI needs to be regulated by governments, even though politicians don't understand computers, just as the government regulates the manufacturer and operation of aircraft, even though your average politician doesn't know their ass from an aileron. Sources today include *In Focus*, *Your Undivided Attention*, *Democracy Now!*, *DW News*, *Today Explained*, and a *TED Talk*, with additional members-only clips from the *Thom Hartmann Program* and *In Focus*.

How are governments approaching AI regulation - In Focus by The Hindu - Air Date 11-16-23

G. SAMPATH - HOST, IN FOCUS: So to start with, I was wondering if you can give us a brief idea of what are the real concerns about AI that are animating, that are driving the legislative efforts of governments around the world? What are the core concerns?

DR. MATTI POHJONEN: Yeah, sure. So it's actually a very interesting debate. And as somebody who has been following the debate far before it became very publicly heated alongside JATCPT and some of the new models, is [00:01:00] that there has been a very kind of a mesh of different topics and themes that have been involved or underpinning lying some of the debates around how to best regulate and legislate artificial intelligence.

So I think a good way to start looking at this is that we start off with the kind of a negation or try to articulate or think about what potentially, or what has been one of the drivers of the debate that might not be the key thing to discuss in this podcast or in this conversation.

So there is a very popular kind of public conversation that has been going on around the image of machines, Terminators, artificial intelligence, as these machines take on the world. So there has been a very powerful debate around the kind of existential risk of AI, which has been driving some of the debates.

And once we start going into regulatory aspects of it, we can start seeing that there are various diverse interests that are actually underpinning the contemporary debates that are going on. So part of this what we call an existential AI narrative, there has been a lot of work that has been done around [00:02:00] what happens if AI becomes super, super intelligent and takes over and becomes this massive force that by the pure force of intelligence drives humans into extinction or into kind of a subservient position or what have you.

So there has been a counter-narrative that has been emerging in many, many kinds of different respects to this popular culture or this kind of narrative of AI as an existential threat is that one of the things that is often being hidden from the fact when we think about these very large questions around artificial intelligence is that what do these systems actually do, and how are they being concretely implemented in different aspects of society.

So there's a couple of versions of this kind of more critical narrative that has been advanced more in the attempts of trying to regulate different AI developments and companies.

So one of them is that -- and you can see we can start sketching out some of these debates as they're taking place on the public conversations and starting taking place also in the kind of online conversation that are going on -- but the core idea behind that is that when we move away from this grand narrative of somehow AI [00:03:00] becoming super intelligence and being able to pose a certain existential threat to humanity or to the ones who develop it, there has been various pressures of what are the actual concerns that now the systems are becoming very advanced, developed, and the progress of development is going at a very fast rate. So there's been pressure from society, societal pressure from civil society activism, to think about what aspects of AI should be regulated in terms of questions around bias in the systems. Questions about privacy have been a very big issue around things like facial recognition technology and their practical uses. Increasingly, there has been talk about what happens with especially generative AI of the types of fake or artificial or synthetic content that can be generated. There's also been one big debate that has been also underlying some of these things. So what are the consequences of the use of automated AI systems, and especially security and especially in weapons and autonomous weapons? And there's been a big debate around what happens [00:04:00] when AI becomes embedded into weapons systems and what are the limits and what kind of rules and regulations should we have then? And as we have been seeing in Ukraine and Gaza, this is already a concern that many of the systems are, in one form or another, using different AI models to drive or augment the systems that are being used.

So again, many of these kind of different interests have been meshing for a couple of years, and now they're starting to concretely find form or manifest in various regulations that are being proposed. And I think in that context, there's been two of the key legislative things that have been done, there was the EU AI Act that you mentioned, which was in 2021, where some of these principles were starting to be sketched out into something practical, or what would it mean in practice, and then Biden executed the order. And in a way, the EU AI Act is the next step is going to be, they're trying to move that into a very concrete legislation that then would provide guidelines and rules for this.

So in a way, the environment seems to be right through this various influences [00:05:00] for now to be the moment that some preliminary and legislatively binding legislations will emerge that we look at these various debates. Again, we can start sketching out some of the more detailed nuances out of this, but it's interesting now, especially with the Biden legislation or executive order, how these things are being increasingly pushed from governments and different actors.

So yeah, that's the kind of very broad environment in which many of these various, often conflicting and diverse debates have been finding form in the last two, three years.

A First Step Toward AI Regulation with Tom Wheeler - Your Undivided Attention - Air Date 11-2-23

TRISTAN HARRIS - HOST, YOUR UNDIVIDED ATTENTION: So this 111-page executive order is a sweeping announcement that imposes guardrails on many aspects of the new AI models.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: One of the remarkable things about this executive order is that it really takes seriously the full scale of impacts AI has in society, and that's why it's so broad. So it mandates that companies share internal testing data, and very importantly, that companies must notify the government when they are training new Frontier Foundation models -- that is, models that go beyond 10 to the 26 flops, [00:06:00] which is a fancy way of saying things that are of scale GPT 5 and beyond, as well as anything that poses serious national security, economic security, or public health threats.

The executive order also goes after the intersection of AI and biology by making federal funding for life sciences dependent on using higher standards around gene synthesis and the kinds of things that can be used to do nasty things with AI and biology.

The order also addressed the new development of cutting edge privacy tools and the mitigation of algorithmic bias and discrimination and the implementation of a pilot National AI Research Resource, or NAIR, which will fund AI research related to issues like health care and climate change.

And finally, the executive order tries to solve the deficit of AI talent in the US government itself. They are launching an AI talent search on AI.gov.

TRISTAN HARRIS - HOST, YOUR UNDIVIDED ATTENTION: I think what's most impressive about this order is just that it reflects the many different areas of society that AI touches, that it's not shying away from the multiple horizons of harm -- [00:07:00] privacy, bias and discrimination, job automation, AI expertise, biological weapons. Instead of saying these are way too many issues for the government to tackle, this executive order has bullet points for how it's going to try to signal a first step towards each of these areas.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: So, I actually was in the room as the president was signing the executive order. It was a privilege, really, to be there in this historic moment, and I was chatting with one of the White House lawyers, and he used a phrase that I thought was exactly right. He said, "This is the end of the beginning."

