Do we need an open face recognition search engine?

Alberto Cammozzo[1]

[1] Cammozzo.com and TagMeNot.info, Via Marchesini 5, 35126, Padova., Italy,
a.cammozzo@gmail.com

Abstract. The wide application of face recognition technology may expose us to unforeseen situations. Our ability to cope with this technological innovation may have important consequences for human rights and citizens privacy. One of the most bothering issues is information asymmetry being introduced not only in the web, but also in real life situations. Some imaginary situations are listed, along with the technical and normative means to restore information symmetry. One of the possible solutions being the creation of an openly accessible face recognition search engine.

Keywords: face recognition, facial recognition, search engine, information asymmetry, ethics, social networks.

Face Recognition (FR) has become a mature and well-established technology, silently deployed on both sides of the Infosphere [1]: real world and cyberspace. Nowadays, “anyone may run face recognition on anyone else, online and offline ” [2].

Most FR applications regard security and surveillance: user authentication, biometric passports and borders processing, suspect identification, face in the crowd surveillance, access control and time attendance.

Many commercial applications are maturing, thanks to the use of FR to deliver targeted and even personalized advertising in digital billboards (DOOH), vending machines and TV sets.

Visual data is also being used also for detecting personal features such as sex, age and mood.

Social networks use it for automated tagging, and many applications for smart phones are being developed for real-time image processing in connection with SNs.

Military applications are also being developed, even in connection with drone surveillance and automatic target acquisition [3].

The variety of possible applications has raised a very strong commercial interest in FR. According to some analysts [4], biometric market will strike revenues of 10 billion dollars in 2017, of which up to 33% may come from FR. Startups PittPatt and Face.com have been bought respectively by Google and Facebook for amounts ranging in the tens of millions dollars.

This technology is entering deeply in our everyday life, generating some information asymmetries that may lead to deep social changes, some of which are not so easy to foresee [5].

1 Some situations

Let's imagine some possibly different situations involving automatic face recognition; some of them familiar, some less probable.

> *First*. You receive an email from someone who shows to know you, says you were both at same conference in September, but you don't remember her: so you type her name in Google: nothing that enlightens you: the usual professional information. So you click on Google images, and among the first pictures, her face comes up, and your memory of that person comes along.

This is a case of human face recognition, assisted by a search engine. The search engine knows nothing about the identity of people in pictures; it only suggests pictures that are linked to pages citing the name you are looking for. Note that this could change in the future. Search engines could analyze the picture and automatically recognize people whose identity they are already aware of. In fact the technology for doing so is already mature. Only privacy concerns are keeping them to release it.

This brings us to another possible scenario.

> *Second*. Suppose you meet someone in the street, he apparently knows you well, but, despite your questions, there's no way you remember where you met him before. You discretely take a picture of him with your smartphone using an app that connects to a global face recognition search engine, and a few seconds later the most probable identities matching that person's face are displayed on your screen, along with their Facebook and Linkedin profile. The app suggest you also a list of people you both know. This helps you to remember where and when you met that guy the first time.

Perhaps you are familiar with such situations, but it's rather unlikely you used the app described above. Such apps do indeed exist, but none has ever been released to the wide public for enough time to make its use widespread. Each time one of these applications are announced or released by some startup, that startup was bought by some big firm and included in its software, and the app was retired. This happened to Polar Rose in 2010 (acquired by Apple), to Recognizr by Astonishing Tribe (presented in 2010 but never released [6]). More recently (July 2012) Klick, the app developed by Face.com, was retired by Facebook after its acquisition [7]. PittPatt was acquired in 2011 by Google: its software is now included in the Find My Face service in Google+ (not much after Google's CEO Schwartz defined face recognition “creepy”). In short, face search services described in this second imaginary situation are either retired from the market or included in some social networks (SN) features.

One of the reasons for this may be that in the context of SNs, face recognition is more effective and looks less “creepy”. SNs have an authentication and authorization infrastructure: registered users can decide to allow or block face recognition on their pictures. In SNs, face recognition capability is usually limited to members: members are, if they do not opt-out, the only recognizable subjects. Moreover, usually only members can use face recognition functions: external unregistered users are unable to identify people in pictures, unless these consent to

In fact, given how face recognition works, members do opt-out not from face recognition, but from automatic face identification. Even if I do opt-out, face recognition is still being performed by the SN software platform; once my face is being identified, and according to my privacy preferences, my identity is revealed to others or not. But every photo present in the SN where I appear is still being linked to my identity, even if that identity is not disclosed.

This brings us to other possible imaginary real-life situations.

> *Third*. You are applying for a marketing manager position in a social network firm willing to expand its business in Far-east. You passed the first selection, you know you are qualified for that position. Your potential employer seems very interested at first, but suddenly this interest drops, your application is refused and your further inquiries are declined. From a friend who is employed in the same firm you later know that your application was discarded because of a picture of you – taken years before – when you participated in a public protest against a country that was censoring Internet traffic. That picture appeared nowhere in your various SN profiles, in fact you didn't even know it was taken. But automatic face recognition on your application form photo revealed it in the collection of pictures uploaded by some user of the same SN you were applying to. Even if you opted out from face identification, the recruiters decided according to an information they had: they decided you were not fit for that position, given that very country you were protesting against was one of your possible destinations as a manager.

