

ARTICLE:

# WHETHER A PHOTOGRAPH TAKEN FOR GOOGLE'S STREET VIEW CAN BE USED AS EVIDENCE IN A CRIMINAL PROCESS: A CASE NOTE

By **Nadezhda Purtova**  
and **Arnold Roosendaal**

**On 19 June 2009, the Associated Press reported an arrest by the Dutch police of two suspects in a robbery case. The alleged victim, a 14 year old boy, found a photograph on Google Street View where the suspects were walking directly behind him. The picture was taken minutes before the robbery, and the alleged victim found it on Street View six months later.**

The faces on the photograph used by the application had been blurred. Therefore, to identify the suspects, the police had to make an official request to Google to provide the authorities with the original photograph where the faces were clearly visible. Google complied. A spokesman for the police in the city of Groningen, where the robbery took place, indicated that the photograph could provide an important contribution to solving a crime. At the same time, Dutch press has already expressed public discontent with Google's photographing of streets and people, claiming violations of numerous provisions set out in privacy and data protection legislation.<sup>1</sup> Some members of the general public in other countries have even stronger feelings about Google's practices. In the UK, for instance, cases have been reported where citizens successfully formed a human barrier to prevent Street View's camera cars from photographing their

neighbourhoods.

The discomfort that can be caused to a person if caught on camera can be seen on web sites such as [streetviewfun.com](http://streetviewfun.com), which is a collection of embarrassing photographs gathered from Street View. This note considers the issue of the relationship between the violation of data protection and the admissibility of photographs obtained as a result of such (an alleged) violation. The question posed is whether the clear photograph of suspects that purport to show they are about to commit a crime can be used as evidence in a criminal process if the photograph was retained in violation of data protection requirements. The question implies two further questions: whether there are grounds to regard the retention of a photograph in the clear by Google for six months is contrary to data protection rules, and if the answer is yes, the effect that this illegal retention may have on the use of the photograph as evidence in a fair criminal process. The question is addressed both from the perspective of the European Convention of Human Rights and Dutch national law (implementing the 1995 EC Directive on data protection).<sup>2</sup>

## **Alleged privacy violation**

This section demonstrates that data protection rights of the suspects may have been breached by Google. It is also possible that the Dutch government will have been

<sup>1</sup> 'Privacy-issues rond Google Street View', *Brabants Dagblad*, 30 June 2009, 19.

<sup>2</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection

of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.95, p. 31.

liable of a violation of the right to privacy as provided by article 8 of the European Convention on Human Rights (ECHR).

### Google

In order to provide the service of Google Street View, namely the making available of panorama (360°) pictures of streets in several countries, Google takes photographs to cover a 360 view from a vehicle driving through the streets with a camera on top. Whether this can be regarded as surveillance is the first question to determine in order to define the applicable legislation. It is the view of the authors that Google's practices do not amount to surveillance. Therefore, legislation on surveillance is not applicable to this case. Although the actions of Google qualify as a recording in public spaces by a private party, a major element of surveillance is missing. To qualify as surveillance, there has to be some systematic, structured monitoring over a certain period of time. Google only takes the pictures of a street once. Therefore, the element of a period of time is not involved.

The body of law applicable to this case is the one on privacy and data protection. Google's photographing falls under the data protection law since, first, photographs of the identifiable individuals are personal data,<sup>3</sup> and second, taking and retaining the data in a computer constitutes processing of personal data by automated means. This in turn means the data is the subject matter of Directive 95/46/EC and the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens, Wbp*) that implements the Directive.

When the individuals that are the subject of the photographs have their faces blurred and are no longer recognizable (identifiable in the wording of the Directive), the pictures no longer constitute personal data. However, as becomes evident from this case, Google also stored the original clear photographs. Consequently, there are several conditions of legitimate data processing that Google should have complied with under the Directive and the Dutch law but, on the facts of the case, failed to do so.

First, the processing of personal data is only legitimate on the basis of the individuals' unambiguous consent<sup>4</sup> (article 7 of the Directive). However, in most cases people are not even informed that Google has taken photographs of them, which is a violation of article 10 of the Directive relating to information obligations, let alone the request to opt out if they

object to being photographed. Obviously, asking permission from every individual included a photograph before it is taken is, in practice, impossible. However, the lack of consent only gives an extra indication that the personal data have to be dealt with in a careful manner and that the personal data should be removed or rendered anonymous as soon as possible.

