Say cheese! Privacy and facial recognition

Ben Buckley, Matt Hunter
Linklaters LLP, London, UK

Abstract

The popular social networking site, Facebook, recently launched a facial recognition tool to help users tag photographs they uploaded to Facebook. This generated significant controversy, arising as much as anything, from the company’s failure to adequately inform users of this new service and to explain how the technology works.

The incident illustrates the sensitivity of facial recognition technology and the potential conflict with data privacy laws. However, facial recognition has been around for some time and is used by businesses and public organisations for a variety of purposes – primarily in relation to law enforcement, border control, photo editing and social networking. There are also indications that the technology could be used by commercial entities for marketing purposes in the future.

This article considers the technology, its practical applications and the manner in which European data protection laws regulate its use. In particular, how much control should we have over our own image? What uses of this technology are, and are not, acceptable? Ultimately, does European data protection law provide an adequate framework for this technology? Is it a framework which protects the privacy of individuals without unduly constraining the development of innovative and beneficial applications and business models?

1. How does facial recognition technology work?

Facial recognition is interesting. It is a classic example of a task that is trivial for a human but, until recently, has been challenging, if not impossible for a computer. Just consider the variations in our appearance depending on whether we are wearing glasses or a hat or have recently acquired a suntan in Saint Tropez or by St. Tropez. Add in the fact that a facial image might be seen from different angles, with different expressions and under different lighting conditions and the scale of the challenge becomes apparent.

However, great strides have been taken in the last few years with effective facial recognition products now becoming widely available. Broadly speaking, facial recognition algorithms are either geometric or “photometric”. Geometric algorithms extract particular features from an image of the subject’s face. For example, an algorithm may analyse the size and shape of the eyes, nose, cheekbones, and jaw and their distribution in relation to one another. These details are then used to search for other images with matching details. Photometric algorithms adopt a statistical approach by distilling an image into values and comparing those values with templates to eliminate variances.

New developments in facial recognition applications are increasing in their accuracy and the scope of their use. For example, 3D facial recognition software allows more comprehensive collection of distinctive features on the surface of a face, such as the contours of the eye sockets, cheekbones, nose, and chin. Such applications have the advantage of being largely unaffected by changes in lighting and allow the identification of faces from a variety of angles, including a profile view. Some new applications also make use of “skin texture analysis” which captures the visual details of the skin as shown in standard digital or scanned images.

© 2011 Linklaters LLP. Published by Elsevier Ltd. All rights reserved.
Finally, facial recognition technology is not only used to identify individuals but can also be used to identify particular characteristics about that individual. For example, is the individual a man or a woman? How old are they? What is their physical or emotional state — happy, anxious, tired?

2. Applications of facial recognition technology

2.1. Recent developments

Until recently, one of the most common applications for facial recognition technology was crime prevention, detection and enforcement. The most widespread use has occurred in the United States, where the technology has been used to detect the attendance of wanted criminals and terrorist suspects at large gatherings, such as sporting events and music concerts. It has also been used for law enforcement purposes in Europe. For example, it has been reported that the German Federal Criminal Police Office uses centralised facial recognition tools to scan a database of centralised “mug shot” images to help recognise unknown suspects, while the London Borough of Newham has trialled a facial recognition system built into the borough-wide CCTV system.

Facial recognition tools have also been used widely in maintaining national border security. For example, the German Federal Police use a voluntary facial recognition system to allow travellers to pass through fully-automated border controls at Frankfurt airport. The UK government also allows travellers with biometric passports to travel through automated border controls that use automated facial recognition technology.

More recently, however, these tools have been adopted for recreational and social networking purposes. The most public example of this development is Facebook’s rollout of facial recognition tools. The Facebook facial recognition tool allows users to “tag” friends more easily by automatically searching uploaded photos for the faces of users’ friends. The names of those friends are then suggested to the user for tagging purposes.

Facial recognition has also been rolled out by a number of other technology suppliers in their photo editing and storing software, such as Google’s Picasa, Apple’s iPhoto, Sony’s Picture Motion Browser and Microsoft’s Windows LivePhoto Gallery.1

2.2. The potential power of facial recognition technology

This, however, is merely the tip of the iceberg and a huge number of other applications is possible. Some of these could serve important, life-saving functions, e.g. in-car systems designed to recognise if a driver is drowsy and to alert the driver accordingly by changing the radio station.

The ability to target marketing material at individuals based on their appearance is one obvious but as-yet largely untapped opportunity which the technology presents to businesses. This is not simply a matter of speculation; for example, the multinational foodstuffs manufacturer Kraft, recently announced a joint project with an unidentified supermarket chain to use the technology to identify and target those shoppers most likely to buy its products. Kraft’s CEO summarised the technology as follows.

