



ATTORNEY GENERAL GEORGE JEPSEN

ATTORNEY GENERAL GEORGE JEPSEN ADVISES RESIDENTS TO SECURE WIRELESS INTERNET NETWORKS

For Immediate Release

FRIDAY JAN. 28, 2011

HARTFORD – In recognition of Data Privacy Day, Attorney General George Jepsen Friday advised Connecticut residents to protect their personal and communications data by encrypting their own wireless Internet networks.

The recommendation stemmed from Connecticut’s investigation into Google Inc.’s collection of payload data being transmitted over unsecured business and consumer networks. That investigation led to a stipulation with Google that will avoid the need to go to court as settlement negotiations continue.

“Google’s collection of payload data demonstrates that others may be watching your Internet activity without your knowledge,” Jepsen said. “Consumers should know that the wireless routers they purchase from the store are not automatically encrypted, and they need to activate the encryption feature to ensure better protection,” Jepsen said.

Payload data may include user e-mails, passwords and browsing activity. Jepsen also urged consumers to review their privacy settings on social media sites, such as Facebook, to make sure they are controlling the information they share.

Manufacturers often deliver wireless routers with the encryption feature turned off, Jepsen said. Consumers should consult the instructions for their wireless router or obtain additional information from the manufacturer’s website to enhance the security of their home networks.

OnGuard Online, a consortium of federal government agencies and technology industry experts recommends additional precautionary steps to secure wireless networks. Details are available at <http://www.onguardonline.gov/topics/wireless-security.aspx>.

The consortium recommends:

1. Use anti-virus and anti-spyware and a firewall.
2. Turn off identifier broadcasting.
3. Change the identifier on your router from the default.
4. Change your router’s pre-set password for administration.
5. Turn off your wireless network when you know you won’t use it.
6. Don’t assume that public “hot spots” are secure.
7. Be careful about the information you access or send from a public wireless network.

Data Privacy Day is recognized by the National Association of Attorneys General to raise awareness about data privacy and to educate consumers about ways to protect themselves from financial fraud or privacy offenses.