I remember Tristan, you and I, back in March, really realizing that we're going to have to have something like an executive order. We did the AI Dilemma, and while, of course, it's not us pushing for an executive order that made it happen, we've now sort of completed this process where in March, this was not an issue. The executive order was signed.

And so we're going to be discussing that today with Tom Wheeler. Tom Wheeler knows the tech industry from both [00:08:00] government and business perspectives. He was a venture capitalist in the cable and telecommunications industry, and he was chairman of the Federal Communication Commission, the FCC, from 2013 to 2017. These days, he is a Visiting Fellow in Governance Studies at the Brookings Institution, where he's been researching 21st-century tech regulation for his new book, *Tech Clash: Who Makes the Rules in the Digital Gilded Age*. Tom, welcome.

TOM WHEELER: Aza, thank you. It's great to be with you guys.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: Well, and to the storytelling of one of the first times we visited Washington DC, trying to meet the various institutions in DC, Tom, we were actually at a meeting, I think was that at the United Nations, or it was held by Dick Gephardt and some other groups, to try to figure out how are we going to get our hands wrapped around this? And I'm so curious, given your very, very deep expertise in government and in Washington, what is your overall take on the executive order?

TOM WHEELER: Well, let me back up first of all to both of you have been engaged in a missionary effort [00:09:00] that has been really important. And I think you ought to feel good about the fact that the President of the United States has stepped up as he did. You know, it's been interesting to watch as Congress talked, the administration moved forward and they move forward in an evolutionary process, if you will, the first thing out of the box was the AI Bill of Rights, which was kind of aspirational. And then came the NIST standards for management and mitigation, which are terrific, but without any enforcement. Then came the voluntary commitments of the major AI model companies that again were well intended, but so general as to almost be unenforceable. And now what President Biden signed in the executive order -- I mean, 111-page executive order -- I was [00:10:00] struck by his use of the Defense Production Act and its enforceability, mandatory nature to require certain things.

But the problem with executive action is that most of the other things are guidance and are not enforceable. We need enforceable oversight of the digital activities and that, absent action by Congress, we're not going to get there because of the fact that we're still operating under industrial-era rules and industrial-era statutes and industrial-era assumptions.

So, bottom line on the executive order, hooray, great leadership throughout this entire process. But we really need an enforceable strategy that only the Congress can create.[00:11:00]

You know, I often consider AI to be like the mythological Greek monster Hydra, the multi-headed monster. And, as I looked at the executive order, I think the president took a swing at every head he could find on the Hydra-headed AI monster. And that's terrific.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: In terms of just signaling power, and it wasn't lost on any of us that the UK AI summit was

happening directly after this announcement. And so there's a signaling value in saying the US is going to do something, or rather, that the US is taking it really seriously. And in the sense that we all have to do what we can do, I viewed this as incredibly good.

TRISTAN HARRIS - HOST, YOUR UNDIVIDED ATTENTION: This was sort of the maximum that Biden, or really the executive branch, could do. And so before we go into how might we fix the limits of our medieval or maybe industrial revolution-era [00:12:00] institutions, I do think it's important to walk through at least a little bit of what's in this executive order, especially around the use of the Defense Production Act to force government in the loop for frontier models and things like that.

And then let's step back to this larger question of structurally how might we redo governance to match the times?

TOM WHEELER: Sure. Back to the question of enforceability and the Defense Production Act and the requirement that certain of the companies, and I guess it is yet undefined, but certain of the companies that are building foundation models need to inform the government as to what the training is going on, need to be running some red team activities to try and identify vulnerabilities and share that information, because it has national security and economic security implications, therefore there can be mandatory [00:13:00] requirements. Those are all good and those are important steps and we need to understand what's in the black boxes and have an ability to, based on that understanding, deal with whatever reality is created. I think it falls short of the Food and Drug Administration, for instance, we will run government tests on every new pharmaceutical and determine whether or not it can be released to the market, but it's a move in that direction.

And it's a mandatory requirement that the government is at least aware of what is going on.

Now, the interesting thing, and we can get to this later, but the interesting thing is, I didn't see in the order specifically who was covered. And one of the fascinating things is, okay, how do we deal with open source models -- that is coming definitely from people [00:14:00] who we know are not covered by this.

Artificial Intelligence Godfathers Call for Regulation as Rights Groups Warn AI

Encodes Oppression - Democracy Now! - Air Date 6-1-23

AMY GOODMAN: Tawana Petty, welcome to *Democracy Now!* You are not only warning people about the future; you're talking about the uses of AI right now and how they can be racially discriminatory. Can you explain?

TAWANA PETTY: Yes. Thank you for having me, Amy. Absolutely. I must say that the contradictions have been heightened with the godfather of AI and others speaking out and authoring these particular letters that are talking about these futuristic potential harms. However, many women have been warning about the existing harms of artificial intelligence many years prior to now — Timnit Gebru, Dr. Joy Buolamwini and so many others, Safiya Noble, Ruha Benjamin, and so — and Dr. Alondra Nelson, what you just mentioned, [00:15:00] the Blueprint for an AI Bill of Rights, which is asking for five core principles: safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives, consideration, and fallback.

And so, at the Algorithmic Justice League, we have been responding to existing harms of algorithmic discrimination that date back many years prior to this almost robust narrative-reshaping conversation that has been happening over the last several months with artificial general intelligence. So, we're already seeing harms with algorithmic discrimination in medicine. We're seeing the pervasive surveillance that is happening with law enforcement using face detection system to target community members during protests, squashing not only our civil liberties and rights to organize and protest, but also the [00:16:00] misidentifications that are happening with regard to false arrests, that we've seen two very prominent cases started off in Detroit.

