FRAMING:
Resolved: The most powerful generative AI models should, by law, be compelled to be open. (Luis/Casey's burden to prove)

RUN OF SHOW: (Assuming 40 minutes for panel)

[4 minutes] Moderator: Introduction and ground rules

[10 minutes] Opening statements (2.5 minutes each):
- Luis Villa, Co-founder and General Counsel, Tidelift, Inc.
- Paul Ohm, Professor of Law; Chief Data Officer, Georgetown University Law Center
- Casey Feisler, Associate Professor, Information Science, University of Colorado Boulder
- Blake Reid, Associate Professor of Law, University of Colorado Law School

[15 minutes] Q&A: Questioner (may direct questions to specific opponent or team):
- Luis
- Paul
- Casey
- Blake
- Luis
- Paul
- Casey
- Blake

[10 minutes] Closing statements (2.5 minutes each):
- Blake
- Casey
- Paul
- Luis

[1 minute] Moderator thank yous and wrap up

Guiding Principles:
- Have fun, inform the audience, and don't try too hard to win!
- Formulating your questions:
    - No "gotcha" questions
    - No questions that turn too specifically on research
- Issues that are nuanced and are "second order" issues, better relegated for later in the debate:
    - Copyright
    - The Waymo example

OLDER NOTES:

Framing Prompts

A: The risks of releasing powerful generative AI models to the public outweigh the benefits.

B: Generative AI models should be released openly

C: Government regulation of, and investment in, AI, should favor [not actively make illegal?] models built with open development practices, including multi-participant governance, transparency, replicability, and reusability.

Potential arguments

It would be useful to list arguments you would like to engage with, either affirmatively stating your case, or responding to something you've heard argued on the other side. This will help us develop the framing prompts better, and it'll help us avoid issues we'd rather just as soon avoid!

To encourage you to do this, Paul is going to put words in your mouth below, based on what he heard during the call! He is definitely going to misrepresent what you really meant, so please fix this!

Paul: These models are capable of doing great harm to innocent people, and once one has been released to the public, there is nothing we can do to prevent those harms.

Luis's response: We're not great at protecting people from these harms even with closed models!

BER: And we're never going to be able to stop these harms once the models' widespread availability drags down the political economy of regulation.

Blake: Allowing companies like Meta to release models like these makes it impossible to regulate their behavior.

BER: This is in two senses: first, it makes the regulatory enforcement job vastly more challenging by increasing the number of targets by orders of magnitude and introducing targets with affordances in terms of size, publicness, behavior, etc. that make them harder to regulate than big tech companies. Second, it undercuts the political economy of regulation by substituting "small businesses and entrepreneurs" for "Big Tech," even though the substantive case for innovation by small business is dubious.

Luis: The alternative to openness is gatekeeping, and gatekeeping concentrates power in the powerful and keeps us in this oligarchic market.

BER: One core barrier to entry in this market is having enough money to sustain liability for (potentially) illegally assembling sufficiently robust data sets. This isn't necessarily a dimension of competitiveness we should actually care about. And it's not just copyright; there's a good

chance that any kind of AI regulation, whether we're focused on discrimination and bias, privacy, accessibility, fitness for purpose, truthful advertising, etc. is going to disfavor small companies, because this technology is extraordinarily complex and difficult to use safely. (We've seen this in non-AI contexts, where small businesses tend to be quite terrible at generating non-innovation public goods.)

If we really care about competition, we should be focused on more obvious antitrust issues like Microsoft's de facto acquisition of OpenAI, Meta's and Google's ability to cross-subsidize AI R&D with surveillance ad tech monopolies, etc.

Luis: Clipper chip! We're terrible at controlling code. It'll just be an endless game of whack-a-mole, wasting resources on what we could better accomplish in other ways.

BER: A lot has changed in 30 years. The FTC now has tools like algorithmic disgorgement that are relatively easy to train on big companies.

Luis: Lots of great stories about what openness has done for the innovation economy.

