

**FCC CHAIRMAN GENACHOWSKI JOINS SENATOR SCHUMER, D.C. MAYOR GRAY,
STATE POLICE DEPARTMENTS, AND WIRELESS CARRIERS TO ANNOUNCE NEW INITIATIVES
TO COMBAT MASSIVE SMARTPHONE & DATA THEFT**

**WIRELESS INDUSTRY COMMITS TO CENTRALIZED DATABASE SYSTEM IN SIX MONTHS TO PREVENT
REACTIVATION OF STOLEN CELL PHONES, CONSUMER CAMPAIGN**

FCC TO CONSUMERS: USE LOCATE, LOCK & WIPE APPS TO PROTECT DATA

FCC Chairman Julius Genachowski joined major police department chiefs, including New York City Police Commissioner Raymond E. Kelly, Philadelphia Police Department Commissioner Charles Ramsey, Washington, D.C. Metropolitan Police Chief Cathy Lanier, Washington, D.C. Mayor Vincent Gray, wireless carriers, and Senator Chuck Schumer to announce new initiatives to combat cell phone and data theft. Genachowski commended police departments and members of Congress, in particular Senator Schumer, for calling attention to a growing epidemic of robberies targeting smartphone users. Genachowski announced an industry commitment to develop a shared, centralized database that will record unique identifiers of stolen wireless devices to prevent their reuse, thereby making it harder for thieves to resell stolen wireless devices. Legislation, sponsored by Senator Schumer, will ensure that authorities have the tools they need to crack down on efforts to evade this technological solution.

There is a growing epidemic of robberies involving smartphones and other cell phones:

- More than 40% of all robberies in New York City involve smartphones and other cell phones.
- The situation is getting worse: In Washington, D.C., cell phones were taken in 54% more robberies in 2011 than in 2007, and cell phones are now taken in 38% of all DC robberies.
- Other major cities have similar statistics, with robberies involving cell phones comprising 30-40% of all robberies.
- Robberies are, by definition, violent crimes, and there are many instances of robberies targeting cell phones resulting in serious injury or even death.
- A recent Symantec study indicates that a loss or theft of an unsecured smartphone often results in access to sensitive personal data.

Chairman Genachowski, with the support of major city police chiefs and the wireless industry, announced new initiatives by wireless carriers, initially including AT&T, T-Mobile, Verizon and Sprint who cover 90 percent of US subscribers, to deter theft and secure customer data:

- **Implement a database to prevent use of stolen smartphones.** Within six months, when Americans call their participating wireless provider and report their wireless devices stolen, their provider will block that device from being used again. This system will be rolling out globally using common databases across carriers over the next 18 months.
- **Encourage users to lock their phones with passwords.** Smartphone makers will notify and educate users in the most highly visible ways—through messages on the smartphone itself and through “Quick Start” user guides—about how to use passwords to deter theft and protect their data.
- **Educate users on lock/locate/wipe applications.** Wireless providers will directly inform their customers about how to find and use applications that enable customers to lock/locate/and wipe smartphones remotely.
- **Public education campaign on how to protect your smartphone and yourself.** The wireless industry will launch a campaign, with media buys, to educate consumers on how to protect their smartphones and themselves from crime.
- **Progress benchmarks and ongoing dialog.** The wireless industry will publish quarterly updates and submit them to the FCC on progress on these initiatives.

Accountability:

- The FCC will engage the public safety community and wireless carriers in an ongoing dialog, with regular, quarterly meetings, to ensure that the most effective technological processes are in place to deter smartphone theft and data exposure.
- The FCC will launch a proceeding if progress on the above deliverables falls behind schedule.

Legislation expected to criminalize tampering with unique hardware IDs on cell phones:

- Members of Congress are planning to introduce legislation that will make it a federal crime to take steps to evade the effective deployment of a stolen phone database, including by tampering with hardware identifiers on wireless devices.
- Criminalizing tampering with unique hardware identifiers has been an integral part of successful foreign deployments of stolen cell phone databases and the deterrence of cell phone theft.