# **Mirror, Mirror Full Transcript**

## **Welcome to Optopia!**

Hey there! You made it! Welcome to Optopia! [1]

It's the land of algorithm-driven utopia. Remember all those crazy scientists talking for decades about creating artificial intelligence? Well, this is it! We all laughed at them and said it was impossible to do [2], but you know what...They were right. They did it. And now they just sit back and relax while their artificial replicas do all the work. Look at this guy, he just published a new paper, all while sipping a nice glass of wine.

I know what you’re thinking...Is this yet another whitewashed Hollywood production? Where are all the women and people of color? If Technological Supremacy lies at the summit of the AI mountain that humanity must scale at all costs, then our preparation for the climb and the equipment available to us will make all the difference. Based on our current trajectory, not everyone will make it.

## **Part 1. Rockfall: What work do we fund?**

AI is the shiniest toy on the block and so, inevitably, all the money magpies have come flocking. However, beyond the usual slew of popular applications of this technology (such as Vision and Language Modelling), the money seldom trickles down.

For example, take Human-Computer Interaction (HCI). This work focuses on foundational principles of the digital age, such as Equitable Access, and yet it seldom sees the kind of economic backing or media coverage as ML does. Let’s give HCI a moment in the spotlight, shall we?

“The power of the web is in its universality. Access by everyone regardless of disability is an essential aspect” -Tim Berners-Lee

Did you know? 15% of the world’s population experience some form of disability- visual, auditory, motor or cognitive [3]

So, what is digital accessibility? This volume is about ML and data, so you’re probably imagining robotic arms trained on hundreds of thousands of runs of simulated movement and customized to the wearer’s measurements and motion of action. Or ground-breaking, hyper intelligent goggles for the blind that collect the distorted image from the wearer’s retinas and reconstruct it to a sharp, 10800000 p image for superhuman vision. Or how about a fully automated, hyper-sensitive robotic armor that self-learns and auto-navigates for the physically disabled? Maybe, if Elon Musk decided to get into the accessibility game…

In our reality, digital accessibility is focused on making sure web platforms are easily navigable and usable for people with any kind of disability. It is this very work that makes sure that the image you just posted on Instagram has captions, so that the blind users of the platform can also partake in your triumph over that sourdough recipe. Or when you drop your new tutorial video for all one squillion of your subscribers to enjoy, it is this work that converts your vocal pearls of wisdom into text for your deaf followers.

Accessibility needs to be a fundamental design principle for building websites and software. But in our quest for Optopia, it is usually overlooked. Without a11ies [4], the demographic that was holding onto the Accessibility rope are now cut off.

Let’s get rid of the Magpie Mentality? For your next fun data science project, instead of some community-overfitted Image recognition challenge, maybe choose an open problem in digital accessibility, such as automatic video captioning? Then hopefully one day there will be “No More CRAPtions” [5]

## **Part 2. Ghosts in the Shell****: Who are we building models for?**

### We haven’t yet figured out how to make existing digital platforms accessible to everyone, yet we’re already jumping to forge a new “intelligent” class of web applications. We’re so caught up in the “how” (using ML/AI/DL/DS !!!) that we forget to ask, “for whom’’?

When platforms are not designed for everyone, they give off the stench of “encoded inhospitality” [6]. Seemingly innocuous things such as pop-ups and expiring forms on websites completely hijack the online experience of users with disabilities who rely on screen readers. As accessibility advocate Chancey Fleet puts it most eloquently [6]; “Akin to how a ghost writer is the person who is paid to compose a novel that someone else could not be bothered to write themselves, Ghostwritten code is software that the organization has offloaded on programmers to design for users that the company cannot be bothered to engage with or employ themselves.”

These ghosts are making their way into data-driven products as well. Take the infamous facial recognition software that has been the all over the news recently. Racial injustices are problematic enough, but have you considered how these models discriminate against Black disabled people? As disability rights advocate Haben Girma explains [7], “My eyes move involuntarily, each one swinging to its own music. They’ve danced this way for as long as I can remember.” How well do you think facial recognition would perform on Black blind people? Having been trained on the facial dynamics of sighted white people, facial recognition technology peddles an ableist and racist narrative. The atypical, asymmetric mechanisms of the eyes of some blind people are perceived as abnormal, anomalous and threatening by these systems.

