UNIVERSITEIT VAN TILBURG

At First Sight

An exploration of facial recognition and privacy risks in horizontal relationships.

Esther Keymolen, Merel Noorman, Bart van der Sloot, Colette Cuijpers, Bert-Jaap Koops, Bo Zhao.

Universiteit van Tilburg
TILT – Tilburg Institute for Law, Technology, and Society
Postbus 90153
5000 LE Tilburg
Contactperson: dr. E.L.O. Keymolen
e.l.o.keymolen@uvt.nl
Date: 12 March 2020

Summary

Facial recognition technology is used to recognize faces or facial features based on digital images (for example a photo or video). For some time, governments have deployed the technology on a limited scale for detection and security purposes but in recent years, it has also become available to businesses and citizens. This opens up a range of opportunities for commercial companies and individuals to identify, track and profile people. For example, search engines and social media platforms, use facial recognition technology to automatically describe and label (tag) portraits and images; in the retail sector the technology is used to monitor shopping customers and to provide personalized services and promotions; at events it is used to grant or deny access; and various companies offer facial analysis and facial recognition modules and APIs so others can develop, for example, smartphone applications. Such do-it-yourself facial recognition applications can be used to identify others on the street and find information about them, such as previous behavior, relationships with others or personal preferences.

As it is likely that facial recognition applications will be available on a substantial scale for both citizens and businesses in the near future, it is necessary to evaluate whether and, if so, what adjustments to the current legal framework and other regulatory instruments are needed. It is important to note here, that this research focuses exclusively on the use of facial recognition technology in the horizontal relationship: relationships between companies and citizens and citizens themselves. The use of face recognition technology in the vertical relationship, that is to say between governments and citizens, is not part of this research.

This research is based on a broad literature study into automated facial recognition technology and privacy violations for which, in addition to academic literature, news reports, websites, blogs, press releases and brochures have been investigated. For this, we have studied material from both the Netherlands and abroad. The literature study focused on four specific facial recognition applications (so-called domain studies). These domain studies focus on: the event sector, smartphone apps, the smart doorbell and the retail sector. For these domain studies, the literature study was further supplemented with 11 stakeholder and expert interviews. A workshop was also organized with 12 experts, during which a number of domain studies were critically discussed, and the first findings were presented. To map out the current legal means to regulate facial recognition technology, a legal review has been carried out that focuses on privacy and data protection, private law and criminal law. Finally, a number of regulatory options have emerged as well as factors that determine the choice between the various options.

Two questions are central to this study:

1) *How is facial recognition technology used by Dutch citizens and companies and how can the use of facial recognition technologies by citizens and companies infringe the privacy of citizens (now and in five years)?*

2) How can privacy violations, both current and potential, be prevented or limited?

The answer to these questions as it follows from the research is as follows:

Answer to question 1: applications and privacy risks

Facial recognition applications in the horizontal relationship (company-citizen and citizen-citizen) are still in the experimental phase in the Netherlands. Companies are researching, on a limited scale, whether cost-effective facial recognition applications can be introduced. This step-by-step approach taken by companies is not merely motivated by economic motives. The growing awareness that the use of facial recognition entails privacy risks and careless handling leads to potential risks of harm, which leads to companies not wanting to act prematurely. Interviews with the representatives of companies show that it is not always clear to them how the various legal requirements, such as those laid down in the General Data Protection Regulation (GDPR), should be interpreted with regard to facial recognition. This also contributes to the choice of a cautious course.

The number of facial recognition applications in the Netherlands is relatively limited; the projects that are already running are mainly at the initiative of companies. So far, they mainly use this technology for unambiguous and specific purposes. It often concerns a certain form of access control. These applications are not purely of Dutch origin. For instance, American companies also provide facial recognition services to the Dutch market. The initiatives that have taken off in the citizen-citizen relationship mainly concern applications aimed at convenience and entertainment (for example smartphone apps) and access control (for example smart doorbell with facial recognition). Finally, it is also possible for citizens to get started with facial recognition technology. Citizens with some programming knowledge can use online services to develop facial recognition applications themselves.

