Cell phones reveal more than users may realize

By Massimo Calabresi, Time

If someone wanted to create a global system for tracking human beings and collecting information about them, it would look a lot like the digital mobile-device network. It knows where you are, and – the more you text, tweet, shop, take pictures and navigate your surroundings using a smart phone – it knows an awful lot about what you’re doing.

Which is one reason federal officials turned to Sprint, Verizon, AT&T and T-Mobile in early 2009 when they needed to solve the robbery of a Berlin, Conn., branch of Webster Bank. Using a loophole in a 1986 law that allows warrantless searches of stored communications, the feds ordered the carriers to provide records of phones that used a nearby cell tower on the day of the crime. The carriers turned over to the prosecutors the identities, call records and other personal information of 169 cell-phone users–including two men who were eventually sentenced to prison for the robbery. With a simple request, the feds cracked a case that might have otherwise taken years to solve.

In the process, they collected information on 167 people who they had no reason to believe had committed a crime, including details like numbers dialed and times of calls that would have been protected as private on a landline.

Such cases are common. In response to a request from Representative Ed Markey, major cell carriers revealed in July that they had received more than 1.3 million requests for cell-phone tracking data from federal, state and local law-enforcement officials in 2011.

By comparison, there were 3,000 wiretap warrants issued nationwide in 2010.

That revelation has added to a growing debate over how to balance the convenience and security consumers now expect from their smart phones with the privacy they traditionally have wanted to protect. Every second we enjoy their convenience, smart phones are collecting information, recording literally millions of data points every day.

The potential for good is undeniable. In recent years, the average time it takes the U.S. Marshals Service to find a fugitive has dropped from 42 days to two, according to congressional testimony from Susan Landau, a Guggenheim fellow.

Cell phones have changed criminal investigation from the ground up.

“There is a mobile device connected to every crime scene,” says Peter Modafferi, the chief of detectives in Rockland County, New York.

But as smart phones’ tracking abilities have become more sophisticated, law enforcement, phonemakers, cell carriers and software makers have come under fire for exploiting personal data without the knowledge of the average user. Much of the law protecting mobile privacy in the U.S. was written at the dawn of the cell-phone era in the 1980s, and it can vary from state to state. Companies have widely differing privacy policies.

Now conservatives and liberals on Capitol Hill are pushing legislation that would set new privacy standards, limiting law-enforcement searches and restricting what kinds of information companies can collect.

Read the whole story