Paul's response (channeling AI Now): This has nothing to do with "Open Source Software." It's a narrower and less generative thing.

Quick luis thought: much of this hinges on the regulability of open; are we all conceding too much to the historical unregulability of open? Is there an interesting framing around "can open AI be meaningfully regulated" or something along those lines? Thinking out loud as I sprint to something else; more later hopefully

Related: there's a communalist vision of open, and an … anarcho-libertarian one? query whether we'd be having a very different discussion if our society had actively chosen to foster the communalist one, instead of leaving it solely to the libertarians. (Ponder a publishing industry without libraries.)

BER: what do we mean by "open" here? Are we talking about an MIT-license-style, "we're giving you this model and you can do whatever you want with it" sense of open? Are we talking about a FSF-style "you may use this model in exchange for keeping your future work using the model open," legally-establishing-openness-as-a-requirement sense of open, which is really a form of regulation onto itself? (See Doe v. Github.) Are we talking about what e.g. Meta and OpenAI are actually doing, which is situating models as platforms *qua* instrument of control/gatekeeping, either through licensing (Meta) or app-store models (OpenAI)? Are we talking about the openness of the data sets? The trained models? Derivative models that are trained by users? APIs into the models? The openness of the corporate governance structure? (Perhaps in the ironic sense that OpenAI now means it by refusing to release corporate governance docs.)

"Openness" without constraints is just a meaningless declaration of goodness, a half-hearted rejection of "closed means bad."

Whatever the definition, I think it's likely to be contestable that open has yielded greater innovation than closedness. In reality, a lot of impactful innovation mixes open and closed metaphors.

OPENING: Luis first 2.5 minutes:

- we're being told this is the most dangerous and unpredictable technology since either the nuclear bomb or the printing press - by people who talk a lot about alignment but can't even align their own boards
- choice is between defaulting to fighting with tech oligarchs over every scrap of information for society, and defaulting towards visibility, regulability, and competition
- open is feasible in AI
    - OpenAI did it for a while
    - Llama *can* be truly open (but isn't)
    - Eleuther.AI and Mistral point the way to deep open
- open is the best way to get competition
    - only browser to take back market share from Microsoft: Mozilla
    - only OS to take back market share from Windows, Solaris: Linux
    - only mobile OS to take back market share from iOS: Android

- open is the best way to get societal understanding and regulation of new technologies
    - regulators aren't alone, helped by media and techies
        - eg Washington Post article on ChatGPT2+C4 - only possible because data set was open; with closed/non-transparent data set no opportunity for media scrutiny
    - helps keep even large companies honest
        - eg Chrome backing off of some bad behaviors when observed in the codebase

- open is pro-social
    - brand of open is anarchist and insular, but lots of success stories like AO3, Wikipedia, even [self-regulating deepfake communities]
- open is pro-efficiency
    - much research on how to run AI more efficiently, all driven by open researchers and desire to get out of the cloud

CASEY OPENING: Casey - TRANSPARENCY

- Researchers can inspect the underlying code to e.g. identify potential sources of bias and allows external parties to audit systems
- Allows for reproducibility, which also helps with benchmarks and standards
- Will make it easier to find security vulnerabilities, maybe even allow for a responsible disclosure regime

- More people able to look for harms is better
- Helps allow for traceability - knowing what's in the model and if YOU'RE in the model

CASEY CLOSING:

Casey - DIVERSITY & DEMOCRATIZATION

- More diversity of people contributing to AI is good
- People with different kinds of goals! (Not free as in beer or free as in speech but free as in gift?)
- Too much concentration of power is bad.
    - If development is ONLY driven by profit motives, we're in a really bad place.
    - Completely closed means lack of competition. (Competition can even lead to ethical practices as a market differentiator.)
- More, smaller AI models are better for the environment
    - if just Big Three clouds, little demand for efficiency since they'll just buy nuclear power plants
- Reduces redundancy by not having everyone rebuilding the same thing - including requiring more and more collection of people's content for training data without their consent
- Allows for education and skills development

LUIS CLOSING:

- moment calls for urgent optimism: open is the right way
- open will need to learn to meet this moment, no doubt about it
    - but open has been much better at organizational learning in the past 25 years than public companies, whose learnings in the past 25 years have mostly been about shedding their public goals (Google: don't be evil; OpenAI: public benefit lol)

Where can we talk about gates?

questions:

- do you think any level of US government would actually shut down OpenAI if it did something bad?