Whereas the Netherlands is still in the experimental phase, there are already more diverse facial recognition applications abroad - particularly outside the EU - which, however, are often still in the implementation phase there. These foreign applications give an idea of what is technologically possible and what might be expected in the Netherlands in the near future. Possible directions for development of facial recognition applications in the next 5 years may include use for:

- **Ease and efficiency:** At present, facial recognition applications are mainly marketed with the promise of making existing processes run more smoothly. A quick check-in at events via facial recognition, paying in stores via facial recognition, remote access to your house via the smart doorbell, etc. Facial recognition can also be used to enrich existing activities with extra possibilities, such as dating apps that offer the possibility to search for look-a-likes of famous people. Most facial recognition applications that are used in the Netherlands are focused on

efficiency, convenience and entertainment. If this tendency continues and goes together with faster systems that also work independently on portable, small devices, a possible consequence may be that facial recognition will take a prominent place in social settings. Smartphone apps used for social interactions may therefore get a facial recognition component, for example to enable people who get to know each other through online platforms to be able to identify each other offline. Conversely, the large amount of information that has become available online about people in recent years may be linked to individuals offline when they are recognized through facial recognition. Moreover, if ease and efficiency remain the guiding principle in future developments and application of facial recognition, then it may also be the case that all actions that are now required for identification are replaced by facial recognition. Access cards, bonus cards, all kinds of passwords and access codes then become superfluous.

- **Security and control:** Often the above examples also have a control and / or safety component. Checking in via face recognition is not only useful, it also offers the possibility of automatically denying unwanted individuals' access to certain areas on the basis of blacklists. Face recognition is not only used to tag photos but also to prevent identity fraud. Emotion detection as a specific form of facial recognition can also play a role in security and control, such as when certain emotions such as fear and anger are automatically recognized and used to act quickly and prevent escalation. If the use of facial recognition for such purposes continues and the accuracy and speed of the technology increases, then it is conceivable that facial recognition will be linked to restricting access to places and services. It can then become a powerful tool to ward off individuals or groups and to combat behavior that is deemed undesirable.
- **Personalization and proactive services:** Facial recognition can also be used to personalize services and offer them proactively. In the retail sector, menus and offers are already being adjusted based on face and emotion recognition. Certainly, the possibility of being able to monitor how customers feel with emotion detection, a specific form of facial recognition, automated and real-time, and then be able to respond proactively to this is an application that is considered promising by commercial parties. New functionalities that further refine personalized services or advertisements, such as measuring the heart rate on the basis of digital video images of faces, make the automatic analysis of faces even more attractive. If this tendency continues, it is possible that through facial recognition, data can be linked in real time to individuals in the (semi) public space with the aim of influencing their actions (also known as nudging) or profiling them. Nobody will get to see the same offers in stores anymore and in an automated way a distinction can be made in the way people are treated. Facial recognition then becomes an important key to make data-driven decisions and to influence citizens' choice infrastructure in daily life.

Based on facial recognition developments and the scenarios outlined above, the following privacy risks have been identified:

- **Non-transparent information collection**: a lot of facial recognition technology currently works on the basis of models that have been trained with data for which no permission has been given. The internet is an important source for this, but also images obtained in the public space are used for this. Because this data collection takes place on a global level, it is difficult to control this. Citizens lose control of what happens with their photos and videos.
- **Autonomy under pressure:** From a commercial point of view, well-functioning facial recognition often means that citizens do not have to perform extra actions to let the technology do its work. However, the absence of an active action also deprives them of an important choice and reflection moment. Do I really want this? In the situation that citizens are aware of the presence of the facial recognition application and are offered the possibility of obtaining a service or entering space without facial recognition, it might often be the case that the alternative without facial recognition becomes a very stripped-down option with very little being invested in it. Those who hold on to the latter option must then be satisfied with a less-sophisticated service or basic product.
- **Bias and errors in facial recognition:** Although the quality and reliability of facial recognition technology has increased enormously in recent years, it remains a known and not to be underestimated problem that, among other things, *biases* in the training data, facial recognition applications generate outcomes that are discriminatory in nature and work less well with certain groups (such as women, children and persons with a tinted skin color). For these groups there is a greater chance that they will either be recognized incorrectly or not recognized at all, with the result that they will, for example, be denied access to an event, or that they cannot use certain services, which can lead to exclusion and stigmatization.
- **The end of anonymity:** When facial recognition becomes widespread in the horizontal relationship and can be easily deployed by both companies and citizens, it will become increasingly difficult for people to move anonymously into the public, semi-public, and even private space.
- **Dependence on others**: When facial recognition through example apps is used by citizens in social interaction, they are largely dependent on the prudence and discretion of the user to not infringe on their privacy. However, many citizens already find it difficult to estimate, for example, how large the audience is that they reach with online information sharing. This problem is intensified by facial recognition.
- **Secondary use of data:** Although the focus of this study is on the horizontal relationship, an important privacy risk is that governments turn to companies to be able to use the facial recognition information collected in the horizontal relationship. This specific form of secondary use is already known from internet companies that receive - sometimes compelling - requests to share information with, among others, intelligence services. Guaranteeing privacy in