How is it that we can forget to consider entire demographics while designing products? Take Facebook’s “real name” policy that indiscriminately targeted Native Americans [8]. The largest social network in the world sure overlooked the cultural and linguistic differences in names across the globe. And ended up deploying a bigoted algorithm that blocked users whose names did not conform with the western archetype of names. In addition to completely overlooking who we are building a product for, have we altogether done away with the question of whether a certain product \*should\* even be built?

Sure, you have several hundred terabytes of user data and a fleet of engineers waiting to dip their hands into the ML pie, but is your product a solution to an actual problem, or is it simply solutionism?

## **Part 3: The Poisoning: What problems are we trying to solve?**

Technology is supposed to drive innovation and move us towards a more sophisticated and advanced future, right? And so, when the new flavor of technological advancement comes to market, what else must we do but eagerly lap it up? Well, if there’s any mention of “intelligence” on the product being handed to you, you might not want to drink that. It’s snake oil! [9]

What is AI-snake oil? Snake oil is the mystical substance that is created by taking equal parts media hype and public misinformation and stirring them into a potion, with an irresistible label that screams “data” and “intelligence”. And after years of experimentation, the tech industry has finally perfected the recipe!

Developments such as AlphaGo (the Go playing AI) and Shazam (the music recognition app) are indicative of genuine scientific progress and do demonstrably more good than harm. Why? Because the rules of Go don't change whether the player is male/female, black/white, rich/poor!

Perception tasks, such as facial recognition, that are intertwined with the social, political and cultural underpinnings of the data on which they were trained, are far more toxic.

Things start to get really toxic in settings such as hiring, moderation of hate speech or allocation of grades [10], when we needlessly try to impose objectivity (fit a mathematical function onto the data) on human judgement, which is inherently subjective. We get really creative with what we think we can achieve with technology when we start predicting social outcomes using algorithms, such as COMPAS for Criminal Sentencing [11].

We look around and see the hardest problems known to us and decide that since we cannot solve them, we must instead get a machine to do it for us. But do you know why these are the hardest problems to solve? Because these are systemic issues that have been slowly stewing for centuries over. With a dash of historical context, a sprinkle of culture and a generous heaping of race, gender and class politics. All compounding into a stew complex broth of entropy. Expecting a machine to take a whisk of this stew and be able to predict the future is just fundamentally dubious.

## **AI Circus**

Underneath all the bells and whistles of this larger than life spectacle is a dangerously high-risk game that we don’t even know we’re a part of! Welcome to the AI Circus!

The balancing act between making a model simultaneously accurate, fair and feasible is really a spectacle for all to see! Take AI for hiring. If a company indulges in discriminatory hiring practices for years on end, predictive models that automate such decisions will favor the same pedigree of candidates that were historically hired. An extremely “accurate” algorithm will faithfully replicate the discriminatory behavior of its human trainers.

Counteracting data bias by enforcing a notion of “fairness” in prediction comes at the cost of model accuracy -- when accuracy is measured on the biased training data. Why? Because an algorithm that is extremely accurate but trained on biased data will be discriminatory by construction!

This problem gets harder because ML models are opaque. We have limited understanding about how a prediction was made.

Sometimes the data is so terribly biased, that in order to deliver fairer outcomes, we need to go back and collect a whole new sample. This might not be feasible in all circumstances and so companies have to take a stand on which metric they value most: Feasibility or Fairness? Do they push for a fair but expensive algorithm or settle for the “most fair” algorithm that they can afford at the least cost?

Then there’s the Pyramid of ML Scholarship. At the very top of the pyramid sits (precariously) our MO of SOTA chasing. SOTA or State of The Art refers to the latest reported metric on some task. SOTA chasing is about outperforming the competition on that benchmark, even marginally. We create a benchmark dataset and then declare a metric, usually accuracy, by which we will measure success. Now, project after project and paper after paper sets out to attain that 0.01 increase in accuracy to be deemed “publishable”, all the while taking it for granted that accuracy is even the right metric against which to measure progress.