“If it recognizes that there is a female between 25 and 29 standing there, it may surmise that you are more likely to have minor children at home and give suggestions on how to spice up Kraft Macaroni & Cheese for the kids.”

In a similar vein, Adidas has announced that it is working with Intel to create “digital walls” which recognise the sex and approximate age of individuals who walk by, and present advertisements for the products that those individuals would be most likely to purchase.

At least for the present, it appears that marketing campaigns are using facial recognition only to ascertain the broad demographic category into which an individual falls (e.g. by reference to age and sex). Some fear, however, that by linking to social networking sites or other databases, companies may, in future, be able to target marketing at particular individuals based on their particular personal circumstances.

The future of this technology could deliver much more invasive applications. The “Google Goggles” app, available on smart phones, allows users to take photographs of inanimate objects and immediately identify them (e.g. wine labels, famous monuments and book covers). Google acknowledges the tool could be rolled out to recognise photographs of individuals. This raises the prospect of your photograph being taken on the street and your life secrets being immediately revealed. Eric Schmidt remarked.

“We do have the relevant facial recognition technology at our disposal. But we haven’t implemented this on Google Goggles, because we want to consider the privacy implications and how this feature might be added responsibly… I’m very concerned personally about the union of mobile tracking and face recognition.”

Google clearly recognises that a line needs to be drawn somewhere. However, is that line in the right place? What

---

3 See Fraport AG’s website: <http://www.fraport.com/content/fraport-ag/en/products_services/traffic_terminalmanagement/easypass_new_automaticbordercontrolatfrankfurtairport.html> which includes a video (and background music) to show the technology in action.
4 See the UK Border Agency: <http://www.ukba.homeoffice.gov.uk/customs-travel/EnteringtheUK/e-passport-gates/>.
happens to those who overstep the boundary? These issues are largely determined by rights to privacy conferred by European and domestic law.

3. Data protection implications of facial recognition technology

3.1. How do data protection laws characterise facial biometrics?

European data protection laws protect “personal data” i.e. information about an identified or identifiable living individual.

It has long been accepted that a person’s image can, by itself, constitute personal data and benefit from the protection conferred by data protection legislation. In the UK, the Information Commissioner’s Office has made this clear in its CCTV code of practice, which states that images of individuals and the information derived from those images relate to individuals and this data is covered by the Data Protection Act 1998 (the “DPA”). However, much depends on the circumstances. For example, it seems less likely that the images captured by Kraft to promote macaroni cheese would be personal data – i.e. it is unlikely that Kraft could identify any of the individuals photographed or that there would ever be any intention to indentify those individuals. All Kraft wants is a general demographic assessment.

European data protection laws also apply additional, stricter rules, to a sub-category of personal data, “sensitive personal data”, which includes data relating to race and ethnicity, sexual life and health. Given a data subject’s facial appearance might constitute personal data, might it also constitute sensitive personal data? It is arguable that facial images are sensitive personal data because, for example, they allow users to determine a subject’s racial or ethnic origin. This was the conclusion in the English case, Murray v Express Newspapers & Big Pictures (UK) Ltd [2007] EWHC 1908, though the judge went on to say that the processing of that personal data was justified, as the data was made public by the relevant individual. The potentially bizarre consequences of this decision (for example, that it would be possible to compile a collection of photographs of individuals publicly leaving a particular mosque or a synagogue) are the topic for another article.

A number of other European member states, including the Czech Republic and Estonia, have concluded that this type of information is inherently deserving of enhanced protection and have expanded the definition of sensitive personal data to include biometric data. This suggests that facial images would, in those jurisdictions, automatically be sensitive personal data.

3.2. How do data protection laws control the use of facial recognition technology?

The application of facial recognition technology to an individual’s facial image constitutes processing of personal data and, therefore, can only take place if a legal justification exists. This means the processing should fall within one of the processing conditions set out in Article 7 of the Data Protection Directive and individuals ought to be informed of any use of their information under Articles 10 and 11 of that directive. European data protection law also imposes a range of other obligations e.g. the data is kept secure, accurate and for no longer than is necessary.

For facial recognition, one likely processing condition is that the relevant individual has consented to the processing. Alternatively, it may be possible to show the processing is in an organisation’s legitimate interests and those interests are not overridden by the fundamental rights and freedoms of the individual (the so-called “legitimate interests test”). Stricter conditions apply to the processing of sensitive personal data which normally requires consent.

The roll out of the new Facebook “tagging” function, described above, provides a useful illustration (assuming Facebook is subject to data protection laws). In rolling out this function, Facebook should have informed individuals of this new feature and ensured it satisfied a relevant processing condition. In this regard, Facebook did not obtain consent from users as to the use of the tool in relation to their images and instead provided it on an “opt-out” basis, such that, in order to avoid the use of the tool, users were required to take action to change their privacy settings on the site. This approach is inconsistent with the “privacy as default” model, which would have dictated an opt-in arrangement, generally.