horizontal relationships is therefore also important for protecting privacy in vertical relationships.

- **Inequality of power and chilling effect:** Facial recognition applications that focus on control or personalization actually always do this in combination with other, already existing data files. The face becomes a starting point for other (online) available information about that person. Facial recognition is then no longer simply about recognizing someone, but about making a whole range of information about that person accessible. The information-rich profiles that this creates can affect the privacy of citizens in various ways. This makes it increasingly difficult for citizens to estimate what others know about them. This can lead to power shifts in the horizontal relationship that cause citizens to adjust their behavior as a precaution (chilling effect). Moreover, when the information gained through facial recognition is used to stalk or threaten someone, physical privacy may also be at stake.

Answer to question 2: Best practices and regulatory options

In order to understand how current and potential privacy violations can be prevented or limited, we charted the existing best practices of companies that use and / or develop facial recognition technologies, we conducted a legal analysis, and identified a range of regulatory options.

The following are referred to as Best Practices for protecting the privacy of citizens in the literature and by companies. It should be noted that we have not been able to verify their effectiveness:

- **Services and products instead of data as a pillar of the business model:** Business models where data trading is not the core are preferred.
- **Privacy-by-design:** The design of the system focuses as much as possible on privacy-friendly choices.
- **Company values:** Company values such as transparency, consent, fairness and accountability underpin and limit business choices.
- **Public information:** Companies invest in quality education for customers and citizens.
- **Regulation:** Companies are demanding clear regulation from the government and are developing self-regulation.
- **Permission**: Companies opt for asking consent, even if this is not required by law.

From the legal analysis follows that the current legal tools for regulating facial recognition technology are mainly found in the General Data Protection Regulation, in private law and in particular in the unlawful act and to a limited extent in criminal law. In general, the General Data Protection Regulation will apply to facial recognition technology. This implies that the use of facial recognition in horizontal relationships will only be permitted by law in limited cases. There are legal questions about, among other things, the existence of a legitimate processing basis, and more

generally there are doubts about the necessity, proportionality and subsidiarity of facial recognition applications. After all, the mere fact that a user agrees to a technology or application does not in fact permit its use.

In addition, it must be borne in mind that for the use of facial recognition, biometric data is processed that is legally designated as special personal data, for which a no-unless regime applies. For the use of biometric data in horizontal relationships (specifically: employer-employee relationship), the legislator gives the example that a nuclear power plant may be allowed to use facial recognition technologies to provide access to the facility for registered employees only. This means that most of the other examples discussed in the report are incomparable in their seriousness, importance and necessity. The Dutch Data Protection Authority can play an important role in the supervision of such technologies.

Criminal law currently plays only a limited role in the regulation of facial recognition technologies. However, by analogy with the existing protection against covertly making pictures, the legislator could consider making covert facial recognition punishable, even if the camera itself is recognizable. It must be considered whether applications and use are so serious that prosecution and enforcement through criminal law is appropriate. Finally, it is obvious that this should be done through private law and tort in case a citizen or a company wants to take action themselves.

A range of regulation options is open to the legislator, such as:

- **Total ban:** First of all, the Dutch legislator can choose to lay down a (temporary) total ban for the use of facial recognition technologies. This provides clarity and only a marginal number of possible applications that are currently legally legitimate are nipped in the bud. In other words: this is now still an option with relatively limited negative consequences. The functionalities of apps are still very limited, the results are not always reliable, and the potential benefits are mostly marginal. If the Netherlands opted for a strict regulatory line, that line could be evaluated at a later time, once the technology and applications have developed. This would tie in with the strict line that seems to be developing in the EU.
- **Prior approval:** With this option, applications may only be used and offered if prior approval has been obtained. The Netherlands Data Protection Authority has a natural role to play here. Because this is a technology that uses special personal data, it is obvious to perform a Data Protection Impact Assessment. The Data Protection Authority could issue a guideline from which follows that parties must always submit a Data Protection Impact Assessment and that they may only start after explicit approval of the Data Protection Authority.
- **Diversified approach:** In order to eliminate the legal uncertainty regarding the admissibility of specific facial recognition applications, the legislator, government or the Dutch Data Protection Authority may decide to state explicitly which applications are permitted and which are not. A

distinction can be made between domains, applications and the positive or negative effects on the lives of citizens.