And so, there are many examples of existing harms that it would have been really great to have these voices of mostly White men who are in the tech industry, who did not pay attention to the voices of all those women who were lifting up these issues many years ago. And they're talking about these futuristic possible risks, when we have so many risks that are happening today.

NERMEEN SHAIKH: So, Professor Max Tegmark, if you could respond to what Tawana Petty said, and the fact that others have also said that the risks have been vastly overstated in that letter, and, more importantly, given what Tawana has said, that it distracts from already-existing effects of artificial intelligence that are widely in use already?

MAX TEGMARK: [00:17:00] I think this is a really important question here. There are people who say that one of these kinds of risks distracts from the other. I strongly support everything we heard here from Tawana. I think these are all very important problems, examples of how we're giving too much control already to machines. But I strongly disagree that we should have to choose about worrying about one kind of risk or the other. That's like saying we should stop working on cancer prevention because it distracts from stroke prevention.

These are all incredibly important risks. I have spoken up a lot on social justice risks, as well, and threats. And, you know, it just plays into the hands of the tech lobbyists, if they can — if it looks like there's infighting between people who are trying to rein in Big Tech for one reason and people who are trying to rein in Big Tech for other reasons. Let's all work together and [00:18:00] realize that society — just like society can work on both cancer prevention and stroke prevention. We have the resources for this. We should be able to deal with all the crucial social justice issues and also make sure that we don't go extinct.

Extinction is not something in the very distant future, as we heard from Yoshua Bengio. We might be losing total control of our society relatively soon. It can happen in the next few years. It could happen in a decade. And once we're all extinct, you know, all these other issues cease to even matter. Let's work together, tackle all the issues, so that we can actually have a good future for everybody.

AMY GOODMAN: So, Tawana Petty, and then I want to bring back in Yoshua Bengio — Tawana Petty, what needs to happen at the national level, you know, U.S. regulation? And then I want to compare what's happening here, what's happening in Canadian regulation, the [00:19:00] EU - European Union - which seems like it's about to put in the first comprehensive set of regulations, Tawana.

TAWANA PETTY: Right, absolutely. So, the Blueprint was a good model to start with, that we're seeing some states adopt and try to roll out their versions of an AI Bill of Rights. The president issued an executive order to strengthen racial equity and support underserved communities across the federal government, which is addressing specifically algorithmic discrimination. You have the National Institute of Standards and Technology that issued an AI risk management framework, that breaks down the various types of biases that we find within algorithmic systems, like computational, systemic, statistical and human cognitive. And there are so many other legislative opportunities that are happening on the federal level. You see the FTC speaking up, the Federal Trade Commission, on algorithmic discrimination. You have the [00:20:00] Equal

Employment Opportunity Corporation that has issued statements. You have the Consumer Financial Protection Bureau, who has been adamant about the impact that algorithmic systems have on us when data brokers are amassing these mass amounts of data that have been extracted from community members.

So, I agree that there needs to be some collaboration and cooperation, but we've seen situations like Dr. Timnit Gebru was terminated from Google for warning us before ChatGPT was launched upon the millions of people as a large language model. And so, cooperation has not been lacking on the side of the folks who work in ethics. To the contrary, these companies have terminated their ethics departments and people who have been warning about existing harms.

The EU agrees on AI regulations - What will it mean for people and businesses in the EU - DW News - Air Date 12-9-23

ANCHOR, DW NEWS: Now, the European Union has agreed on legislation to govern the use of artificial intelligence. The deal includes limits on facial recognition technology and [00:21:00] restrictions on using AI to manipulate human behavior. The EU says the future legal framework for AI will include tough penalties for companies breaking the rules but will not stifle development of the industry in Europe. It follows years of discussions among member states and lawmakers in the European Parliament.

BRANDON BENIFEI: We had one objective: to deliver a legislation that would ensure that the ecosystem of AI in Europe would develop with a human-centric approach, respecting fundamental rights and the European values.

THIERRY BRETON: This is really something that is much more, I believe, than a rule book. It's a launchpad for the European startups and also researchers to lead the global race for what our fellow citizens want, a trustworthy AI.

ANCHOR, DW NEWS: For more on this, let's bring in our correspondent in Brussels, Bernd Riegert. Hello Bernd, uh, why did the EU decide that this law was needed?

BERND RIEGERT: Well, the [00:22:00] EU felt it is about high time to regulate, and the EU wants to be the first in the world, the first big regional business area to regulate artificial intelligence. Neither the U. S. nor Asian markets have this regulation, and in this way the EU wants to set the world's

standards for the whole industry, and the EU also felt that it is a high time to do this now because there are some dangers deriving from artificial intelligence and the EU sees itself as at the forefront of a revolution, actually, in business because AI will have impact on every field of daily life in the future.

ANCHOR, DW NEWS: The future is quite tricky when you think about AI, isn't it? Walk us through some of the measures that will be put in place and what they will mean for people and companies in the EU.

BERND RIEGERT: The EU will divide AI applications into four risk classes. Some of them will be completely forbidden, like facial [00:23:00] recognition on a mass scale. There are some exemptions for military and law enforcement. And also behavioral control and the control of your thoughts, that will be also banned. But high risk applications, for example, in self-driving cars, will be allowed in the EU, but they have to be certified, the technique has to be open so that everybody can see how that works, and normal AI, I would call it like ChatGPT, on a medium risk level, that can be in the EU without any restrictions, but it has to be documented how this thing works, and everybody has to know that he is dealing with AI, that he's not talking to a human.

This is one of the essential measures in the whole legislations. You as a consumer shall always decide, Do I want to talk to a machine? I have to know that it's not human. This is the basic principle, but there are also some AI applications that will be not regulated. For [00:24:00] example, audio and video altering programs that make these well known deep fakes. These are not regulated. They don't pose a higher risk in the view of the EU.

ANCHOR, DW NEWS: Okay, what has the reaction been so far? I assume quite mixed, right?