Why is this a problem? Because SOTA chasing assumes that the benchmark is even worth chasing! That the dataset is representative of the population. And that a marginal accuracy improvement makes a difference.

A natural shortcut in this game for SOTA-premacy is to just use a bigger dataset. For all you GPT-3[12] fan boys and girls out there, this is exactly what you’ve been raving about: The sheer, unfettered access to a gargantuan dataset and compute (or moolah to pay for compute), to create models that beat the state of the art and give the illusion of scientific progress.

Sure, there are those folks in the community who are thinking deeply about problem formulation, real world impact and scientific rigor. Unfortunately, deep, thoughtful work of this kind is just not glamorous...and so, when the curtain falls, it isn’t these researchers you are applauding.

How come these folks never take center stage? Well, it’s partly because, like in every other domain, the rich just keep getting richer. The set of researchers who debunk societal harms of technology are likely to be from the same demographic that will be most deeply affected by those very harms. And this is never the majority.

If our scholarship is a reflection of our ideas, then we cannot afford to censor or erase the voices of entire demographics. If our products are a reflection of the problems that we are trying to solve, then we cannot build solutions that help one stratum of society and cause extensive damage to another.

The AI circus has already added some exceedingly grotesque spectacles to its line-up; Wrongfully sending a man to prison [13], Massive differences in gender identification for different skin colors[14] (can you imagine the mayhem that such a system would cause if used on persons who do not conform with binary, heteronormative gender allocations?), Discriminating against women in hiring[15], in allocation of credit limits[16] … the list just keeps getting longer. Who else needs to go up on this dreadful line-up before we stop clowning around, once and for all?

## **Techno Optimism vs Techno Bashing**

But before you reach for your smartphone to get on Twitter to rage against the AI Machine or join the ranks of the Techno Bashers, stop and look around.

It really is a Mad world. And it’s driving us particularly crazy because we’ve become so used to seeing the world in extremes. You can either be a Techno Basher or a Tech Optimist and if you are one you CANNOT and SHALL NOT sympathize with the other side. Give AI the reigns to run the entire world or pile it all up and throw it all out. We’ve become so used to ‘hulking-out’ at the first sign of disagreement on social media, that the entire discourse around tech, and AI in particular has been completely stripped of subtlety. It's 2020. How is it that we can appreciate a comedic take on Hitler and the Nazi youth camps [17], without getting our feelings hurt but we can’t have one discussion about bias in the data without it immediately devolving into blows. Maybe we need to stop reacting to everything we read and instead take a moment to re-read, think deeply and then respond.

Because the truth is, we can't really do away with these discussions on social media if we want to invite the general public to partake in the discourse. But when a discussion devolves into gaslighting and personal attacks, it really doesn’t benefit anyone. The extant celebrity culture and internet trolling that shrouds scientific discussions needs to go, or else we just end up throwing the baby out with the bath-water. So, what do we do about this? Well, for starters, can we get some nuance with our discussion meal, please!?!

Here is a more nuanced take on whether AI leads to a utopia or to a dystopia.

For starters, there is rarely an objective ground truth! More often than not, the efficacy of a model depends upon the context for which it was designed. The ground truth that we pretend exists, and against which we measure model accuracy, is just the clothes that the ML emperor is not wearing. The engineering mindset is to take class labels as gospel and blindly optimize for them. But class labels are just proxies for underlying social phenomena and no amount of mathematical formalization will turn social constructs into objective truths.

The reality is that all models are wrong. Some models are useful! In this art gallery, each painting depicts an apple. But only one of them is potentially useful as a real-life apple detector. We often find it hard to judge which model is most useful, because that requires deep domain expertise. We have been dangerously conflating expertise in training and deploying a model with domain expertise. Instead we should acknowledge the limitation of our expertise as Scientists and Engineers and invite the true domain experts to come to the table.

Some contexts are inherently difficult to build for. We have the tendency to summon our Deep Learning hammer and go about nailing square pegs into circular holes. Unfortunately, the most promising results that you read about were obtained on toy problems within experimental set-ups and are not designed to scale to the real world. The world is a complicated and messy place and the limited performance of existing models reflects that. Improving the generalization ability of models is a hot area of research and maybe we’ll get around to creating models that can perform reliably in contexts that they did not encounter during training. But we aren’t there yet.