- **Regulatory framework specific to facial recognition:** The legislator or the Dutch Data Protection Authority has the freedom to develop a specific regulatory framework for facial recognition technologies, whether or not in collaboration with other supervisors and (international) parties, in which the general legal principles are formulated in concrete terms with regard to this technology and for the type of applications that are foreseen and considered legitimate.
- **Ex post control:** It may also be decided to maintain the current regulatory framework and to focus on ex post control of technologies, applications and their use. This check can be carried out either at the initiative of a citizen or company submitting a complaint or at the initiative of an enforcement organization, such as the Dutch Data Protection Authority.
- **Code of conduct and certification:** The General Data Protection Regulation makes it possible to develop a separate code of conduct for specific sectors or applications, with a specific enforcement and supervisory organization established by that code. The question is whether facial recognition is really a separate sector where a representative body can draw up such a code and submit it to the Dutch Data Protection Authority. Perhaps working with certification is therefore the more obvious choice, for which the General Data Protection Regulation also offers scope. It is then up to a possibly accredited certification body to issue a certificate to a company that is expected to use facial recognition technology in accordance with the General Data Protection Regulation. The Dutch Data Protection Authority can supervise whether such certification is done correctly.
- **Awareness:** The government can focus on public campaigns to make it clear to citizens and businesses what dangers and legal (and possibly also social and ethical) limits there are to applying facial recognition technologies. Social norms will play an important role in the way facial recognition is applied, especially in citizen-citizen relationships. With facial recognition, a social norm could be helpful, for example, to deliberately not target smartphones at people in a way that they would feel viewed, recognized and categorized. Although such a standard cannot be imposed, policy-oriented awareness-raising interventions can contribute to the development of social norms that can help reduce the privacy risks of facial recognition. A great deal can also be gained with regard to companies. An investigation by the Dutch Data Protection Authority into the admissibility of facial recognition technology in a specific case can also have a clear normative effect and create more awareness of the potential dangers of facial recognition technologies.
- **Tolerance policies:** Finally, the Dutch Data Protection Authority or the government can indicate in policies that the use of facial recognition will be tolerated for a certain period of time and compliance with legal frameworks will not be enforced, in order to give it the chance to reach maturity and to evaluate only after a few years what advantages and potential

disadvantages there are to facial recognition technologies. However, it should be borne in mind that citizens can enforce their rights as enshrined in the European Convention on Human Rights and the General Data Protection Regulation through judicial proceedings, and that ultimately the European Court of Human Rights and the European Court of Justice will pass judgment.

To support the decision-making, we have made a distinction between types of relationships, objectives, and approaches. A thorough assessment can be made by looking sharply at who and for what purposes facial recognition is applied and making abundantly clear what the general attitude of the government is towards facial recognition (from risk avoiding to optimizing opportunities).

Three specific, horizontal relationships can be distinguished:

- **Citizen-citizen:** In this study we have seen virtually no examples of applications that will stand the test of necessity, proportionality, subsidiarity and legitimacy. It should be noted that the technology can facilitate malicious citizens in their actions (such as stalking or identity theft) and that at present citizens have access to commercial services that offer them the opportunity to work with facial recognition technology themselves.
- **Company-citizen:** Although this relationship often involves applications with a clear and serious purpose, the study shows that the most important legal stumbling block to using facial recognition applications here is that there are perfectly good and less invasive technological alternatives.
- **Employer-employee:** Overall, an employee will not be able to give free permission. Grosso modo, as the ground for processing, only the existence of a generally important interest can be invoked (think of the security protection of nuclear power plants).

