Scarlett Eisenhauer

What the potential EU-Commission FR ban have to do with trust?

It's on the table: the EU announced that it might put a stop to the implementation of facial recognition technologies – at least for now. The reason? In the wake of the Clearview Report and other rising concerns, it is unclear as of yet how these kinds of technology will end up interfacing with our social lives. What the EU policy proposal shows clearly: We need to develop "solid mechanisms to evaluate the impacts of [facial recognition] technologies and possible risk management mechanisms." (Fanta, Alexander, 2019).

Should facial recognition be banned for 3 to 5 years, it seems to be one of the only large scale regulations placed on the big and innovative tech businesses in recent years in pursuit of societal good. If so many technologies have been able to be developed, tinkered with, and innovatively pushed into social realities, then why the need for protective mechanisms now? And what might trust processes have to do with that?

For starters, facial recognition feels intimate since it is about something that we feel sovereignty towards and feels less abstracted: our faces. When governance over our facial features become outsourced it can feel strange and invasive. Such was the reaction which led to a public apology, when police in the Chinese city of Suzhou used facial recognition technology to identify and publicly shame people for wearing pajamas in public. Perhaps seemingly banal, shaming and being subject to surveillance can cause stress, discomfort, and result in rippling societal impacts. And it's not hard to imagine how else facial recognition could be used. Currently, artists are painting their faces with geometric shapes and counter-surveillance fashion is on the rise.

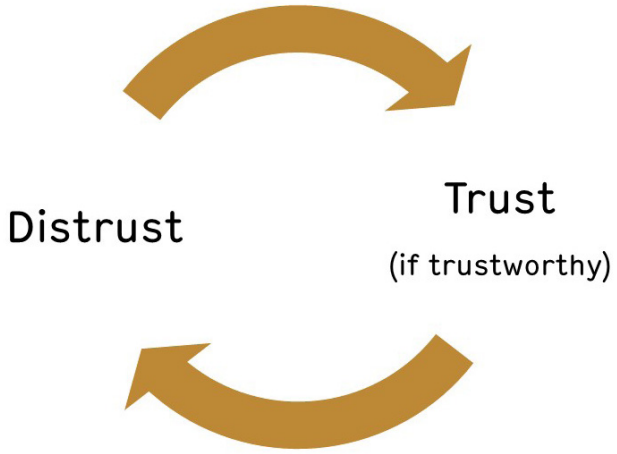
Broad applications of facial recognition seem to violate a need we feel towards controlling our own identification and threaten our right to privacy when our every step can be subjected to surveillance and tracking. This is coupled with a lack of knowledge regarding who is using the technology, who controls the information and for what purposes (or for whose ends) it is being implemented. In short, we are uncertain about future outcomes regarding ourselves: the perfect distrust scenario.

And distrust is a first good step.

ethix

In our ethix White Paper Trust in Innovation, we put forth a conceptualization of trust in the context of novel technologies. For obvious reasons, trust and mistrust are intimately tied to each other. Trust is a future oriented relationship in which we make some assumptions about another party regarding our own imagined future (generally including favorable outcomes for ourselves). If the party fulfills certain "requirements," then we can begin to trust them. Often, we give trust only for certain activities (what we call context-specific trust), so we can say that: [A trusts B to do X]. With the necessary trust in place, we can face risks with a little more confidence.

Trusting someone or something without having properly distrusted first, what is sometimes referred to as blind trust, does not do us any good, because the relationship lacks an element of scrutiny. We should place our trust in what is actually trustworthy through "intelligent" deliberation. Working that out is going to take some time and requires different building blocks to be established before a joint construction of a trusting relationship can take place. It is important to realize that the technology side of the relationship (e.g. the developing company) also needs to do do their leg work by providing ways in which trustworthiness can actually be thought about.



Let's take a look at trust building blocks in relation to facial recognition.

1. Reliance Trust includes an element of reliability. In facial recognition, we want to rely on the technology being able to consistently make the right facial identification (training data biases and skin tones seem to present some problems here). Perhaps more importantly regarding our personal outcomes, we want to rely on the fact that the technology and data are consistently only used for the specified purposes that are beneficial to ourselves. As the technology is being implemented in increasingly diverse situations and has been shown to be problematically instated, achieving this reliance is difficult.

2. Transparency
Transparency can help us make the right decisions regarding trust only when the right kind of information about facial recognition is being given. A good starting point are the basic W's: who, what, where, when, why. Too often it is described as doing one thing, when really it is serving duel or alternative purposes. In addition, facial recognition is pretty easy to hide. First, it does not require direct consent to be trained using an individuals' features – any clear photo will do the job, as was shown in the Clearview case, where millions of pictures were scraped from social media platforms without the users' consent. Second, the technology can be running without the individual's direct knowledge (at airports or through the internet, for example), even if it is crossing into the realm of illegal activities as may be the case with Clearview. Not to mention that it can be used on a mass scale, potentially hiding its present more effectively. There is, then, a lack of transparency regarding what exactly is being done with data, as well as when a person is subject to such scrutiny. An exemplary measure of transparency was provided by the UK Metropolitan Police in their "Notes to Editors," which describe how and why Facial Recognition will be implemented.