BERND RIEGERT: Well, there are positive and negative reactions on both sides of the aisle, if you will. The business lobby is saying this is far too much. It's too far because, uh, it's over-regulation, it will hamper competition, it will prevent startups from coming up with new solutions. Some companies might even leave Europe to go to the United States or Asia to develop their applications there. On the other hand consumer protection groups say this is not far enough because the data are not protected very well. And there are some AI applications, for example, in toys that are not regulated, that could attack the thoughts and the behavior of our [00:25:00] kids. So both sides are not really satisfied that shows that they somehow reached a balance.

EU vs. AI - Today, Explained - Air Date 12-18-23

ANU BRADFORD: So I would go back to early 1990s. That's when the U. S. really stepped back from regulation.

PRESIDENT BILL CLINTON: Because the Internet has such explosive potential for prosperity, it should be a global free-trade zone.

ANU BRADFORD: Up until then, the U. S. had often been setting the rules that had global impact, but then the U. S. really adopted this market-driven dogma that was very anti-regulation. So the U. S. took the lead in promoting this deregulation agenda.

PRESIDENT BILL CLINTON: It should be a place where government makes every effort first, as the vice president said, not to stand in the way.

ANU BRADFORD: And the EU stepped in and filled the vacuum because at that very point, the EU was ramping [00:26:00] up its own efforts to integrate the common European market. And that meant it needed to harmonize regulations so that we remove the barriers from within the member states for trading within the EU. So, the EU started proactively building a regulatory state, not for the purpose of ruling the world, but for the purpose of making Europe an integrated, strong trading area.

JACQUES DELORS: We will strengthen the impact of this community through the ongoing implementation of common foreign and security policies.

ANU BRADFORD: So then the EU started focusing its regulatory efforts on digital economy.

NEWS COMMENTATOR: The European Union has approved rules to force big technology firms such as Google, Facebook, and Twitter to remove illegal content... the European Union has hit tech giant Meta with a record breaking fine of over a billion dollars for defying privacy rules.

ANU BRADFORD: And the gap between what the EU was producing and what the U. S. was failing to do in the regulatory space just became [00:27:00] larger and larger. But initially, it was really the U.S.'s decision to say that, Look, we trust the markets and the EU making philosophically a very different rule.

And I think the inadvertent effect, the unintended consequence, was that the U. S. basically ceded this whole governance base to the EU.

SEAN RAMESWARAM - CO-HOST, TODAY, EXPLAINED: And what has it accomplished? Give us some of the greatest hits.

ANU BRADFORD: Well, I would say the GDPR is by far the most famous hit.

NEWS COMMENTATOR: The European Union's General Data Protection Regulation, known to friends as GDPR, goes into effect tomorrow....

ANU BRADFORD: So, that was enacted in 2016. And that is a very significant regulation in shaping the entire global data privacy conversation and legislative frameworks.

Then also antitrust. So, the Europeans are very concerned about the abuse of market power by dominant tech companies.

MARGRETHE VESTAGER: You have to recognize [00:28:00] that you have powers beyond anyone else's and with that comes the responsibility.

ANU BRADFORD: So, there have been four antitrust lawsuits against Google that have been successfully concluded in the EU and that have resulted in around 10 billion dollars in fines.

And then there is the content moderation space. So, the Europeans are very concerned about disinformation, they're very concerned about hate speech, and the toxic environment surrounding Internet users when they are using the platforms.

MARGRETHE VESTAGER: And we need to say to some of these service providers, you have a responsibility for the way you do business to make sure that people feel as comfortable when they are online as well as when they are offline.

ANU BRADFORD: So, the Europeans have moved to limit hate speech and limit disinformation, even though they remain committed to freedom of expression. There is just a sense that that important commitment to free speech is balanced against some other fundamental rights, [00:29:00] including a right to dignity.

SEAN RAMESWARAM - CO-HOST, TODAY, EXPLAINED: And a hard pivot away from dignity to your phone chargers, maybe the most tangible of all these Brussels effects.

NEWS COMMENTATOR: There are USB-A chargers. There are USB- B chargers. There are USB-C chargers There are micro USB chargers. There are mini USB chargers...

ANU BRADFORD: The EU also regulates consumer electronics. So there's an environmental concern surrounding consumer waste. And then another concern, just the consumer convenience, if you like, the idea that we do not want the consumers to have to buy different cords for all the different devices and all the different jurisdictions where they are using them.

So, uh, the EU standardized the common charger, which then led Apple to also switched its own charging port and extend that change, not just to Apple in Europe, but also outside of the EU.

NILAY PATEL: [00:30:00] You know, the word from Apple basically is like, 'the Europeans made us do it. But it's time, and we don't think people will freak out'.

SEAN RAMESWARAM - CO-HOST, TODAY, EXPLAINED: Now, in a case like that, with the Apple USB-C charger situation, where literally everyone around the world who has this device will have their tech now changed because of this EU regulation, why does it make more sense for a tech company like Apple to change this charging port for the whole world instead of just for the European market. Tell us how the Brussels effect makes sense for a business.

ANU BRADFORD: So, often for these tech companies, it's just a matter of efficiency and a cost calculus. So it is not efficient to run multiple different production lines. There are scale economies in uniform production. So they don't want to be producing different variations for different markets. And same applies for companies [00:31:00] like Meta's Facebook. They pride themselves of having one global Facebook. So if you and me are having a conversation and I'm in Europe and you are in the United States, they don't want there to be a different speech rules that apply to the conversation whereby I would not be seeing a part of the conversation that you are able to see because there are different content moderation rules that would make it really difficult to have effective cross border conversations. But I would say, Sean, that the most common reason is just simply it is just too expensive to have many varieties off the same product.