The overwhelming majority of problems that plague AI today are not because of just the data or just the algorithm in itself, but because of one critical confounding factor that we keep overlooking: the world. Data is a mirror reflection of the world [18]. When data is biased, that reflection is distorted. There are several possible explanations for this.

The mirror could be distorted: We could be collecting the wrong data, or looking at a non-representative sample. To fix this type of bias, we can attempt fixing the mirror to collect better and cleaner data. But there is also the possibility that the mirror is perfect and the world itself is distorted. We tend to under-appreciate this possibility because we instinctively compare the reflection (data) with how we want the world to be, rather than with how it actually is!

Based on the reflection, and without knowledge or assumptions about the properties of the mirror and of the world it reflects, we cannot know whether the reflection is distorted, and, if so, for what reason. Data alone cannot tell us whether it is a distorted reflection of a perfect world, or a perfect reflection of a distorted world, or whether these distortions compound. Changing the reflection does not change the world. We’ve come up with better ways to collect data, clean it and remove some of its bias. But all these fixes are applied on the mirror or on the reflection, and they do not propagate back to change the world. The underlying societal inequities that give rise to discriminatory outcomes remain intact if we only intervene on the data. Hence, our intervention should expand beyond technological solutions, towards systemic change.

## **Culpability and the Role of Regulation**

Prediction is difficult, especially about the future! [19] When things (inevitably) go wrong, who is responsible? It cannot be the algorithm. But given the many stakeholders who play a part in the creation and operation of a software product, how do we determine which human is culpable? Are they all? I know what you're thinking…I see where you’re going with this...you’re not seriously going to get into regulation now, are you? Well...time to remind you of our recommended approach to thinking about AI. Remember. NUANCE?!

Silicon Valley would have you believe that technology needs to be allowed to run free. Regulation is a catastrophe of cosmic proportion and would be the end of the Internet and, by extension, of innovation and progress. The fact of the matter is, we put our children on the AI hype-bike and sent them off at full speed. We were too brash in our rapid adoption of AI and it has led to some terrible outcomes with very real impacts on people’s lives. And so, while tech companies and their celebrity CEOs protect their interests by bad mouthing regulation, there’s really no excuse for the general public to buy into this narrative and be complicit in the vandalism of our moral social fiber. We need to come to an agreement on how to go about regulating technology, and so we must start educating ourselves and partake in this lofty enterprise in good faith. It’s time to consider other parenting styles!

**Precautionary**. Think of the old adage “It’s better to be safe than to be sorry”. This principle calls for caution in situations of uncertain harm, ie. risks that have not been scientifically studied yet. A common criticism of this approach is that it is “paralyzing” and “self-cancelling” since any new technology in its early stages of adoption would have risks that cannot be accounted for.

**Risk-based**. Under this paradigm, we regulate based on known risks and model the likelihood that these risks will lead to harm. A promising approach is Algorithmic Impact Assessment (AIA) - a framework that helps understand and reduce the risks to individuals and communities. Under AIA, the likelihood and severity of harm determines the level of oversight. The higher the risk of harm, and the more significant the harm itself -- the more stringent the oversight requirements. And the less autonomy is granted to the automated system: A human must be brought into the loop to take responsibility for impactful decisions. AIA will only work if the risks are known. This gives each and every one of us the opportunity to be a part of the change! Now’s the time to get involved in public consultations, to make your concerns heard!

If we want our attempts at regulation to be truly effective, we need to reconcile some inherent disagreements between tech and law. For starters, how do we ensure the law keeps up with a rapidly evolving socio-technological landscape? Another major problem is how do we regulate? Notions such as fairness, accountability, interpretability, etc. have become the poster children for AI policy, but they still don’t have universally accepted technical manifestations. Why? Because ambiguity in definitions is an intentionally wielded tool that allows for interpretive and contextual readings of law, but the very same ambiguity is catastrophic for tech, which relies entirely on mathematical formalizations that can be written into code, and for regulators who need precise definitions to build rules and policies. To come up with good definitions, we need examples of systems that are used today!