The case for open in AI

preface: what is open anyway?

- The case I'm making is for open as **commons-based peer production** (cf Yochai)
- not arguing for Meta-style faux-open (single-source, "no-fee to reuse")
    - if the means of production are still controlled by big tech and the commons only gets outputs, the benefits are much weaker (though not zero)
    - (aside for debate prep: I'm prepared to concede at the end that we don't know enough yet about whether commons-based peer production of AI is actually feasible, so it's possible that we'll find in a year or five that the benefits are small. Of course, given the other benefits to society of open, government should at minimum not accidentally crush the thing before it starts, and at best should invest in making sure it can succeed)
- some genuine confusion and disputation about what "open" as peer-production means in this moment
    - traditional definitions and legal tools (licenses) are recognized to be insufficient; new ones are not yet firmly in-place, meaning these debate terms have been set in large part by opponents rather than practitioners

The bad is not that bad

Important to ask "regulable compared to what"

- joke but serious: OpenAI can't even align its board (a well-known and well-studied technology), and we're supposed to believe they're going to align AI?
- if the Ohm and Reid get to argue that the government will successfully regulate Meta and OpenAI (which they have not yet done to date, despite, respectively: genocide, and rampant flaunting of California non-profit law and federal copyright law) then I get to live in a fantasy-land too
    - "Self-driving cars" are AI systems that *have killed multiple people, have designated regulatory authorities, and yet no effective regulation*, why do we think LLM regulation is going to go any better
    - deepfakes have been possible for a long time, with non-LLM techniques, and yet essentially no prosecutions 2021 survey with few results. Let's *try* to regulate outcomes before preemptively destroying a general-purpose technology?

CBPP is regulable

but even putting aside the question of "regulable compared to what", open is regulable

- stereotype of open is that it is anarchic and unregulable; this is incorrect
- as Wu/Goldsmith laid out c. 2005, tech lives in the real world; so open (just like the web) is reachable in a variety of ways; levers for open include:
    - employers
    - platforms (eg GitHub)
    - simple moral suasion (much easier to talk a community into doing the right thing than talking the board of a publicly-traded company into doing something unprofitable and not legally mandates)
    - investment into research/prevention (government should be funding mass research into auditing, fine-tuning for safety, and publishing all of that)
- existing examples:
    - "stewards" in new EU CRA
    - ITAR/export control
    - community-level CoCs/self-censorship (eg, Wikipedians handling GDPR; Widder on deepfakes: https://davidwidder.me/files/widder-ossdeepfakes-facct22.pdf)

perfect regulation to prevent CBPP would require authoritarian tech governance

- no way to prevent open AI without *all of*:
    - censorship of academic research into more efficient training and inference
        - (LV doesn't actually think code is speech in a First Amendment sense, but LV definitely thinks publishing research into AI efficiency is speech)
    - hardware-level kill-switches: Clipper Chip, but with ability to shut down computing altogether, not just monitor it
    - network-level censorship: Great Firewall of China to prevent dissemination of models
- so "benefit" of open AI is "we don't accidentally build 1984 in an effort to stamp out open AI"

Western Democracies are better at open than competitor states

Risk of authoritarian governments developing a *lead* in AI because of open is overstated, because the skills/resources necessary to be good at CBPP are still overwhelmingly western.