A First Step Toward AI Regulation with Tom Wheeler Part 2 - Your Undivided Attention - Air Date 11-2-23

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: One thing I wanted to ask you about, Tom, for people who are not really familiar about this, one of the levers that the executive order uses is federal funding conditions. So basically in a few different places, the government's saying in this executive order as a condition, for example, life sciences funding, to get that funding from the government, you have to do these new and improved practices. So, for [00:32:00] example, one of the things executive order covers in the hydra -- which I think is a great term, it covers the many horizons of harm, to use our internal phrase here at CHT, that because AI affects bias, discrimination, jobs, labor, biological weapons, risks of doom scenarios, sci-fi scenarios, all the way up to the long term when something affects all those different horizons of harm at the same time, that's the hydra that you're speaking to. And I think again, applaud the people who are working extremely hard at this at the White House, Ben Buchanan, Bruce Reed, the whole teams that have been working very, very hard on this, and done in record time, I think six months, unprecedented. It's the most aggressive action that they could have taken. And one of the areas that they covered in that hydra is actually the intersection of AI and biology, and them mandating that there needs to be new and improved genetic synthesis screening so that labs have tighter controls on the kind of materials that one would use with AI to do nasty stuff with biology.

Can you speak to any of the history of this, the power of this lever? Because obviously this is only going to affect places that are affected by federal funding, but I think you have some background here. [00:33:00]

TOM WHEELER: There are two principal ways in which the government affects the marketplace. One is through direct regulation, and the other is through its role as typically the largest consumer. And that's what this second part that you've been talking about is doing. And again, it's terribly important.

I just have to pause here for a second. I agree with everything you just said about the incredible effort, speed, and dedication that went into doing this. I don't want to have that as somehow being Eeyore and complaining about the significance of this effort. But one of the drawbacks, one of the shortcomings of relying simply on government procurement or government funding is that it only goes to those who are procuring or being funded. And again, as you guys

have been so terrific in your missionary work in pointing [00:34:00] out, this is much more expansive than that.

So huzzah, yes, use every tool at your disposal, but we also need new tools.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: I Think another thing that this executive order does is it lets us see when the tech companies are speaking out of both the left side and the right side of their mouth. It forces that hand. Because I remember, Tristan and I were at the Schumer AI Insight Forum and there was the moment that I think Schumer really wanted, when he asked, who here thinks the federal government will need to regulate AI and should regulate? And every single CEO, from Sam Altman to Mark Zuckerberg to Satya Nadella, from all the major companies, raised their hand. Right? And that led to headlines like "Tech industry leaders endorse regulating artificial intelligence." And "The rare summit in Washington."

And then right after the executive order comes out, NetChoice, which is funded by a lot of those same organizations, releases their quote, which is "Biden's new executive [00:35:00] order is a backdoor regulatory scheme for the wider economy, which uses AI concerns as an excuse to expand the president's power over the economy."

So here we go, right? They're saying like, yes, please regulate us. Just not that one. And they're with one hand they're saying yes, and the other hand they're saying no. So I would love for you to talk a little bit about that dynamic.

TOM WHEELER: So Aza, as a recovering regulator, this is like the line in Casablanca, where Claude Rains says "There's gambling going on here?" This is a classic move in these kinds of environments that yes, I am all for puppies and apple pie and the flag. And now let's talk about what the specifics of that means. Oh, golly, we can't go there. This would be terrible. This would be awful. And against innovation and, then all come out all the detailed imaginary horribles. One should not be surprised. One of the things I'm proudest of is my term as chairman of the FCC was net [00:36:00] neutrality. I would meet with industry executives or listen to them make their speeches or testify. And we're all for net neutrality, but let's define net neutrality *my way*, which is it's only about blocking and throttling.

This is why the job of policymaking is so damn difficult. I'd come home from work when I was chairman and I'd sit there at the dinner table with my wife and I would say, the public interest is fungible. There is nothing clear cut about "this is the public interest." There's *this* aspect of the public interest, and *that* aspect

of the public interest, and the job of the policymaker is to sift through all of that and figure out what is the fungible answer to address the public interest.

AZA RASKIN - CO-HOST, YOUR UNDIVIDED ATTENTION: You're saying, in the end, you have to choose a process that does good like sense [00:37:00] in decision making. It's not gonna be something just static in time. And one of the parts of the EO is this personnel as policy thing. Right now there's a dearth of knowledge of expertise about AI in the government. And so there's a huge hiring spree. There's going to be a head or chief of AI, I think in now every federal agency. And I think the White House is creating a White House AI Council, which will coordinate all the federal government's AI activities, staff from every major federal agency.

So I'm curious then, in the frame of "the end of the beginning," what happens next? Is the AI Council the right way to think about it? And, of course, back to your fundamental question of how do we have governance keep up with the increasing pace of AI?

TOM WHEELER: First of all, Bruce Reed, who's the Deputy Chief of Staff at the White House and is going to head the AI Council, is a really good guy who understands these [00:38:00] kinds of issues. But his job will be to be the maestro, if you will.

I think, at the end of the day, what we need is a new federal agency that is focused on the realities that digital has brought to a previously industrial economy and society and government. And that there has to be that kind of hands-on authority. At the end of the day, you're gonna need somebody with rule making authority to come in and say, "Okay, these are the decisions that we made; back to the question of what's in the public interest. Here's how we've put those various forces together."

But let me pick up on one other thing that I was thinking as you were saying that. I watched Eric Schmidt on *Meet the Press* a month, six weeks ago, whatever it was, when they were interviewing him about AI, and he said, Oh, you gotta let the companies make the rules here [00:39:00] because there's nobody in government that can understand this. And I got infuriated because we used to hear that in the early days of the digital platforms. Oh, these digital platforms are so complex and if you touch it, you'll break the magic kind of a thing. And it seems to be the same kind of playbook, which is, well, let's let the company just go ahead and make the rules because they are really the only ones that understand.

And, I just kept saying to myself, well, wait a minute. We split the atom. We sent men to and from the moon safely in a government program. And sure, there is not the kind of in-depth knowledge widespread. But you know what? I bet that there are very few members of Congress who can explain jet propulsion or Bernoulli's principle that keeps airplanes in the air, but we sure do regulate the manufacture and operation of aircraft.

