ADVISORY

Federal Communications Commission
445 12th Street, S.W.
Washington, D. C. 20554

News Media Information 202 / 418-0500
Internet: http://www.fcc.gov
TTY: 1-888-835-5322

FOR IMMEDIATE RELEASE:
June 11, 2010

NEWS MEDIA CONTACT:
Dan Rumelt at 202-418-7512
Email: Dan.Rumelt@fcc.gov

BLOG ALERT: FCC POSTS BLOG ON RECENT REPORTS ABOUT ACCESS TO PERSONAL DATA ON GOOGLE AND AT&T NETWORKS

Washington, DC – Federal Communications Commission's Chief of the Consumer and Governmental Affairs Bureau, Joel Gurin, posted a blog today responding to concerns about recent breaches by Google and AT&T. The text of the blog follows. The blog can be accessed online at: http://reboot.fcc.gov/blog?entryId=493624.

BLOG TEXT: Consumer View: Staying Safe from Cyber Snoops

Recent news reports have focused attention on a growing concern: The ways in which wireless and WiFi networks can make consumers' private data accessible.

In May, Google reported that its Street View cars – used to develop Google Maps – had mistakenly collected personal information sent over WiFi as they drove around, in addition to gathering less intrusive data about the WiFi networks themselves. http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html

Now this week, a group of hackers reported that it had gotten the e-mail addresses of more than 100,000 Apple iPad owners by hacking the Web site of AT&T, Apple's partner. The hackers also got the ID numbers the iPads use to communicate over the network. The Google and AT&T incidents are different kinds of intrusions, each worrisome in its own way, and each with a different remedy.

The iPad incident appears to be a classic security breach – the kind that could happen, and has happened, to many companies – and is exactly the kind of incident that has led the FCC to focus on cyber security. Our Public Safety and Homeland Security Bureau is now addressing cyber security as a high priority. The FCC's mission is to ensure that broadband networks are safe and secure, and we're committed to working with all stakeholders to prevent problems like this in the future.

Google's behavior also raises important concerns. Whether intentional or not, collecting information sent over WiFi networks clearly infringes on consumer privacy. Here, there are some immediate remedies. The Google incident is a reminder that "open" WiFi networks – those that are not encrypted – are all too vulnerable to cyber snooping. The Federal Trade Commission

has a guide to wireless safety at http://www.onguardonline.gov/topics/wireless-security.aspx that can help you keep your information safe over WiFi. As consumers explore the many benefits of WiFi and mobile broadband, we would all do well to keep these important safeguards in mind.

- FCC -