



**Information Commissioner's Office**  
Promoting public access to official information  
and protecting your personal information

Simon Davies  
Director – Privacy International  
6-8 Amwell Street  
Clerkenwell  
London  
EC1R 1UQ

30 March 2009

Dear Simon

**Re: Google Streetview Complaint**

I write regarding your letter to Richard Thomas about Google Streetview. Richard has asked me to respond on his behalf. We are aware of the interest and concern generated by this product and that is why we were keen to discuss the data protection implications with Google at the time the images were being collected.

You raise some important and interesting points which I will come to but I would first of all like to clarify the status of the comments attributed to ICO on this matter and take issue with your assertion that ICO gave a “green light” or an “approval” to Google. As you will be aware, it is important that organisations looking to develop new products can seek advice from the relevant bodies and that those bodies can approach such companies for information on how their products and services will be implemented. It was in this context that we spoke with Google about Streetview in July 2008. As a result of these discussions we did announce that we were satisfied that Google was putting in place adequate safeguards to avoid the risk to the privacy of individuals. Note that this was intended to express that we had been made aware of and were satisfied with the fact that actions were being taken to protect privacy. At this stage, it would not have been possible to approve of or even comment on the efficacy of those actions because they were some way off being deployed. You will know from your own work that it is important for organisations to be given advice such as this even where implementation might give rise to practical problems.

You ask for the basis on which this assessment was made and specifically whether we were provided with technical data regarding the blurring technology. We made the assessment based on the information provided by Google about how the product works and what steps they intended to take with regard to those

images which happen to include individuals or vehicle registration numbers. We did not request technical data about the blurring technology. In coming to our view it was not necessary to know how the technology actually operated, only that it would be in place – the significance in data protection terms of the blurring technology was not whether it could successfully ‘de-identify’ all individuals or registration plates captured by the Streetview camera but that it was the means by which the product was designed to minimise the risk to individuals whose image might be displayed. The fact that the technology has not been 100% successful should not be a surprise to anyone but it does not change our view that it was and remains an adequate safeguard put in place by Google to avoid unnecessary risk to the privacy of individuals. We also take into account that the efficacy of the technology improves with time and that the number of instances where a face has not been adequately disguised will gradually reduce. That it was likely to miss some images that should be blurred was the reason why we emphasised to Google the importance of including the facility for individuals to report problem images, that such a facility should be accessible to all users and that Google act promptly on those reports. We have not been contacted by any individuals concerned that a reported image has not been amended or removed.

It is entirely appropriate that when giving advice on the DPA98 we take at face value the information, explanation and assertions provided by the organisation we are advising. As a result, while we can be satisfied that what they have outlined to us is an accurate reflection of their intentions this would not prevent us from changing our view if it turns out that the assurances they give us turn out to be entirely without merit. In this case, while we are not surprised given the attention devoted to Streetview that it was possible to pick out images where the blurring had not been entirely effective we would only revisit our initial assessment if we were to receive continual and regular correspondence.

However, it is important to note that our assessment of Streetview was based on more than the capability of the system to blur faces and numberplates. Like you, we also make the point that blurring someone’s face is not guaranteed to take that image outside the definition of personal data. Even with a face completely removed, it will still be entirely likely that a person would recognise themselves or someone close to them. However, what the blurring does is greatly reduce the likelihood that lots of people would be able to identify individuals whose image has been captured. In light of this, our analysis of whether and to what extent Streetview caused data protection concerns placed a great deal of emphasis on the fact that at its core, this product is in effect a series of images of street scenes. Granted, it is a massive and systematic collection of such images but the important data protection point is that an individual’s presence in a particular

image is entirely incidental to the purpose for capturing the image as a whole. In other words, there is a great deal of difference between publishing images which might enable people to identify themselves and others they know well, and the publication of images which are intended to identify that a particular person was doing a particular thing at a particular time. In terms of our regulatory role, it is important for us to take this into account when assessing whether processing personal data in a particular way is likely to lead to a breach of the DPA98. As with other new uses of data we are asked to comment on, we feel that requiring the removal of an entire service would be disproportionate to the relatively small risk of privacy detriment. Indeed, while you assert that there have been a 'substantial' number of problematic images reported in the media I would argue that this number is relatively tiny considering the tens of millions of images published via Streetview and that it is tiny despite the intense level of attention given to Streetview by journalists in the first few days after its launch.