A distinction can also be made between different purposes for which facial recognition technology is used. In addition, there is obvious overlap with the previous list; it's just another way to categorize the various applications:

- **Health care purposes:** The health care context is a special context because it often concerns vulnerable people and sensitive data. At the same time, it is also a context in which facial recognition technology may offer added value. Recognizing people or granting access to the home of a person with memory loss or an app that helps visually impaired people to perceive people in their immediate environment are examples of applications that can support people in their lives and autonomy.
- **Commercial purposes:** Many of the anticipated applications of facial recognition technology can be categorized within the business-citizen relationship, which involves increasing user-

friendliness (rapid check-in and registration at events), responding to customer emotions to adjust products or services (retail) or to achieve more efficient business operations.

- **Security purposes:** Facial recognition can also be used for security purposes, such as the use of facial recognition technologies for identification and authentication purposes for critical infrastructure. To what extent, for example, a smart doorbell, used other than for the sick and those in need of help, should really be seen as a tool in the context of a safe entry policy for a private home or rather seen as a nice gadget, cannot be clearly determined at the moment.
- **Recreational purposes:** Many of the applications of facial recognition technology within citizen-citizen relationships can be classified as applications for entertainment.

It is important to make explicit what the basic attitude of the legislator is towards developments in the field of face recognition technology, such as:

- **Avoiding risks:** In principle facial recognition technologies currently have little power and the question is whether this will be different in the future. In any case, there are necessary disadvantages and risks identified with regard to the application of such technologies. That is why the use of these technologies is being restricted as much as possible, possibly until there is reason to believe that such technologies would offer more benefits than is currently the case. This is in line with the precautionary principle: because it is not yet possible to estimate how the technologies will develop and how the data that is currently being collected may be used or misused in the future, restraint is appropriate.
- **Risk mitigation**: It is assumed that facial recognition technologies use highly sensitive data and are not only highly invasive but can also entail the necessary risks. Yet it is recognized that in special contexts, the application of this technique could have a positive effect. That is why the regulation that is currently available should be further specified and further adjusted to make it clear that facial recognition technology cannot in principle be used, unless where explicitly indicated and under the conditions laid down, either in legislation or in other types of regulation.
- **Promoting opportunities:** It is assumed that facial recognition technologies involve a number of risks, but also the necessary opportunities. That is why one can opt for a diversified approach in which efforts are made within a number of sectors to allow (experiments with) facial recognition technologies. Based on the results achieved there and an evaluation of the various advantages and disadvantages, a choice may then made with regard to the other areas in which facial recognition technologies could possibly play a role.
- **Optimization of opportunities:** It is assumed that facial recognition technologies will develop in the long term in a way that has many positive effects for citizens, business, the economy and well-being in the Netherlands. These positive effects can in any case, possibly with the help of support measures, overshadow any negative consequences. It is therefore considered

important that the various barriers and obstacles that are now contained in the legislation are removed as much as possible.

These four approaches will be broken down into the tables below, indicating which regulatory option is obvious with regard to which type of relationship and which type of purpose. In addition, the regulatory choices will be indicated in colors: **risk-avoiding**, **risk-limiting**, **chance-promoting** and **chance-optimization**.[1] It should, of course, be noted that awareness of every regulatory choice can be seen as supportive.

	Citizen-citizen	Company-citizen	Employer - employee
Total ban			
Prior approval			
Diversified approach			
Specific legislative framework	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////	//////////////////////////// ////////////////////////////
Ex post control			
Sectoral control			
Awareness			
Tolerance policy			

Table 1: Regulatory options per type of relationship

	Health care purposes	Commercial purposes	Security purposes	Recreational purposes
Total ban				
Prior approval				
Diversified approach				
Specific legislative framework	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////	//////////////////////// ////////////////////////
Ex post control				
Sectoral control				
Awareness				
Tolerance policy				

Table 2: Regulatory options per context

[1] //////////////////////////// refers to the combination of risk-limiting and chance-promoting.

Facial recognition technology in horizontal relationships is not yet an accomplished fact in the Netherlands, it is facial recognition “at first sight”. Nevertheless, the applications that are being developed worldwide and the associated privacy risks are real. This means that Dutch society must now ask the fundamental question: "what do we find desirable when it comes to facial recognition technology in our democratic constitutional state?" This report aims to contribute to this development of ideas and, moreover, to offer guidance to the Dutch government, the legislative power and possibly the relevant enforcement organizations to opt for the most suitable regulatory option(s) in a transparent and systematic manner.