FACE ANALYTICS

GENDER	FEMALE
AGE	± 27
MOOD	
HAPPY	
SUPRISED	
ANGER	
DISGUSTED	
AFRAID	
SAD	
LOOKS AT	ITEM 2

FACIAL ANALYSIS, FUTURE AND PRIVACY

INTERVIEW BY ANDREIA ROCHA

●●

The first time he talked to a computer, he was 8 years old. His first impulse was to introduce himself to the machine, so he typed hello. The answer he got back was "command not found".

Today Roberto Valenti is the CTO of Sightcorp, a company that develops sophisticated computer vision algorithms to understand audience interests by gathering relevant analytics, such as age, gender, emotions, attention and clothing style. This allows to target products, designs and ads to specific interests and profiles, providing them with totally new experiences and improve their level of interaction with devices and software.

Sightcorp has two different face analysis toolkits, InSight SDK and CrowdSight SDK these algorithms analyze biometrics - the measurement of physical characteristics - like age, gender, gaze, emotional expressions. But biometrics can bring too many privacy related concerns when it comes to define the technology. 'The term biometrics is strongly associated with biometric authentication, (i.e. face, fingerprint or iris recognition), which rings alarms bells about privacy issues', says Mr. Valenti. Sightcorp technology does not allow the identification of a person from the biometric data it gathers, but only of its traits.

Sightcorp offers technology packages to be integrated in products. The client doesn't need prior or extensive knowledge on how the technology works. 'You put an image in and you get all the information out, you don't have to do anything else.' Mr. Valenti compares the two Software Development Kit - SDK - to car engines. 'The engine allows you to do a lot of things depending in how you wire it, it could be a car, a tram, a machine, it's about wiring it'.

PRIVACY

'We built the technology overtime with the privacy issue in mind. At the moment, I believe that only humans invade privacy, machines don't invade privacies cause machines don't care about anything.' How these technologies are used is an important point, where does this data get to? 'InSight has no privacy issues, first of all it doesn't recognize you, and you need to be collaborative in order to use it.' According to Mr. Valenti, CrowdSight algorithm throws the images away after being extracted from the camera. Ratios of how the person looks are extracted and put inside the system, after that it is lost forever and there is no way to go back. 'The person is a number. If the system recognizes something too close to that number then it will say it's the same person. You're just a number, not a person. There is no way to go back to who or where was this person. It's not so different than a face 'signature'. From a signature you don't know the person but still it's an authentication.'

Mr. Valenti compares his technology with the boring job of a bouncer, checking and counting people to see if the space reaches its capacity. 'Is the bouncer looking at you invading privacy? He knows that you are a person, he knows that you are a female, and that you are around this age. This estimation is happening inside the person's brain. A person does this job perfectly. A machine might make mistakes, it might double count you, it might think that you're male and you are female. There are decision boundaries that are hard and it all depends in how you train the system. A person has a whole life of training, to understand and recognize what a face and what a female looks like. If you always go to this place, and the bouncer recognizes you, he says hello, is that invasion of privacy? He is going to count that you went in and that you came out. There

is a record. Is not that it records that you are Andreia. It is a female that came in, that is the whole difference. Now if someone decides that females are illegal, then there is a problem. He knows that there are 3 females inside the room.

So at this point privacy is a very big concern. The issue is not the technology invading privacy, it is what you do with the technology and what you allow people to do with the technology.' The combination of technologies and the crossing and combining of data might be the greatest problem. Selling information gathered for a purpose to be applied in a different context is highly illegal and highly unethical. 'There should be a regulation to avoid the misuse of any kind of technology, there should be some kind of control, there should be a consortium. I call it the privacy consortium. If states start to make this regulation, you need to spend money for police to check it, you need to have tools to detect it, it is not something you can set up in a second.' 'People shouldn't rebel against new kinds of technology, they should go against inappropriate crossing of information.'

CUP OF TEA
'In the future, I believe that a person will have some more ways of doing stuff. Before, one used the fingers or the hands; now, the face or the whole body.' Better interfaces and effective computing that understands how you're feeling will be the next level of interaction, Mr. Valenti says. Since most of human communication is done using the whole body and face, using this kind of technology can improve communication with machines. 'Say you want to speak to a computer, when you're speaking, you have facial expressions, you move your hands, all of which can all be used to improve the situation.' There will be deeper connections between users and machines. 'The machine will be able to read you and act consequently. How does it improve your life? Maybe it will make you a cup of tea.' laughs Mr. Valenti.

REALISTIC ROBOTS
Mr. Valenti is a bit skeptical about a world shared with humanoid robots. He refers to a hypothesis called the 'uncanny valley', which talks about robots and the level of freakiness they represent to us. The closer robots

will be to reality, the freakier they will seem, until they become completely indistinguishable. 'Being completely indistinguishable would be if you would be talking to a robot right now. In that moment is not freaky anymore. Once you know it's a toy, it's a toy, once it gets very close to you, than you're scared cause it's too close but yet different, you feel threatened.' According to this 'rule', the slightest difference is the maximum of freakiness. He believes that even in 50 years from now, it will be difficult to create realistic robots, 'maybe it's thinkable, maybe it's applicable, one doesn't know what kind of [paradigm] shifts we will do in the next 50 years, so I can never say never. Until it gets perfect, it will be freaky.' If it will be the case, realistic robots, to pull it off there will be necessary a lot of marketing and a lot of money invested. 'It's a very slow process. And you need to have a solid reason [to pursue it].'

What if we become robots?

'We already are.' In his point of view we already are androids, because we're using many extensions to our body. Human are constantly interfacing with machines. 'To go home, we use bikes, which is just a device to extend the body capability to get home faster than walking You can go from the level of being in a virtual reality room to the level of using a phone. On each of these two levels, which are a bit of both extremes right now, we are completely interfacing.'

The conversation went on. To the future - interactive bespoke commercials, talking to products, getting paid to watch ads, deep learning, and evolution of information. All the way to science fiction - technology becoming 'self-aware'. There are many life changing applications to these kind of technology without compromising our privacy. Obviously there is great danger in how the data gathered might be used, even worst, if combined. Imagine a powerful state using your information and tracking you down whenever they want. Laws to safeguard the public from abusive use of private information should be developed, a consortium as Mr. Valenti proposes. The technology is here, there is no doubt, and it will develop; towards what will depend on how our privacy and individual consent will be protected. •