Neither of Google's practices fall under exceptions from the consent rule. The legitimate business interest of Google to take the photographs in order to be able to provide its service can be a potential ground for exception under article 7 of the Directive, but it is doubtful whether there is an interest in storing the personal data in the form of clear photographs. A business interest is a valid ground for exception from the consent rule only when it does not infringe upon any fundamental right. Personal data can only be collected for specified, explicit, and legitimate purposes. Personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed' (article 6 of the Directive, article 7 Wbp.) In the case at hand, it is questionable whether this was done. Although the purpose requirement may have been fulfilled at the moment of taking the photograph and up to the moment when the photograph was placed on the Street View to provide a view of the respective street, retaining the original photograph with clearly recognizable faces went beyond this purpose. Indeed, that the application aims to provide views of the streets, not photographs of individuals. Equally, that the clear photographs were stored for a relatively long (at least six month) period after the blurred photographs were placed on-line, contributes to the interpretation of Google's practices as a violation of the purpose requirement. If so, the practices of Google would constitute a violation of privacy and data protection legislation. If this is correct, then the legality of the photograph obtained through those practices may be questioned.

### Government

Although it was a private entity – Google – that is responsible for the alleged data protection breach, the Dutch government may also be found liable for a violation of the provisions of article 8 ECHR, the right to privacy, should either of the individuals recognizable on

<sup>3</sup> See for instance the ECHR case *Reklos and Davourlis v Greece* of 15 April 2009, (Application no. 1234/05).

<sup>4</sup> See also ECHR *Reklos and Davourlis v Greece*.

the photograph in question decide to pursue the claim of violation of privacy before the European Court of Human Rights (after exhaustion of national legal mechanisms) and can receive a remedy from the Dutch authorities, should it be proven that no effective measures were taken by the latter to ensure respect for data protection rights. That is a result of a recent decision of the European Court of Human Rights in *I. v Finland*.<sup>5</sup> The case involved a medical worker diagnosed with HIV whose medical records were viewed by her colleagues. The Finish government argued that it was due to the actions of private parties that the applicant's privacy was violated, and therefore denied liability. The court ruled to the contrary:

Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life .... These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.

In the circumstances of the Google case, this decision implies that the government might be liable, if it is shown that no effective regulatory or enforcement measures were taken to prevent Google from violating data protection and to ensure the respect of privacy. Conversely, the interests of the victim should not be forgotten. This interest will rightfully be addressed because the photograph in question is likely to be admitted into evidence. The violation of rights to privacy (of the offenders) is a different matter and should be treated separately.

### Admissibility of the photograph as evidence

A photograph can be used as evidence in a criminal trial. Articles 339(1) and 340-344 of the Dutch Criminal Procedure Act (*Wetboek van Strafvordering*) sum up what can be used as evidence. The provisions of article 339(1) and 340 permit the judge's own observation to be regarded as a form of evidence. This can also include observation of videos or pictures.

As to the admissibility, it is a well explored area of the Dutch law, especially when the question is whether unlawfully obtained evidence can be used. Two case scenarios are possible: where a state authority commits a violation in the course of obtaining the evidence, and when the evidence is a result of the unlawful behaviour of a private party. As to the first, before 1962, the admissibility of evidence was not affected by the way it was obtained. Judges referred complaints about violations committed by the police to the public prosecutor.<sup>6</sup> However, in 1962, the Dutch Supreme Court (*Hoge Raad*) ruled against the admissibility of a blood test taken without the suspect's consent and therefore in violation of their bodily integrity.<sup>7</sup> Such practices were found to be incompatible with the meaning of the Criminal Procedure Act, and safeguards for the guarantees of suspects as set out in the Act.

The case at hand, however, falls under the second case scenario, where the private party has committed an unlawful act that can potentially be used as evidence in a criminal case. According to the latest case law on the matter,<sup>8</sup> the illegality of a private party's actions may have similar consequences in relation to the admissibility of the evidence, provided the government has had an influence on the obtaining of the evidence. For instance, such an influence will take place if the police requests a private detective to collect the materials. In cases where the police 'accidentally' obtained the evidence or just receive it, the admissibility seems not to be difficult. In the case at hand, the Dutch authorities did not actively induce Google's possible data protection violations. Although a national data protection authority had to be informed about Google's plans to photograph the streets and people who are on the respective streets at the time of photographing, it is more likely that this will not be an obstacle for admissibility of one of those photographs as evidence. A different interpretation is possible if the provisions of article 8 ECHR are taken into account, where the Dutch government has a positive obligation to establish an effective system of data protection, including the prevention of violations by private parties. If a failure to comply with this duty is taken as State interference, it is possible to argue that it results in the inadmissibility of the photograph because of that failure. Whether this line of argument is effective still has to be seen.

<sup>5</sup> Application no. 20511/03, Judgement of 17 October 2008; *I. v Finland* heavily relies on the previous ECHR case-law on the positive obligations of the State: *Airey v Ireland*, judgment of 9 October 1979, Series A no. 32, p. 17, § 32). These obligations also involve the adoption of measures to secure respect

for private life 'even in the sphere of the relations of individuals between themselves' (see *X and Y v the Netherlands*, judgment of 26 March 1985, Series A no. 91, p. 11, § 23; *Odièvre v France* [GC], no. 42326/98, ECHR 2003-III).