In this case the SN company used pictorial information about you that was given to them by someone else. Using that information recruiters knew things about you that were not in your resume, you were not prepared to discuss, and that you even did not know exist. The use of such images may be legally questionable, according to terms of use and user agreements, but usually there are carefully crafted. In this case, the SN has an advantage position on its employees, and even potential employees. While textual information present on the web is content-searchable, visual information is not. This may be clearer in the following example.

> *Fourth*. A stalker uses a face recognition search engine to obtain personal information on his potential victims: he takes a picture of her, uploads it to the FaceLeaks.com website, and gets back all the links of

> pictures where his victim is depicted, including the web pages referencing them. That way he gets pointers to her workplace page, pictures of her holidays with her family, and even pictures uploaded to some SN (that she is not even member of) by her former boyfriend, who thought it was sufficient not to mention her name to respect her privacy. She was even not aware that some of those pictures existed, and she would certainly have asked for their deletion if she knew. She later knows the FaceLeaks.com website, uses it to help identify her stalker, and eventually asks for removal of several of her pictures from many sites. She later recommends to her friends to do the same to avoid the unpleasant situation she found herself in.

This fourth situation depends on a website that doesn't exist (yet), but that is technically feasible, commercially viable, probably legal at least in some countries, but whose existence is ethically very questionable ("creepy"). While it's clear that making pictorial data content-searchable exposes people to privacy violations, it's also clear that it allows to keep an eye on what information is getting public. In this case the ability to perform content search on facial pictorial data allows the victim to know what information about her is present on the net and take appropriate measures to restore her privacy. She has access to the same information as the stalker. Being content-searchable by anyone, no one has a privileged position on data.

Another different scenario is lined to possible undesired outcomes of security breaches involving the leakeage of biometric data:

> *Fifth*. The website of a major producer of gaming machines has been hacked. The latest model, sold by the millions, included a face recognition capability: the gamers face and facial expressions are reproduced by their character inside the game. As a consequence of the security breach, among personal users data stolen was also face biometrics. The gaming platform used a face recognition library that stores facial features in a standard, interoperable way. This means that users faces can be recognized on other platforms without the need for them to enroll again, but only using standard libraries. The first time they are being recognized is sufficient: any further recognition, even on different platforms, can be performed on that data alone. The facial data belonging to millions of users is being used by hackers to bypass biometric authentication procedures used by newest operating systems, using the same interoperable biometric face recognition systems.

This scenario is perhaps the more distant to reality, but exposes two important issues. Interoperable data, allowing recognition of people even without enrolling, and security breaches involving biometric data. While this scenario is fictionary, it's not so unreal. Face recognition authentication in PC operating systems already exists, while interoperability of biometric identification systems is a concrete research and industrial objective; large scale data leakage following security breaches really

happened (Sony 2011). The possible consequences of a large scale data leakage involving the biometric identities (and possibly credit card data) of millions are unpredictable.

Let's introduce one last scenario.

> *Sixth*. Imagine a country whose democratic process is still maturing. Face recognition is being used to identify criminals and terrorists: the stream of each surveillance camera in cities, airports, railway stations, highway gas stations is subjected to a face recognition engine. The government uses the power from surveillance to effectively stifle crime, terrorism and even reject foreign spies with double identities, but also indulges to the temptation to use it for political reasons: suspects identification list is extended to fugitives and political dissidents, protest rallies are video-recorded, and opposition members are systematically identified. Government says that who has nothing to hide may still proudly show his face in public. But that country becomes less and less democratic in time. Citizens conclude that having a democratic government depended also on their freedom to hide something from their democratic government.

The technical premises to this last scenario are more and more common in many democratic and less democratic countries. Face recognition devices are currently being deployed by governments for security purposes in the major airports worldwide, in railway stations, city halls. Privately owned face recognition systems are used in many casinos (to identify problem gamblers) and hotels (to identify VIPs). ID cards, driving licenses and passports have photos (and sometimes other biometric data as fingerprints) that are used for automatic identification by police. Many police departments have portable devices allowing them to identify suspects by their face. Face recognition is used to identify double driving licenses. Face recognition has been used on data coming from surveillance cameras (both government and private) to identify rioters in recent riots in London and Vancouver.

2 Information asymmetry

What is common to all these situations is that face recognition generates an information asymmetry that raises privacy and human rights issues [5, 8, 9]. One party knows and uses information about another that the latter ignores. There is nothing wrong with information asymmetry *per se*. However we may want to address the issues it raises. Democracy, privacy and the respect of human rights may depend on a correct information balance. Governments, or firms or single citizens may not be allowed to gain too much information on others, and exploit it to their own advantage.