There are, however, powerful public policy reasons for not characterising facial images as sensitive personal data. If such images were sensitive personal data, the grounds required for processing would be greatly restricted, thereby potentially inhibiting even non-invasive uses of facial recognition technology that benefit users. The restrictions on the processing of non-sensitive personal data under the DPA, appear well-suited to permitting these non-invasive, beneficial applications of facial recognition technology while prohibiting, or at least heavily restricting, the types of highly invasive uses identified above.

---

10 See, for example, the Article 29 Working Party’s Opinion on the concept of personal data (Working Paper 136). One factor in determining whether or not information is about an “identifiable” individual is whether the data controller has any intention to make such identification.

11 In Germany a stricter approach to the technology may be taken in the future. A draft bill on protection against severe violations of personal rights on the internet has been updated by the German Minister of the Interior and, although not yet public, it is supposed that it will contain regulations restricting the use of facial recognition software.

12 We assume for these purposes that Facebook is a data controller and is subject to the jurisdiction of European data protection regulators. It has been argued that social networks cannot properly be characterised as data controllers and, therefore, are not subject to European data protection laws but the Article 29 Working Party’s Opinion on the concepts of “controller” and “processor” (Working Paper 169) characterises social networks as data controllers. Again, this is a topic for another article.
favoured by European regulators. Whilst it might be possible to rely on the legitimate interests test as an alternative, regulators in Germany and in Switzerland have launched investigations into Facebook’s new technology.

Google’s “Picasa” website highlights a more practical difficulty in complying with data privacy laws. The user of Picasa teaches the facial recognition system who is in the user’s photographs. The Picasa system remembers and applies what it learns to the next photographs uploaded by the same user. However, the Picasa system does not (and could not) seek consent from the people in the photographs to the processing of their personal data as it has no means of contacting them (in contrast Facebook’s facial technology only works on other Facebook users so Facebook can easily inform them of that processing). Arguably, this is not an issue for Google, as it is only providing software to the users and is not itself processing the underlying information. However it would be a different story entirely if Google were to process this information itself (i.e. a data controller). As it has no direct contact with many of the individuals identified, it would be hard to inform them of this processing or to otherwise justify it under data privacy legislation.

Other forms of facial recognition e.g. recognising gambling addicts in casinos, or minors in age restricted venues, or drowsy drivers behind a steering wheel, may be able to rely on conditions other than consent or the legitimate interests test. For example, the processing may be necessary to comply with the legal obligations of the data controller or to protect the vital interests of the data subject.

3.3 Data protection and social norms

It is also important to recognise that European data protection principles also reflect the public’s expectations about how their personal information will be used. Even if, technically, the law permits these uses, how will they be received by the individuals whose information is being processed?

The impact of the increased use of facial recognition technology by social networking sites has been met with some nervousness. Recent reports are that the numbers of users and the activity of users on Facebook have decreased. This may in part be attributable to a mistrust of social networking sites when it comes to the level of protection of a user’s privacy, and facial recognition might have contributed to this. Indeed, social network sites are now looking to use privacy as a competitive advantage. This could be new ground for competition between the large players like Facebook and Google+ and will clearly be relevant to the deployment of new technology, such as facial recognition.

4. Conclusion

Facial recognition clearly has the potential to add value and bring benefit to society but could also seriously infringe individual’s privacy rights – it raises the potential for a surveillance society writ large.

Do European data protection laws provide the right model to regulate this technology? Arguably, they do. Their principle driven approach, both flexible and technologically neutral, allow the development of new and innovative applications whilst curbing excessive and intrusive uses. Nonetheless, this is also very much a question of how those laws are interpreted and applied. Their flexibility, in this instance, in relation to whether facial recognition includes processing sensitive personal data, is also their potential downfall. Regulators will need to keep abreast of developments in new facial recognition technologies and new, more intrusive applications of the technology.

Finally, facial recognition is one more example of the dazzling advances in computer science. Applications that were once the realm of science fiction are now reality. This is unlikely to be the last time that an extension to the boundaries of technological possibility raises new and interesting legal issues.

Ben Buckley (ben.buckley@linklaters.com) and Matt Hunter (matthew.hunter@linklaters.com) Linklaters LLP, London.

---

13 See, for example, the Article 29 Working Party’s Opinion on the definition of consent (Working Paper 187), which stated the position that silence does not constitute consent nor do pre-ticked boxes, default settings, or opt-out consents processes. Facebook’s opt-out tool, it appears, is at odds with this position.


15 Coincidentally, as this article was being written, Facebook updated its layout and included a new option which lets users approve or reject tags before they appear on the user’s profile. See www.facebook.com/blog for the latest.