Press Releases

March 12, 2013

MADIGAN ANNOUNCES $7 MILLION SETTLEMENT OVER GOOGLE STREET VIEW

Agreement Bans Unauthorized Data Collection, Requires Privacy Training for Employees & National Campaign on Protecting Personal Information

Chicago — Attorney General Lisa Madigan today joined with 37 states and the District of Columbia to announce a $7 million settlement with Google over its collection of personal data of Illinois residents and from consumers across the country while gathering data for its popular Street View service.

Under the agreement, Google also has agreed to destroy the personal data it collected, which could have included people's emails, passwords and browsing history shared over wireless Internet connections.

"While this agreement puts a stop to Google's unwarranted data collection, it should serve as an important reminder to Illinois residents to take the necessary steps to protect their personal information online," Madigan said.

Google Street View allows users to view actual photographs when using Google's map service or driving direction service. Google collects the images for Street View using vehicles equipped with antennae and open-source software that travel all over the world to photograph homes, buildings and other landmarks to include in these location-based services.

The agreement addresses practices by Google between 2008 and March 2010, when Street View vehicles collected network identification information for use in future geolocation services. At the same time, Google was collecting and storing data frames and other "payload data" that was being transmitted by consumers over unsecured business and personal wireless networks. Payload data can include user emails, passwords and browsing activity.

Google has since disabled or removed the equipment and software used to collect payload data from its Street View vehicles. Under the agreement with Madigan and the attorneys general, Google must not collect any additional information without notice and consent.

Google has maintained that it never used the data collected and that the information collected in the United States was not disclosed to a third party. Under the agreement, information collected by Google was segregated and secured and must now be destroyed.

In addition, Google must conduct employee trainings on privacy and confidentiality of user data for at least 10 years. The company must also conduct a public service advertising campaign to help educate consumers about steps they may take to better secure their personal information while using wireless networks.

Protect Your Online Identity
Madigan also recommended Illinois residents consult OnGuard Online, a consortium of federal government agencies and technology industry experts, which recommends additional precautionary steps to secure wireless networks and to ensure safe web browsing. The steps below are provided by OnGuard Online:

1. **Use anti-virus and anti-spyware software and a firewall:** Install anti-virus and anti-spyware software. Keep them up-to-date, and check to ensure that your firewall is turned on.
2. **Change the identifier on your router from the default.** The identifier (SSID) for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate.

3. **Change your router's pre-set password for administration:** The manufacturer assigned the router a standard default password. Those default passwords are available to anyone, including hackers, so change it to something only you know. When choosing a password, make sure to choose one of sufficient length and complexity to prevent it from being hacked.
4. **Turn off your wireless network when you know you won't use it:** If you turn the router off when you're not using it, you can limit the amount of time that it is susceptible to a hack.
5. **Don't assume public Wi-Fi networks are secure:** Café, hotel and airport "hot spots" are convenient, but they are not secure.

Joining Madigan in today's settlement were attorneys general from Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Hawaii, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia and Washington.

Assistant Attorney General Matthew Van Hise handled the case for Madigan's Consumer Fraud Bureau.

-30-

Return to March 2013 Press Releases

TOP