Capitol Hill Briefing:
Street View, Privacy, and the Security of Wireless Networks
Washington DC, 18 May 2011

Statement by Peter Hustinx
European Data Protection Supervisor (EDPS)

The organisers of this meeting have invited me to make a brief contribution to the discussion. As I am unable to attend, I am pleased to submit a short written statement.

Let me mention, first of all, that Google Street View cars have not been active in my jurisdiction, which only covers the activities of EU institutions and bodies. However, it is among my tasks as EDPS to cooperate with national supervisory authorities to improve the consistency of data protection in the EU. In that capacity I have followed most - if not all - relevant inquiries and investigations in the EU.

All those inquiries and investigations have found that Google has been engaged, not only in the recording of images for its Street View service, but also in collecting data from wireless networks, involving both the content of communications and data on the location of devices, for a period of two years and without the users' knowledge.

The outcomes of these activities have been slightly different, due to subtle differences in national legislation and supervisory policies or priorities. Supervisory authorities have typically accepted explanations from Google that the collection of content was the result of a mistake on their part and insisted on the deletion of this information, either immediately or after a careful examination of the nature of that information. Where the information was examined, it was found to include sensitive personal data, such as medical data and information on financial transactions.

It is striking that the nature of the alleged mistake by Google engineers or other staff has not been clarified nor further investigated. In any case, it is hard to believe that the systematic collection and retention of such content, at a large scale and over a long period of time, was the result of a simple mistake and nothing more. Therefore, this

would certainly qualify for further investigation, if the opportunity for such an investigation would present itself.

A second important aspect relates to the collection of location data. Under EU data protection law, MAC addresses of WiFi routers, in combination with the location of those routers, qualify as 'personal data', because those data provide information on the owners of those routers, especially in the context of mobile communication, and in view of the very close link between the users and their mobile devices. The national authorities have therefore also set limits to the collection and retention of such data using their powers under existing data protection law.

This outcome is fully in line with the position of the Article 29 Working Party - the independent group of EU data protection regulators - expressed in its Opinion on Geo-location services on smart mobile devices (Opinion 13/2011) adopted on 16 May 2011. This opinion will soon be published on its website. It contains an overview of the current EU legal framework and its consequences for geo-location services and the different parties involved, ranging from providers of infrastructures, applications and services to developers of operating systems of smart mobile devices.

I hope that these comments are helpful for your discussions and further activities in this interesting and dynamic environment.

Brussels, 18 May 2011