How to Keep AI Under Control Max Tegmark - TED - Air Date 11-2-23

MAX TEGMARK: The [00:40:00] real problem is that we lack a convincing plan for AI safety. People are working hard on evals, looking for risky AI behavior, and that's good, but clearly not good enough. They're basically training AI to not say bad things, rather than not do bad things. Moreover, evals and debugging are really just necessary, not sufficient conditions for safety. In other words, they can prove the presence of risk, not the absence of risk. So, let's up our game, alright? Try to see how we can make provably safe AI that we can control.

Guardrails try to physically limit harm. But if your adversary is super intelligent or a human using super intelligence against you, trying is just not enough. You need to succeed. Harm needs to [00:41:00] be impossible. So we need provably safe systems. Provable, not in the weak sense of convincing some judge, but in the strong sense of there being something that's impossible according to the laws of physics. Because no matter how smart an AI is, it can't violate the laws of physics and do what's provably impossible. Steve Omohundro and I wrote a paper about this, and we're optimistic that this vision can really work. So let me tell you a little bit about how.

There's a venerable field called formal verification, which proves stuff about code. And I'm optimistic that AI will revolutionize automatic proving business. And also revolutionize program synthesis, the ability to automatically write really good code. So here is how our vision works. You, the human, write a specification that your AI tool must obey. That it's impossible to log in to your [00:42:00] laptop without the correct password. Or that a DNA printer cannot synthesize dangerous viruses. Then a very powerful AI creates both your AI tool and a proof that your tool meets your spec. Machine learning is uniquely good at learning algorithms, but once the algorithm has been learned, you can re-implement it in a different computational architecture that's easier to verify.

Now you might worry, how on Earth am I gonna, like, understand this powerful AI and the powerful AI tool it built and the proof, if they're all too complicated for any human to grasp. Here is the really great news, you don't have to understand any of that stuff. 'Cause it's much easier to verify a proof than to discover it. So you only have to understand or trust your proof checking code, which could be just a few hundred lines long. And, uh, Steve and I envision [00:43:00] that such proof checkers get built into all our compute hardware, so it just becomes impossible to run very unsafe code.

What if the AI though isn't able to write that AI tool for you? Then there's another possibility. You train an AI to first just learn to do what you want, and then you use a different AI to extract out the learned algorithm and knowledge for you, like an AI neuroscientist. This is in the spirit of the field of mechanistic interpretability, which is making really impressive rapid progress. Provably safe systems are clearly not impossible.

Let's look at a simple example of where we first machine learn an algorithm from data and then distill it out in the form of code that provably meets spec. Okay? Let's do it with an algorithm that you probably learned in first grade addition, [00:44:00] where you loop over the digits from right to left, and sometimes you do a carry. We'll do it in binary, as if you were counting on two fingers instead of ten. And we first train a recurrent neural network, never mind the details, to nail the task. So now you have this algorithm that you don't understand how it works, in a black box, defined by a bunch of tables of numbers that we in nerd speak call parameters. Then we use an AI tool we built to automatically distill out from this the learned algorithm in the form of a Python program. And then we use the formal verification tool known as Dafny to prove that this program correctly adds up any numbers, not just the numbers that were in your training data.

So in summary, provably safe AI, I'm convinced, is possible. But it's going to take time and work. And in the [00:45:00] meantime, let's remember, all the AI benefits that most people are excited about actually don't require superintelligence. We can have a long and amazing future with AI. So, let's not pause AI. Let's just pause the reckless race to superintelligence. Let's stop obsessively training ever larger models that we don't understand. Let's heed the warning from ancient Greece and not get hubris like in the story of Icarus. Because artificial intelligence is giving us incredible intellectual wings with which we can do things beyond our wildest dreams, if we stop obsessively trying to fly to the sun. Thank you.

Anti-Democratic Tech Firm's Secret Push For A.I. Deregulation w Lori Wallach - Thom Hartmann Program - Air Date 8-8-23

THOM HARTMANN - THOM HARTMANN PROGRAM: I understand from the press release that I got from you a couple of days ago [00:46:00] that these big tech firms that want to basically own artificial intelligence and use it for their own purposes and whatnot, really don't want to be regulated and they're trying to use some of these international trade deals to prevent that regulation. Am I correctly understanding what you're writing about?

LORI WALLACH: That's exactly right. It is happening. It's a play you have revealed from big corporations before. This time it's the big tech sector that wants to use its lobbyists, its money, to rig trade agreements, to basically handcuff Congress, so that, finally, as Congress and the Biden administration and the regulatory agencies realize they need to regulate these behaviors for their monopoly abuses, for their privacy abuses, for who knows what AI civil rights and civil liberties abuses will ensue, [00:47:00] just as that's starting, the companies realize, Wow, we're not going to win in front of Congress in public. Let's try the old Trojan horse. They're trying to put new rules that would basically forbid regulation in trade agreements even though they have nothing to do with trade.

THOM HARTMANN - THOM HARTMANN PROGRAM: I get it. My understanding is that treaties actually supersede federal law. They become the kind of the supreme law of the land, short of the Constitution. But these are being done as trade agreements, not as treaties. They don't require Senate ratification, or am I wrong? What am I missing here?

LORI WALLACH: So, these are what are called international executive agreements. They're not a full treaty, like the past trade agreements were not full treaties. And the great news is the Biden administration isn't doing the bad old trade deals like the NAFTAs. They're not doing the outsourcing incentives. They're not doing the bans on Buy America. They're not doing the corporate [00:48:00] tribunals, the big pharma giveaways. But buried in the guts of a couple different trade initiatives, these big tech lobbyists, put arcane, weasley language that to the average reader doesn't seem like anything so bad: take away the regulatory tools that are needed to get big tech unleashed.

So here's just one example, Tom, and this is what you saw the news release. We just did a report. And folks can see these reports at rethinktrade.org. It's a study

that shows the number one thing that Congress and the regulatory agencies need to regulate AI is transparency, they need to look at the algorithms in advance and make sure they're not racially biased or they're not invading our civil liberties. What the tech firms want is a new rule buried in the trade agreements [00:49:00] that forbid any government from requiring disclosure of even detailed descriptions of algorithms. And it's framed in language that makes you think it's, Oh, trade secrets must be good for business. But what it is is evading regulation and the companies want to put three or four of those kinds of rules buried in the hundreds of pages of trade language that, basically, they take away the ability of being held accountable.