- examples:
    - Linux kernel still overwhelmingly developed in the west despite being copyable for 30 years
    - Wikipedia vastly more compatible with Western democracies than with authoritarian approaches
    - Android *maybe* best counter-example: developed primarily in the US, used widely by Chinese phone manufacturers.
- worst geopolitical outcome: China and other repressive governments do open AI (which they're already starting to do), it takes off for all the reasons open has taken off in the rest of tech, and the next "Linux kernel" all of tech depends on is controlled by China, rather than American companies. IOW, we accidentally get TikTok instead of Android.

the good is very good

CBPP AI provides basis for successful regulation

- transparency
    - open hard to audit, but it's at least possible
        - if we want our societies (including media and government) to be able to inspect AI, it must be open
        - compare exposés on C4 data set and LAION to Nate Matias' work on how private social networks have made research impossible, or the ongoing sagas of seeking DMCA exceptions for research and security work
- competition
    - all competition in the modern tech industry starts from a basis of billions of person-hours of pre-existing open source code
        - banning open AI techniques will grant a permanent monopoly to current tech leaders
    - "forking" right is a powerful counterweight to enshittification

CBPP provides vast economic benefit

- new HBS study excludes most valuable parts of open source software and still estimates $8T valuation
- this analogy is a total stretch but banning open AI would be like saying "cars are dangerous" (good) and therefore we must make all roads toll roads (bad)

CBPP is deeply humane/human (admittedly imperfect but...)

- communities are not magic, but deeply powerful
    - Wikipedia
    - AO3
    - “real utopias” of Erik Olin Wright
    - (freedom of association?)
- supports labor
    - part of why tech labor is the most powerful labor force in the world is because re-use of open tech promotes labor mobility

Selected Citations on Fair Use and Non-Human Copying

Authors Guild v. Google, 721 F.3d 132 (2nd Cir. 2015), cert denied. District Court granted summary judgment in favor of Google, dismissing the lawsuit and affirming the Google Books project met all legal requirements for fair use. The Second Circuit Court of Appeal upheld the District Court's summary judgment in October 2015, ruling Google's "project provides a public service without violating intellectual property law.”

Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701 (9th Cir. 2007). Ninth Circuit held that image search engine's use of thumbnail was a fair use. Copying was fair use because"highly transformative."

> We conclude that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case. … We are also mindful of the Supreme Court's direction that "the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use."
>
> See, e.g. Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003). (same as Perfect 10).

Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991). SCOTUS denied copyright protection to a "white pages" phone book (a compilation of telephone numbers, listed alphabetically); rejected the "sweat of the brow" doctrine.

Naruto v. David Slater et al.,888 F.3d 418 (9th Cir. 2018). Works by animals not subject to copyright protection. Monkey selfie case.

A.V. ex rel. Vanderhye v. IParadigms, LLC, 562 F.3d 630 (5th Cir. 2009). Machine copies of copyrighted work for use in plagiarism detection software is fair use using traditional four factor analysis.

Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992). Reverse engineering of code not infringement.

Bill Graham Archives v. Dorling Kindersley Ltd., 448 F.3d 605 (2d Cir. 2006). Recontextualize a work by surrounding it with other expression not infringement. Grateful Dead case.

White Smith Music Pub. Co. v. Apollo Co., 209 U.S. 1 (1908). Copying of sheet music into player piano rolls not infringement (under 1897 Act).

> These perforated rolls are parts of a machine which, when duly applied and properly operated in connection with the mechanism to which they are adapted, produce musical tones in harmonious combination. But we cannot think that they are copies within the meaning of the copyright act.
>
> It may be true that the use of these perforated rolls, in the absence of statutory protection, enables the manufacturers thereof to enjoy the use of musical compositions for which they pay no value. *But such considerations properly address themselves to the legislative and not to the judicial branch of the Government*. As the act of Congress now stands we believe it does not include these records as copies or publications of the copyrighted music involved in these cases.

17 U.S.C. § 117 allows for software back-ups.

James Grimmelmann, Copyright for Literate Robots, 101 Iowa L. Rev. 657 (2016). Excellent discussion.