**\*Please make a copy of this document and include this in your GitHub repository for your submission, using the tag #AndroidDevChallenge\***

**Tell us what your idea is.**

*Describe in 250 words what the feature or service will do and how you’ll use Machine Learning to push the bar:*

8 out of 10 millennials take illicit photos.

As the next generation of 300 million young adults from emerging markets connect to the internet, they are experiencing world wide web and its nuances for the first time. For such young adults, every 1 in 1000 (about 300,000) experience some form of non-consensual phone hacks, private photo leaks and issues like revenge porn at least once in their lifetimes. In contrast to developed markets which have strong and effective legal recourse and awareness around consent and privacy, such incidents in emerging markets go unreported, have huge social implications and can completely destroy the lives of the people involved. Such a phenomenon occurring at this scale is totally unacceptable! It’s time we come up with a solution.

We believe that this problem can be prevented directly at the source: the end user’s phone, by using smart detection, classification, management and security of user’s private device content using on-device AI/ML solutions.

Need for mobile-first on-device solutions:

-95% of user images/videos is created and consumed on mobile phones.

-Sensitive content \*MUST\* remain protected locally on-device and not stored on any organization’s servers.

-For internet users in emerging markets, it is impractical and expensive to upload all their image/photos using internet data to cloud for the sake of classification/detection/protection.

With >90% of mobile OS market-share in emerging markets being Android, it is imperative that we need to have Android-native solutions.

Among many, some solutions that we have come up with are as follows: Auto-blurring of elicit images/videos on phone if being used by someone else other than the owner, auto-hide illicit content using Steganography, smart file-system based prevention of external sharing, auto-encrypt content when phone is passcode-locked etc.

We believe that with the help of Google’s AI/ML capabilities to identify, classify, identify and secure sensitive images/videos on-device, we can build innovative solutions that address the required challenges. Potentially these solutions can also be plugged into multiple Google products such as Photos, Android Go, Android One, Files Go (as well as Images and Lens).

What have we built so far:

We, a small team of CS engineers based out of Stanford (and University of Toronto), have built a prototype for an on-device (no internet required ever) image classifier and similarity detector that can classify medium resolution images in the order of 10K-12K within 5-7 mins with an accuracy of 95% on a typical mid-end Android device.

Privacy is a fundamental human right. With GDPR and other new privacy laws being currently written around the world, such privacy-focused Android-first solutions not only provide Google an opportunity to create an industry benchmark around data privacy protections around the world, but also safeguard the lives of thousands of new internet users around the world.

**Tell us how you plan on bringing it to life.**

*Describe where your project is, how you could use Google’s help in the endeavor, and how you plan on using On-Device ML technology to bring the concept to life. The best submissions have a great idea combined with a concrete path of where you plan on going, which should include:*

* *(1) any potential sample code you’ve already written,*
* *(2) a list of the ways you could use Google’s help,*
* *(3) as well as the timeline on how you plan on bringing it to life by May 1, 2020.*

Adding to our previous answer:

1>We have a prototype ready with ~100K LOC and can open-source the repo upon request/NDA. We have shared a small sample code snippet in the GitHub repo.

2>Integrating On-Device ML can dramatically improve the scope and performance of our current non-ML based technique and enable us to tackle more user cases in a better way. Secondly, potential integration with Google product such as Photos, Android Go can help us provide our visual privacy solutions to real users at scale.

3>Continuing to work on our current working alpha, we plan to further add ML capabilities, work on the UI and launch early next year. Here’s a short timeline:

Prototype - Built.

Alpha release - Already released.

Beta release - Feb 2020.

Advanced ML integration - March 2020 (requires Google support)

Early production launch - April-May 2020.

**Tell us about you.**

A great idea is just one part of the equation; we also want to learn a bit more about you. Share with us some of your other projects so we can get an idea of how we can assist you with your project.

We are a small team comprised of computer science grads and we love engineering novel solutions. We have been a part of multiple product teams built ground up and have a collective experience of over two decades. We have been affiliated with Stanford, University of Toronto, IITs, Cisco, Intel, IBM and multiple early stage startups. Currently we are based out of Stanford Venture Studio and exploring opportunities at the intersection of privacy and digital media.

**Next steps.**

* Be sure to include this cover letter in your GitHub repository
* Your GitHub repository should be tagged #AndroidDevChallenge
* Don’t forget to include other items in your GitHub repository to help us evaluate your submission; you can include prior projects you've worked on, sample code you've already built for this project, or anything else you think could be helpful in evaluating your concept and your ability to build it
* [**The final step is to fill out this form to officially submit your proposal.**](https://docs.google.com/forms/d/e/1FAIpQLSe43koQL33IzgxXQl29Ex3AhFuqd4hQzxLiXREqwRkDGtx1vA/viewform?usp=sf_link)