THOM HARTMANN - THOM HARTMANN PROGRAM: Now when I wrote this book, *The Hidden History of Big Brother in America*, I, you know, I wrote at some length about the algorithms that are driving social media, for example, and how black box they are. We have no idea why it is that, you know, conservatives do so well on Twitter and Facebook and liberals don't do so well. Um, but there are some indications that a lot of it has to do with how the algorithms are set up and they absolutely refuse to reveal these saying that they're trade secrets. [00:50:00] Are they taking the trade secret path on the AI algorithms too?

LORI WALLACH: I mean, you have a right not to have your confidential business information disclosed to another company, but a trade secret protection is what you get when you are required to give your information to the government, for instance, to show a drug is safe and effective or that a pesticide is not going to give cancer. So, trade secrets protections is a different thing. That means like if I say, Tom, you've just created the best flavor of blah, blah, but the Food and Drug Administration needs to make sure it's safe, you send that to me. You have trade secret protection as the creator of that. That means, as the government, I can't show that to your competitor.

What this is, is a step beyond. This is saying the government can't see it. The government can't make sure it's safe and that's what they're... they already have trade secrets protections. That's already in the WTO. That's in the US law. [00:51:00] No one's giving the information away and in fact, interestingly, all the countries in the world have that WTO obligation not to do it. This is about, you can't regulate. Or here's another one that will just make your toes curl. They've got a rule that gives the company's apps guaranteed control over our data, and it literally says including personal data, as to where it can be stored, where it can be processed, can you get it deleted... it explicitly forbids the government from limiting the flows of data or limiting where it can be stored. And there's no,. Even an exception for like infrastructure where you'd want, you

know, you'd want certainly sensitive data not to be susceptible to cybercrime. It's just given over so the government can't regulate.

So these rules, they hope to slip into whatever trade negotiation gets done first. And they've been pushing this at the WTO, the big tech companies for some years. Now they start [00:52:00] trying to push it for the Indo-Pacific Economic Framework, which is a commercial negotiation the Biden administration is doing. They're pushing it for a U. S. Taiwan commercial negotiation, they're trying to weasel it in there. It's like mushrooms after a rain. There's so many big tech lobbyists popping up with this nefarious language.

But basically what we all need to do, this only works, this kind of Trojan horse strategy, only works if we're not aware. So we need to be running around with our mouths wide open, making sure our members of Congress, our local officials, because state law as well has privacy rules, we need to make sure everyone knows this stunt is afoot. They can't get away with it.

How are governments approaching AI regulation Part 2 - In Focus by The Hindu - Air Date 11-16-23

G. SAMPATH - HOST, IN FOCUS: So I wanted to have a quick response from you on this, which is, this is one aspect, you mentioned it briefly just now, which is a big concern for anyone interested in AI regulation, which is the whole phenomenon of deep fakes. Hardly a week goes by without a deep fake controversy popping up on Twitter and Facebook.

[00:53:00] So are there any common approaches or safety guidelines that have been evolved or that are in the reckoning right now to check this phenomenon?

DR. MATTI POHJONEN: There is a lot of stuff being done in terms of trying to develop these, but it's not very easy in terms of coming up with a very simple solution to various things.

And so some of the kind of things that you mentioned for instance, in the Slovenian elections that took place a couple of months ago, they had been demonstrating uses of, it's not a fake video, but it's the fake audio voice of some of the political candidates. And there has been debate, how much that influenced the final outcomes in a very tight election. And there has been, as I mentioned, there is a very growing concern or almost a panic about what's going to happen

in the upcoming elections now that it's not only video, but you can also fake audio text and at a scale and speed that has not been happening before.

So in terms of when you start looking at the way that people are thinking about mitigating this or trying to prepare for its risks, there's a various couple of different kind of initiatives being [00:54:00] done.

And so I've been following it. So Witness has been one organization that has been trying to establish some guidelines through which companies and policymakers should respond to trying to think about it in a more systematic way, what might be the risk of deepfakes.

And the thing is that at the same time, generative AI is being used for a lot of creative purposes. And the fact that it's being used for so-called inauthentic behavior or politically manipulated behavior, it's a very small component of it. So the balance is that how should we try to maintain the creative edge of it while dealing with this more nefarious purposes. UNESCO has a working group that they're trying to come up with some things.

There's a kind of arm's race in the computer science platform, social media platform of trying to find ways of trying to watermark them or creating ways that you could actually detect how things are fake. I'm a lecturer at the university. So why lecture at the university? So now the debate is that how much can students be using them and what are the ways of catching them?

So in a way, it's one of these things that has been going so quickly that the legislation, again, is trying to figure out what would [00:55:00] be the best balance to draw between the creative stuff, and then it's being used for political purposes.

I just wanted to add very quickly, if you have time, one thing that there are two fundamentally different strategies that are now being competed, dealing with, especially the development of AI models. You have the proprietary models, such as Midjourney, and then you have ChatGPT and some other ones, which have quite strict control on the moderation of the content that can be produced by them because they have been receiving a lot of criticism.

But then there's a whole ecosystem of open source models that are then openly available that can be used for various purposes and have been already used for things like stable diffusion, for instance, was one of the big ones that was there. But it's even a more fundamental debate that because the foundation models,

stable diffusion is no open source, but they basically open the model and people can fine tune them for further purposes.

But there is now an interesting division rising both politically and within the corporate sphere between companies that want to keep [00:56:00] models private. So things like Google, some of them are open source, but they want to keep the foundational models private or not open source. And then companies like Meta and some other ones want to keep them open. And now the debate has been shifting all the way to regulation that should open source models should be regulated potentially for their ability to generate things that have not been as moderated as big companies are able to do. At the same time, the other side is saying is that you're actually by overtly regulating these models capability of doing things like also they're using as political disinformation.