3. Percieve similarity We are very good at using visual cues as a means of making assumptions about whether or not someone – or perhaps something – is aligned with our own world views and values. When confronted with facial recognition, we are quickly reminded of totalitarian regimes, with which we do not feel much of a connection – if anything, we would like to avoid them. Thereby, for many, the values and worldviews that feel inherent to facial recognition go against our own and we feel disconnected with the technology.

4. Third party regulation This is the whole point of the EU Commissions proposition to block facial recognition. Innovative developments often fall outside of the scope of regulation. On the one hand this is because they tend to outpace those regulations. On the other hand, we can observe a lack of desire to regulate "in the name of progress" or for economic reasons. Hence, the entire digital economy tends to be unregulated. GDPR was the first piece of major regulation opposing this trend, but it has so far proven to have only limited success and may be a source of mistrust because it has failed to provide the hoped for security. As of yet, the public has very little regulatory assurances regarding facial recognition being used in their lives, despite having little choice about its implementation.

5. Certainty Some amount of certainty regarding future outcomes regarding the application of facial recognition technologies is an important component for building trust. With so many companies popping up, offering different applications of facial recognition, it is hard to make any educated assumptions about how the technology will be used in the future. If fully instated and in the hands of police forces, it seems only a small step to Fahrenheit 451 or Orwellian scenarios. This does not have to happen, but the uncertainty surrounding the future use of facial recognition exists.

5. Information from trusted partners Facial recognition is new enough – or hidden enough – that we don't have others to rely on for firsthand experience accounts regarding the technology. With other types of technology, we rely on asking our good friends about their experience and opinions on the technology. Since we trust them, we believe in the information they give us on the topic. But information that does not yet exist, cannot be passed on to us. Likewise, there is no well-known representative (in the form of some impressive CEO) for facial recognition technology, who gives us the „who, what, where, when, why" answers, based on which we can make our own conclusions. Who would this person be, when there are seemingly endless numbers of start-ups and big tech companies vying for a spot in the facial recognition market place?

6. Ethos of trust Facial Recognition may be perpetuating a devil's cycle in regards to our ethos of trust. The more we have a generalized feeling of trust within our communities and societies (what we call the ethos of trust), the more we are able to face risks and uncertainties as a group. Facial recognition is often sold as a mechanism providing safety: it can ensure proper identification so that information cannot be mixed, or can seemingly be used for catching all the dangerous criminals living in our midst. But that narrative establishes our society as being generally unsafe and untrustworthy, which in turn makes us more risk-averse, including when faced with new technology. The Clearview scandal has been linked to police forces implementing facial recognition on a large scale. This might quickly create a general feeling of constantly being watched (à la Foucault's revitalized Panopticon) which can encourage a feeling of distrust and unease. The absence of an ethos of trust also shows itself in the recent scrutiny that the companies behind the technology have been put under: they can no longer operate under the assumption that the general public supports them.

7. Values Establishing clear values that underlie possible implantations of facial recognition, is perhaps the most important task the EU Commission has in front of them should they force a pause on facial recognition. In their released White Paper Outline, the EU Commission emphasizes the need to uphold European values and principles throughout technological development of facial recognition. What values does this kind of technology reflect? Is it really, for example, a major breach of privacy, autonomy, or even solidarity? And if so, are these values we wish not to infringe upon with our innovations? In other words, it needs to be established which values facial recognition risks breaking and which it is able to uphold – realistically. And given that information, how does the further development of this technology need to be changed? Once these values are well established and a plan made for integration into future developments is made, we as potential consumers or subjects of facial recognition can be more deliberate about our (dis)trust in relation to it. Perhaps, this discussion ought to be held for the deployment of surveillance and identification techniques more broadly.

Next Steps for the facial recognition tech world

Ultimately, the discussion is not about winning consumer or user trust. It is about a thorough analysis of these diverse building blocks, based on which developers behind the technology can make changes to fulfill some of those requirements, if not all, in order to signal real trustworthiness. Based on which values and based on how much certainty, for example, will we be willing to accept facial recognition and use it for positive applications? And yes, there will be some vulnerability involved: no matter how trustworthy one appears, trust is still a two way street and as a society or individual we may still decide to distrust.

What a potential ban on facial recognition might offer us is the breathing space to carefully examine under which conditions we should accept facial recognition or not: this seems to be an important societal discussion to have. It allows to fully engage in distrust of the technology to then carefully decide under what conditions to build trust towards facial recognition in the future: as a society we trust facial recognition to do X.

At the same time, the exact agenda for the ban should be clearly set since a ban in the EU will not prevent companies and entrepreneurs in other countries developing these technologies, with their own values and criteria. What would the ban need to accomplish to make this a productive and innovative move?

Should the ban come through, it will be interesting how subsequent deliberation impacts vulnerabilities on both sides – consumers and companies – and what kind of trust, if at all, can form as a result.