Moving away from the general assessment of the possible risks to privacy, it is important to address whether there are specific breaches of the legislation enforced by this office. Your complaint refers to the DPA98 and, indeed, states quite forcefully that "capturing images per se is unlawful". The Court of Appeal has recently clarified that there is a difference between street scenes which include images of individuals and images of individuals captured deliberately. Aside from that, it is not clear to me from your complaint which provisions of the law you feel have been breached though you do imply that it is unlawful to obtain images of people and use them without consent. In data protection terms this is simply not true. Notwithstanding my point above relating to the difference between an image in which a person happens to appear and an image of that person, if consent were required by the law, then the producers of, say, Match of the Day, would have to gain the consent of all people attending televised football matches who might be caught on camera. In particular those individuals who are picked out by the cameras as having an interesting reaction to a goal or because they are directors of a club facing a heavy defeat would have to be asked to give their consent prior to broadcast. Similarly, the numerous vox pops used to illustrate news stories about Streetview contained images of people walking past the interviewee. Even where these images could be stored and searchable via, say, BBC iPlayer, none of these people would have given their consent to their image being obtained.

In any event, consent is just one of the grounds for processing personal data and the regulatory focus must be on whether the processing is fair to individuals who might be identified and what safeguards are in place to deal with those relatively rare situations where it is not.

Moving on, you are correct to note that Streetview is not equivalent to a CCTV system. However, you then state that some of the provisions in the Information Commissioner's CCTV Code of Practice should be applied to Streetview. My first point is that, referring to the points made above, the Code of Practice does not require that CCTV systems can only operate on the basis of consent, even where the operators of the system are much more interested than Google in the whereabouts and identity of individuals. However, it is just as important to note that while you are right to suggest that some of the advice in the Code might apply to Streetview, this is because the Code is an explanation of how the provisions of the DPA98 apply to CCTV systems so by definition there will be some overlap as those principles apply to all processing of personal data. In other words, the focus here should be on compliance with the data protection principles and we do not feel that Streetview is per se a breach of those principles; applying the CCTV code would not add anything to this analysis.

You refer to the need to inform individuals that images are being captured. Again, I would stress that because of the very different purpose for capturing images, it is not helpful to apply the advice given to CCTV operators directly to this (or any other) mapping product. It would clearly be impracticable to provide what the Act terms fair processing information to any individual who happened to be in a public place at the same time as the Google cameras. We would not expect any organisation collecting images in this way to go to such lengths unless the images were being collected for purposes which required the identification of individuals and which resulted in some decision being taken about them. Also, I am not being too glib when I suggest that the media interest in Streetview has caused more people to be interested in the possibility that their data might be held in this way (and to search for it and, in some cases, request that it was removed) than is ever the case with CCTV signage.

You urge ICO to require Google to remove all images on the basis that Streetview operates outside the law. I hope the points made in this response are clear but perhaps I could summarise our position:

- It is true that Streetview is capable of obtaining personal data and that as a result it is necessary for Google to ensure that processing of that data is compliant with the DPA98
- In giving advice on compliance, ICO has taken into account the nature of the images displayed including the fact that images of people are incidental to the overall purpose of Streetview; that the images are snapshots rather than continuous footage; that Google has taken steps to reduce the possibility that individuals could be identified through blurring;

- that even where concerns remain, images can be reported and dealt with quickly
- So, our focus has to be on compliance with the DPA98 and in this regard your complaint does not require us to revisit our initial view on Streetview
- We will, of course, keep the operation of Streetview under review and take steps to address any issues raised by individuals who feel that Google has not removed problematic images.

I would take issue with your view that the ICO has put people at risk of intrusion by taking a pragmatic approach to regulation. We are pragmatic about giving guidance on and enforcing the Act and we would not apologise for that. However it is important to note that pragmatism is not the issue here – in this case we cannot conclude that the way Streetview operates is outside the requirements of the DPA98. You state that if the rights of the few are compromised then we should ensure that a system is not deployed. The inference to be drawn here is that in finding a balance between individual rights and commercial (or other) interests a regulator should always find in favour of individuals whose rights and interests might be compromised even where the potential for detriment is very low and where any associated risks are mitigated by safeguards put in place for exactly that purpose. I would argue that whilst we will always look at the impact on individuals in assessing data protection risks, such a sweeping approach is not only unpragmatic but impractical and that it would do the wider interest of privacy and data protection no good whatsoever – e-commerce, for example, brings with it obvious and specific privacy risks but we simply could not seek to stop it on that basis and neither should we; the pragmatic approach is to advise on good practice and enforce when necessary.

Finally, you mention that we should review our approach and take ‘community expectations’ into account. Our data protection strategy commits us to basing our interventions on what actually matters to those we are seeking to protect and how likely it is to occur. We do take the “community expectations” into account but it is clear to us that the “community” expect that good regulation is, to a large extent, pragmatic regulation. In our opinion, there is no clear evidence that the community find Streetview particularly harmful or insidious.

I hope I have been able to clarify the ICO position on this matter.

Yours sincerely

Dave Evans  
Senior Data Protection Practice Manager