If you regulate them too much, that means you're actually giving big companies support for their business. And you're getting rid of this more creative, small companies working with open source. And that's also becoming, so there's a lot of active lobbying going on behind the scenes where on the one hand you have some computer scientists like working for Meta who are saying open source ecosystem is better for development, it should be left open despite some of the concerns, whereas then there's other ones that we should regulate significantly so that the open source models [00:57:00] won't be given as much ability to cause damage.

So in a way, when you start looking at the kind of debate around regulation, it's also partially a debate around who gets to own the systems and the infrastructures for building new types of content. And so when you're looking at these proposals to regulate deepfakes, it builds into these various networks of different underlying debates that apply to more broadly also to like AI regulation that we have been discussing.

Final comments on the need to understand the benefits and downsides of new technology

JAY TOMLINSON - HOST, BEST OF THE LEFT: We've just heard clips today, starting with *InFocus* explaining the public policy approach to AI. *Your Undivided Attention* broke down Biden's executive order on AI. *Democracy Now!* looked at the social justice threats from AI. *DW News* looked at the EU's approach to AI. *Today, Explained* explained the Brussels effect. *Your Undivided Attention* looked at more ways to inform policymakers about proper regulation.

And a *TEDTalk* proposed a technical solution to creating safe AI. That's what everybody heard, but members also heard bonus clips from the *Thom Hartmann Program*, looking at how big [00:58:00] tech is trying to undermine regulation through trade agreements. And *In Focus* discussed the risk of deep fakes on elections and hurdles to regulation.

To hear that and have all of our bonus content delivered seamlessly to the new members only podcast feed that you'll receive, sign up to support the show at bestoftheleft.com/support. During December, we are offering 20% off memberships for yourself or as gifts. So, definitely take advantage of that while you can, or shoot me an email requesting a financial hardship membership, because we don't let a lack of funds stand in the way of hearing more information.

Now to wrap up. I just wanted to reiterate an idea about new technology that I think can't be said enough because it helps to frame the discussion in an important way. The debate so often comes down to tech boosters versus the tech doubters, or the naysayers, or the ones pointing out that new tech based on old patterns will reinforce old systems of oppression like [00:59:00] racism, or otherwise, rather than remove it, and so on. So, my concern is that the average person listening to this debate - and is not like super well-informed - will just wonder, What, well, which is it?: Good or bad. Or even the people who are informed will feel the need to come down on one side or the other and proclaim that the new technology in question is either good or bad. But anyone who falls into that trap is going to be making a mistake and potentially blinding themselves to the perspectives of the other side. And that ends up getting us nowhere.

The more accurate truth is to understand that new tech often ushers in simultaneous versions of both utopia and dystopia all at once. And I got this framing from Tristan Harris, who we heard from today on *Your Undivided Attention*. Years ago, he described this idea using ride hailing apps as the example. You know, the ability to [01:00:00] tap a button on your phone and have a car pick you up in a few minutes. And that's, like, a genuinely amazing thing. It's like sort of a techno utopia that that's possible now. But he also pointed to how that business model was looking to undermine the hard-fought benefits that cab driver unions had won. And, uh, you know, they were looking to reduce the pay and benefits earned by professional drivers, which is just the latest in the unbroken chain, going back all the way through capitalism, to attempt to pay labor as little as possible and maximize the profits for owners. And that is certainly not utopia.

But it's important to understand both sides and appreciate why tech boosters believe in the benefits they trust the tech will bring. Genuinely good things come from technology all the time, from ride hailing apps to next generation vaccines. But similarly one must understand the current and potential [01:01:00] downsides that new tech has brought and will continue to bring. Otherwise these advocates on both sides will continue to just talk past each other.

If you want to sing the praises of new technology, your entire framework must include safeguards, and not just against existential Terminator-type threats, but against everyday abuses and structural flaws that create oppression, as we heard about today. But if you are one of those, as I am, cautioning against the potential downsides of new tech, you also have to understand why people are so excited about the potential good that new tech like AI can bring, so that we're not equally dismissive of the upsides as the blind optimists tend to be of the downsides.

Now one of my favorite phrases, that I only came across recently, is that you can't invent the ship without inventing the ship rack, which basically encapsulates this whole [01:02:00] idea. Because it highlights the in escape ability of downsides without making it sound like you shouldn't pursue the upsides. There are very few people, I would wager, who think that we shouldn't have invented ships because shipwrecks are so bad. But also it's really, really important to try to prevent wrecks as much as possible and to mitigate the harm they cause as much as possible when they do inevitably happen. As *The Onion* satirical newspaper wrote about the sinking of the Titanic, "World's Largest Metaphor Hits Iceberg. Titanic representation of man's hubris sinks in north Atlantic. 1500 dead in symbolic tragedy".

So, the question is just whether we're going to introduce new tech with the hubris of the builders of the Titanic and not plan for any downside because we don't expect them to happen. [01:03:00] Or do we move ahead with the modesty and, yes, the regulation that has pushed modern ship builders to have to plan for the worst.

That's going to be it for today. As always keep the comments coming in. I would love to hear your thoughts or questions about this or anything else. You can leave a voicemail or send us a text at 202-999-3991, or simply email me to jay@bestoftheleft.com. Thanks to everyone for listening. Thanks to Deon Clark and Erin Clayton for their research work for the show and participation in our bonus episodes. Thanks to our Transcriptionist Trio, Ken, brian, and LaWendy for their volunteer work helping put our transcripts together. Thanks to Amanda Hoffman for all of her work on our social media outlets, activism segments, graphic designing, web mastering, and a bonus show co-hosting. And thanks to

those who already support the show by becoming a member or purchasing gift memberships at bestoftheleft.com/support. You'll find that link in the show notes, along with a link to our Discord community, where you can also [01:04:00] continue the discussion.

So, coming to you from far outside the conventional wisdom of Washington, DC, my name is Jay, and this has been the *Best of the Left* podcast coming to twice weekly, thanks entirely to the members and donors to the show from bestoftheleft.com.