United States Attorney
District of New Jersey

FOR IMMEDIATE RELEASE
January 18, 2011
www.justice.gov/usao/nj

CONTACT: Rebekah Carmichael
Office of Public Affairs
(973) 645-2888

TWO MEN CHARGED IN NEW JERSEY WITH HACKING AT&T'S SERVERS

Defendants Allegedly Stole E-mail Addresses and Personal Information Belonging to 120,000 Apple iPad 3G Subscribers

NEWARK, N.J. – Two self-described Internet "trolls" were arrested today for allegedly hacking AT&T's servers and stealing e-mail addresses and other personal information belonging to approximately 120,000 Apple iPad users who accessed the Internet via AT&T's 3G network, United States Attorney Paul J. Fishman announced.

Andrew Auernheimer, 25, of Fayetteville, Ark., and Daniel Spitler, 26, of San Francisco, Calif., were taken into custody this morning by special agents of the FBI – each charged with an alleged conspiracy to hack AT&T's servers and for possession of personal subscriber information obtained from the servers. Auernheimer was arrested in Fayetteville while appearing in Arkansas state court on unrelated drug charges, and is expected to appear this afternoon before United States Magistrate Judge Erin L. Setser in Fayetteville federal court. Spitler surrendered to FBI agents in Newark and is expected to appear in Newark federal court before United States Magistrate Judge Claire C. Cecchi.

According to the Complaint unsealed today:

The iPad is a touch-screen tablet computer, developed and marketed by Apple Computers, Inc., which allows users to, among other things, access the Internet and send and receive electronic mail. Since the introduction of the iPad in January 2010, AT&T has provided iPad users with Internet connectivity via AT&T's 3G wireless network. During the registration process for subscribing to the network, a user is required to provide an e-mail address, billing address, and password.

Prior to mid-June 2010, AT&T automatically linked an iPad 3G user's e-mail address to the Integrated Circuit Card Identifier ("ICC-ID"), a number unique to the user's iPad, when he registered. As a result, every time a user accessed the AT&T website, his ICC-ID was recognized and his e-mail address was automatically populated for faster, user-friendly access to the site. AT&T kept the ICC-IDs and associated e-mail addresses confidential.

At that time, when an iPad 3G communicated with AT&T's website, its ICC-ID was automatically displayed in the Universal Resource Locator, or "URL," of the AT&T website in plain text. Seeing this, and discovering that each ICC-ID was connected to an iPad 3G user e-mail address, hackers wrote a script termed the "iPad 3G Account Slurper"and deployed it

against AT&T's servers.

The Account Slurper attacked AT&T's servers for several days in early June 2010, and was designed to harvest as many ICC-ID/e-mail address pairings as possible. It worked by mimicking the behavior of an iPad 3G so that AT&T's servers would be fooled into granting the Account Slurper access. Once deployed, the Account Slurper used a process known as a "brute force" attack – an iterative process used to obtain information from a computer system – against the servers, randomly guessing at ranges of ICC-IDs. An incorrect guess was met with no additional information, while a correct guess was rewarded with an ICC-ID/e-mail pairing for a specific, identifiable iPad 3G user.

From June 5 through June 9, 2010, the Account Slurper stole for its hacker-authors approximately 120,000 ICC-ID/e-mail address pairings for iPad 3G customers.

Immediately following the theft, the hacker-authors of the Account Slurper provided the stolen e-mail addresses and ICC-IDs to the website Gawker, which published the stolen information in redacted form, along with an article concerning the breach. The article indicated that the breach "exposed the most exclusive email list on the planet,"and named a number of famous individuals whose emails had been compromised, including Diane Sawyer, Harvey Weinstein, Mayor Michael Bloomberg, and Rahm Emanuel. The article also stated that iPad users could be vulnerable to spam marketing and malicious hacking. A group calling itself "Goatse Security" was identified as obtaining the subscriber data.

According to its website, Goatse Security is a loose association of Internet hackers and self-professed Internet "trolls" – people who intentionally, and without authorization, disrupt services and content on the Internet – to which both Spitler and Auernheimer belong. Auernheimer previously has been outspoken about his trolling activities, bragging to *The New York Times* in August 2008: "I hack, I ruin, I make piles of money." Auernheimer has also made Internet video postings taking credit for trolling Amazon.com and causing a "one billion dollar change in their market capitalization."

During the data breach, Spitler and Auernheimer communicated with one another using Internet Relay Chat, an Internet instant messaging program. Those chats not only demonstrate that Spitler and Auernheimer were responsible for the data breach, but also that they conducted the breach to simultaneously damage AT&T and promote themselves and Goatse Security. As the data breach continued, so too did the discussions between Spitler, Auernheimer, and other Goatse Security members about the best way to take advantage of the breach and associated theft. On June 10, 2010, immediately after going public with the breach, Spitler and Auernheimer discussed destroying evidence of their crime.

U.S. Attorney Fishman stated: "Hacking is not a competitive sport, and security breaches are not a game. Companies that are hacked can suffer significant losses, and their customers made vulnerable to other crimes, privacy violations, and unwanted contact. Computer intrusions

and the spread of malicious code are a threat to national security, corporate security, and personal security. Those who use technological expertise for malicious purposes take note: your activities in cyberspace can have serious consequences for you in the real world."

"One primary principle of our society is confidence in a reasonable expectation of personal privacy, which includes expectations of financial privacy, medical privacy, and privacy in our communications," said Michael B. Ward, Special Agent in Charge of the FBI's Newark field office. "Unauthorized intrusions into personal privacy adversely affect individual citizens, businesses, and even national security. Such intrusion cases, regardless if the motive is criminal gain or prestige among peers in the cyber-hacking world, must and will be aggressively pursued to ensure these rights are protected to the highest degree."

Each defendant is charged with one count of conspiracy to access a computer without authorization and one count of fraud in connection with personal information. Each count with which the defendants are charged carries a maximum potential penalty of five years in prison and a fine of $250,000.

U.S. Attorney Fishman credited special agents of the FBI, under the direction of Special Agent in Charge Michael B. Ward in Newark, with the investigation leading to the charges. He also thanked special agents of the FBI, under the direction of Special Agent in Charge Valerie Parlave in Little Rock, Ark., and the U.S. Attorney's Office for the Western District of Arkansas, under the direction of U.S. Attorney William Conner Eldridge.

The government is represented by Assistant United States Attorneys Lee Vartan and Zach Intrater of the Computer Hacking and Intellectual Property Section of the United States Attorney's Office Economic Crimes Unit.

The charges and allegations contained in the Complaint are merely accusations, and each defendant is presumed innocent unless and until proven guilty.

11-025 ###

Defense counsel:
Spitler: Susan C. Cassell, Esq., Ridgewood, N.J.
Auernheimer: Candace Hom, Esq., Federal Public Defender, Newark