Take the NYC Automated Decision Systems (ADS) Task Force, the first of its kind, envisioned to be the beacon for transparency and expert insight into the use of algorithms to aid decision-making by city agencies. [20] But they didn’t get very far. A good definition was lacking, as were examples. What is an ADS? A calculator is not an ADS. But a system that collects data, builds a model, and then enacts policy that impacts people’s lives -allocates school budgets, or offers homelessness assistance, or matches students with spots in high schools certainly- certainly is.

## **Revisiting Optopia**

With all of this in mind, let’s revisit humanity’s quest for Optopia. If we discard entire societies and demographics on the way, and completely overlook societal problems that render algorithmic interventions futile, is the trek still worth pursuing? Maybe instead of a power-trip in the name of a technological mission (when did we all agree that human intelligence is worth replicating?), we should focus on harnessing the power of Learning Technologies to positively impact people? And not one, affluent, highly influential demographic of persons, but truly all persons, of all social strata, classes, genders and races. Maybe what we need instead is to ground the design of AI systems in people.

Using the data of the people, collected and deployed with an equitable methodology as determined by the people, to create technology that is beneficial for the people.

## **Cite As**

Falaah Arif Khan and Julia Stoyanovich. “Mirror Mirror”. Data, Responsibly Comics, Volume 1 (2020) <https://dataresponsibly.github.io/>comics/vol1/mirror\_en.pdf

## **About Data, Responsibly Comics**

Falaah is a scientist/engineer by training and an artist by nature, chasing a passion for building Robust and Ethical ML all the way from industry to academia. In the face of having to incessantly remind everyone around her about the limitations of current ML capabilities, Falaah started MachineLearnist Comics, a collection of scientific comics about the current AI landscape.

Julia is an Assistant Professor of Computer Science and Engineering and of Data Science at NYU. She is passionate about responsible data science and leads the “Data, Responsibly” Project, the latest offering of which is the inimitable, interdisciplinary course on Responsible Data Science.

With the undecipherable alchemy that is grad-school admissions, the cosmos brought these two creative minds together and thus was born: Data, Responsibly Comics!

Whether you’re a student, unsure about where to get started in the panacea of ML scholarship; or an educator, looking for a fun new pedagogical instrument for your students; or a practitioner, looking for some relatable content about all the idiosyncrasies of the current AI landscape; or just a good ol’ John/Jane Doe who likes to read comics and is intrigued by the prospect of a long form scientific volume,  
Data, Responsibly Comics are for you!

## **References**

[1] [https://mrtz.org/gradientina.html#/](https://mrtz.org/gradientina.html)  
[2]<http://www.hutchinsweb.me.uk/MTNI-11-1995.pdf> .   
[3] <https://www.who.int/disabilities/world_report/2011/report/en/>  
[4]<https://www.a11yproject.com/>  
[5] [http://nomorecraptions.com](http://nomorecraptions.com/)/  
[6] <https://datasociety.net/library/dark-patterns-in-accessibility-tech/>  
[7] <https://twitter.com/habengirma/status/1278035954628915200>  
[8] <https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy>  
[9] <https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf>  
[10] <https://sarahwyerblogs.wordpress.com/2020/08/17/classed-outliers-the-algorithmic-divide-in-plain-sight-a-levels-and-highers-divide-the-uk/>  
[11] <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>  
[12] <https://github.com/openai/gpt-3>  
[13] <https://www.nbcnews.com/business/business-news/man-wrongfully-arrested-due-facial-recognition-software-talks-about-humiliating-n1232184>  
[14]<http://gendershades.org/>  
[15] <https://in.reuters.com/article/amazon-com-jobs-automation/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idINKCN1MK0AH>  
[16] <https://www.nytimes.com/2019/11/10/business/Apple-credit-card-investigation.html>  
[17]<https://www.imdb.com/title/tt2584384/>  
[18] <https://dataresponsibly.github.io/documents/mirror.pdf>  
[19] <https://quoteinvestigator.com/tag/niels-bohr/>  
[20] <https://www1.nyc.gov/site/adstaskforce/index.page>