The solution may come either filling the asymmetry allowing both parties to have access to the same information or not allowing one of the two parties to build the asymmetry first.

The issues presented in the particular situations above come from a series of general issues.

1) First of all, in most countries governments have access to any kind of information that is not disclosed to the public. This may happen – even when warrants are needed – in an automated way. Some countries may exert pressure even outside clear legislative frameworks. This applies also to SN data, despite privacy options. Agreements between companies detaining biometric data and governments may or may not be transparent to the public.

2) Second, pictorial data present on the Internet can be used for unauthorized identification, connecting faces loaded with identity data (as pictures in SNs) to pictures of people in anonymous public contexts (for instance: riots, political rallies, religious assemblies). This procedure is called de-anonimyzation and has proven effective both in research contexts [2] and by police authorities identifying offenders (Vancouver and London riots[10, 11]). Technically it is possible to conceive a system leading to real-time identification of people in public places, using only publicly available data.

3) Third, as a consequence of the previous two points, selected operators, including SNs and governments, but also firms specialized in information gathering, may have access to visual information about me I don't have access to. For instance pictures of me taken and uploaded by others, unbeknown to me. This may lead to situations depicted above in the second, third and fourth scenarios imagined above (the FaceLeaks.com website). A private operator can build an image crawler sweeping the Web and link together all pictures of each recognizable face, and sell that information to anyone needing a background check, including government agencies and potential employers. All that is needed is a clear picture of the target.

3 An Open Facial Search Engine?

In order to fill the information asymmetry described above, legislative or technical measures can be taken. One possible technical measure is making all information available to anyone.

This has of course very serious consequences, as the fifth example has shown: it may represent a “stalker's paradise”. However it may lead to a full awareness of what kind of personal pictorial information is available and allow to take privacy measures, to mature more respectful social norms.

Acquisti [2] suggests that these new technologies are “democratizing surveillance”: a global open facial search engine may represent a drastic way to make surveillance available to anyone. The group of those that have access to surveillance technology and those that have no other choice but being subject to surveillance may overlap.

As said above, it is now possible in theory, and technically feasible, to build a global face recognition search engine that 1) crawls the whole web for images or videos picturing faces 2) does face recognition on those images and 3) links together all the images where the same face appears, with some degree of probability.

Is this search engine legal? Does it treat personal information? Is it biometric information?

Such a search engine does not need to keep personal information. It keeps only a list of URLs where the same face appears. No names, no identities, no other biometric personal data. This data does not directly provide de-anonymized data, put only points to data present in linking pages, that may be useful for de-anonymization.

Ethical issues are still open. Is the world where such an engine exist more creepy than another where the same search activity is done in a covert way? Since it is unlikely that Face Recognitions gets subject to intense legal regulation that makes the use of a facial search engine (may it be open or not) illegal, ethical issues and social impact of such a technology has to be explored in advance, in order to devise proper technological and legal framework for its socially acceptable use.

4 References

1. Floridi, L.: A Look into the Future Impact of ICT on Our Lives. The Information Society. 23, 59–64 (2007).
2. Acquisti, A., Gross, R., Stutzman, F.: Faces Of Facebook-Or, How The Largest Real ID Database In The World Came To Be. Blackhat 2011 (2011).
3. Shachtman, N.: Army Tracking Plan: Drones That Never Forget a Face | Danger Room | Wired.com, http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/.
4. Acuity: The Future of Biometrics Market Research Report. Acuity Market Intelligence (2009).
5. Cammozzo, A.: Face Recognition and Privacy enhancing techniques. In: Bissett, A., Bynum, T.W., Light, A., Lauener, A., and Rogerson, S. (eds.) The Social Impact of Social Computing. p. 101–109. Sheffield University, Shaffield Hallam University, Sheffield, UK (2011).
6. Perez, S.: Recognizr: Facial Recognition Coming to Android Phones, http://www.readwriteweb.com/archives/recognizr_facial_recognition_coming_to_android_phones.php.
7. TheNextWeb: That was quick. Facebook shuts down Face.com APIs, kills Klik app, enrages developers, http://thenextweb.com/facebook/2012/07/07/that-was-quick-facebook-shuts-down-face-com-apis-kills-klik-app-enrages-developers/.
8. Brey, P.: Ethical Aspects of Face Recognition Systems in Public Places. Journal of Information, Communication & Ethics in Society. 2, 97–109 (2004).
9. Pagallo, U.: La tutela della privacy negli Stati Uniti d'America e in Europa. Giuffré (2008).
10. Hui, S.: ICBC offers facial-recognition technology to Vancouver police's riot investigation, http://www.straight.com/article-399779/vancouver/icbc-offers-facialrecognition-technology-vancouver-police%E2%80%99s-riot-investigation, (2011).

11. Elias, E.: Face tagging of photos raises privacy concerns | Vancouver, Canada | Straight.com, http://www.straight.com/article-390719/vancouver/face-tagging-photos-raises-privacy-concerns.