## Hi Matt,

In this letter, I'm representing a group of Clarifai employees who are looking for clarification on our values, since so much has changed in the last few months. The people I'm representing in this message are all invested in Clarifai's success as a company, and only want to be sure that we are working towards a shared definition of progress, as it's stated in our new company mission. We have serious concerns about recent events, and are beginning to worry about what we are all working so hard to build. I'll begin by sharing our motivation and concerns, and there's a long list of specific questions at the end.

Lately, tech companies have been in the news about the ethical implications of machine learning quite a lot. Google employees signed a petition asking the company to decline to participate in Maven. Amazon employees asked Amazon to stop serving ICE. I do believe that any company has the right to police itself and to do business within the confines of the law and according to the content of their own values. It's up to us as employees to decide whether those values are also ours.

And yet, in conversations I've had with you and with other members of the executive team about our position on ethics in facial recognition, there have been mixed messages, and our values seem to be changing every day. At first, we refused to take on projects that involved pornography or military work because they didn't improve life. Now, 75% of our revenue comes from the Department of Defense. New executives have indicated that there's no project we would fail to consider if the price is right, given our lack of growth and product-market-fit.

Google and Amazon employees' open letters have described some of the more obvious applications of CFR that are terrifying (mass surveillance, social credit scoring, political oppression/registration), but there is a fourth elephant in the room that few are addressing: autonomous weapons. Given our focus on DoD/military contracts, and recent conversations with Cellebrite, it's even more important for us to ask: will Clarifai participate in projects that might lead to large scale warfare, mass invasions of privacy, or (perhaps a bit dramatically) genocide?

Because that's the fear behind autonomous weapons, after all. That we open Pandora's box, and that there will come a time when we want to close it, but can't. That's not to say that the Terminator is knocking on our door tomorrow. But this fear is deeply embedded in our culture. Asimov wrote about it extensively. Black Mirror did an episode on the topic. Thousands of researchers have signed an oath never to work on autonomous weapons. Britain vowed not to pursue them (mostly). Ethicists are writing about the issue every day. We in the industry know that all technology can be compromised. Hackers hack. Bias is unavoidable. Ordinary people now have access to advanced technology that can be combined with a little ingenuity and know-how to achieve big things. Consumer drones with autopilot already exist. And that's why it's concerning that certain executives on the team have indicated in private conversations that autonomous weapons would be perfectly ok for us to build.

How else would this notion of autonomous weapons be achieved if not by some combination of drones, the DoD, aerial photography, object detection, local SDKs, and CFR? It's time we stop pretending that these fears aren't justified when looking at the technology that exists today. The technology to make [very basic] autonomous weapons is just around the corner. In fact, it's probably already here.

And, as if on cue, the DoD is about to revise their position on the issue of autonomous weapons by June:

https://m.govexec.com/technology/2019/01/pentagon-seeks-list-ethical-principles-using-ai-war/1 53951/?oref=ge-android-article-share

We are doing exactly two things for Maven now (aerial photography and object detection), that could be used in autonomous weapons, where they claim it's not for "offensive" use. However, when the government engages with contractors for large projects, those projects can get broken up into smaller pieces where no single company has a complete view of what they are building. When my grandfather was building the Pentagon as an electrical engineer, he didn't know what he had built until it was unveiled to the public. This logic holds true for military vendors today.

With respect to military contracts, is it even possible for us (or any private sector company) to know whether our aerial photography object recognition will be combined with drones that have the power to make a lethal decision without a human in the loop?

Microsoft thinks we should be regulated when we build things as powerful as CFR. I'm not convinced that I agree, but my thoughts on the matter depend largely on your response to this inquiry. Regulation slows progress, and our species needs progress to survive the many threats that face us today. GDPR was hell to prepare for, and it took precious time away from our then-small team. Technology regulation is notoriously ham-handed when it's made by people who don't understand it. GDPR exists because the tech giants violated the public trust too many times, so the government stepped in. We need to be ethical enough to be trusted to make this technology on our own, and we owe it to the public to define our ethics clearly. We should be the ones who set the standard, not the ones who cross the line.

But maybe there are some narrow, specific things about CFR that do deserve regulation? Like bias. We very nearly went live with a version of CFR that had 10% more errors when predicting on people with dark skin. If this technology had been sold to a government for security purposes, it would certainly have a negative effect on all the dark-skinned people who would be disproportionately mistaken for criminals.

And finally, the last questions we have relate our philosophy on data collection. Because the way we treat consumer data is an important part of our ethical framework. It demonstrates how far we are willing to go in the interest of profit, at the expense of privacy and consent. And just this month, we've been asked to download data from cameras whose owners haven't given

consent at all (Insecam), and a few other sources that may walk a legal line but are sketchy at best. There are even rumors going around that the photos in the dataset used to build the general model were stolen from a stock photo site.

All of these things combined with the change in plans regarding our board ethics committee lead us to ask the following questions:

- Will Clarifai continue selling our facial embeddings product through the self-serve platform without any ethical oversight into clients' applications or use cases?
- Will Clarifai vet every large-scale potential customer of CFR with a team of people that includes non-technical and non-executive members, and publish the findings of this team to the broader company every time?
  - Who would be on this team?
  - What would be their criteria and guidelines for making such decisions?
- Will Clarifai vet every military contract to ensure that our work does not get used in the creation of autonomous weapons?
  - How will you approach this endeavor, understanding that the government may try keep this information from us intentionally?
- Will Clarifai sign the open letter, guaranteeing that we never intend to work on autonomous weapons, even if a large enough contract comes along?
- Will Clarifai promise not to sell CFR (or any similar technology that has the potential to be used for oppression) to any totalitarian or otherwise oppressive government for any purpose ever?
- Will Clarifai promise not to sell CFR to any US entity who does not first hold a vote to obtain public consent for the use of that technology for that purpose?
- Will Clarifai promise to evaluate every algorithm we build for racial/age/gender/disability bias as part of our process, and not just as an ad hoc afterthought?
  - Who will define and own this process?
  - What error thresholds will be sufficient for us to launch and sell technologies we know to be biased?
- Will Clarifai promise never to use illegally obtained or otherwise ethically dubious data?

There are those of us who have been with you long enough to remember the original Clarifai mission of improving life. We understand that our financial situation has changed, and we all want Clarifai to succeed. But, we should not be willing to risk the safety, privacy, or survival of humans globally just so that Clarifai can have an IPO.

I hope you know that the people asking you these questions are people who have thrown their lives into helping you build a company that makes the world a better place. We aren't asking to be presumptuous or impertinent. We are asking these questions because we hope to find some common ground. We are looking for a reason to stay with you, not to leave.