<sup>6</sup> G. J. M. Corstens, 'Het Nederlands

strafprocesrecht', (Deventer, Kluwer, 2005), 670.

<sup>7</sup> HR 26 juni 1962, NJ 1962, 470.

<sup>8</sup> See for instance: *Hoge Raad* (Dutch Supreme Court) 26 May 2009, LJN: BH8800, *Hoge Raad* 07/11424.

In addition, when taking the 1962 judgment into account, a violation of a fundamental right might be of influence in the decision on the admissibility of the evidence. Data protection rights are recognized as covered by article 8 ECHR, the fundamental right to privacy. This is also one of the legitimate arguments that may be used to challenge the admissibility of the photograph in question.

### Article 6 ECHR on admissibility

Although the case law of the ECHR acknowledges that the national legislator is better placed to deal with the (substantive) law of evidence, it is still possible to find guidance for the controversy at hand as regards the procedural fairness of a trial. The case of *Khan v UK*<sup>9</sup> may be invoked as a leading case in this matter. It follows from this decision that the provisions of article 6 ECHR, the requirement of a fair trial, concerns criminal proceedings in their entirety and cannot be limited to a single item of evidence. As a result, the ECHR case law treats article 8 in respect of privacy violations and possible consequences vis-à-vis the fairness of the criminal proceedings separately. The former does not automatically undermine due process, providing a defendant is given the opportunity to question the significance and legality of the evidence and its source, as well as whether it was falsified before a court.

### Conclusions

This note has considered issues relating to data protection and admissibility of the evidence involved in the recent Google Street View controversy. The question considered was whether the photograph of the suspects supposedly about to commit the crime can be used as evidence in a criminal trial if it was obtained in violation of data protection guarantees. The following conclusions can tentatively be offered:

First, Google may have committed a violation of data protection guarantees by storing the photograph in question where the suspects and the alleged victim were identifiable. Namely, the requirement the photograph should have been rendered anonymous or deleted after having fulfilled the legitimate purpose for which the data were processed was violated.

Second, where no effective measure is taken by the national government to remedy that data protection violation (and prevent future similar incidents), the Dutch government runs the risk of being in breach of its

positive obligation under the provisions of article 8 ECHR in respect to the right to privacy.

Third, assuming that Google retained clear photographs of the suspects in violation of the data protection provisions under Dutch law, it may only result in the inadmissibility of the photograph in a criminal trial if it is shown that such a violation took place with influence of the authorities. Whether a violation of the State's positive obligation to effectively ensure data protection interests may qualify as such an influence remains to be seen.

Fourth, on the level of the European Convention of Human Rights, a breach of privacy and procedural fairness are not mutually exclusive. That is, the alleged illegality of the evidence will not automatically give rise to the breach of the principle of fair trial, providing a defendant has an opportunity to dispute the legality and the evidentiary power of the photograph.

In addition to the conclusions, this case may have further implications for similar cases and raise several questions, subject to further consideration. For instance, the internet is replete with web sites where witnesses post photographs or video recordings of a crime or other offence that has been committed where the offenders are clearly identifiable.<sup>10</sup> The Google case, if the photograph in question is admitted into evidence, can surely have a tremendous effect on the treatment of other photographs and videos as evidence. What effect that would be remains to be seen.

© Arnold Roosendaal and Nadezhda Purtova, 2009

*Arnold Roosendaal (LL.M MPhil) is a doctoral candidate at the Tilburg Institute for Law, Technology, and Society (TILT, the Netherlands). His research is on the digital representation of individuals and the implications for privacy and autonomy when such representations are used by governments and businesses to make decisions affecting individuals.*

**a.p.c.roosendaal@uvt.nl**

**<http://www.tilburguniversity.nl/webwijs/show/?uid=a.p.c.roosendaal>**

*Nadezhda Purtova is a PhD candidate at Tilburg Institute for Law, Technology, and Society. Her interests primarily lie in the field of privacy and data protection, information technology and human rights, constitutional and comparative law, as well as property.*

**n.purtova@uvt.nl**

**<http://www.tilburguniversity.nl/webwijs/show/?uid=n.purtova>**

<sup>9</sup> 12 May 2000 (Application No 35394/97).

<sup>10</sup> See for instance this post on a neighbour mistreating his child: <http://www.geenstijl.nl/mt/>

[archieven/2009/01/buurman\\_slaat\\_zijn\\_kind.html](http://www.geenstijl.nl/mt/archieven/2009/01/buurman_slaat_zijn_kind.html).