Privacy

You’re Under Arrest! Hand Over That iPhone

► Police buy up devices that break passwords to get at suspects’ data

► “There’s a lot of valuable evidence on those phones”

The spread of smartphones is increasing the popularity of a different sort of handheld device: “forensic extraction” tools that allow law enforcement officials to crack suspects’ mobile phones and mine them for incriminating information.

About the size of a chunky paperback, they plug into almost any phone to peer into e-mails, photos, and Web histories.

The federal government, the Pentagon, and police departments across the country, including New York and Los Angeles, now use the devices, which cost a few thousand dollars for basic versions and as much as $11,500 for models that can retrieve deleted files. (No, you can’t buy one; they’re sold for official use only.) Sheriff’s investigators in Sacramento pulled pictures and texts from gang members’ phones to build a successful murder case against a 16-year-old who killed an officer. U.S. Immigration and Customs Enforcement, an agency under the Department of Homeland Security, “has about 100 of these devices in the field,” according to spokesperson Danielle Bennett, who says the agency uses them to scan suspects’ mobile phones in money laundering and drug smuggling investigations. The U.S. Army uses the technology for “the capture of critical mission information from apprehended digital devices,” according to government documents. “People’s PCs are basically in their hand now,” says Jim Grady, chief executive officer of Cellebrite USA in Glen Rock, N.J., a leading maker of the devices. “There’s a lot of valuable evidence on those phones.” There are also a lot of questions about whether taking that evidence violates constitutional protections against unreasonable searches and seizures. The authority of arresting officers to pat down a suspect or go through his pockets is well established. “But the idea that you would pull all the data that they might have about any number of activities and private matters is really a stretch to a new dimension,” says Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington. “It’s just too easy to pull too much.”

The question comes down to whether plundering information from a suspect’s phone is similar to searching his pockets or more like a search of his house, which usually requires a warrant. Bennett says Homeland Security extracts phone data “pursuant to a judicially authorized search warrant” or after getting consent. Dan Morrissey of the Sacramento Sheriff’s Department says about 80 percent of the mobile searches he does are tied to a warrant. He says court approval isn’t always required for people on parole or probation, or to search a device at the time of arrest.

Courts are split on whether it’s fair game to examine the contents of a mobile phone without a warrant. Last year the California Supreme Court ruled, 5 to 2, that a warrantless cell phone search in a drug case was permissible because the phone was in the suspect’s immediate possession. The justices said its capacity to store personal information wasn’t relevant. Ohio’s Supreme Court reached the opposite conclusion, ruling in 2009 that warrantless phone searches at the time of arrest are prohibited in most cases. The phones store “a wealth of digitized information” and people have an expectation that it’s private, the court said. It may be up to the U.S. Supreme Court to settle the matter.

Meanwhile, the market for mobile-phone-forensics devices is rapidly expanding. The military and government agencies—including Homeland Security, the FBI, and the Drug Enforcement Administration—awarded at least $5.7 million in contracts for the products in fiscal 2011, up 1,066 percent from five years ago, according to data compiled by Bloomberg. Once a novelty, the ability to rummage through smartphones has become a routine part of law enforcement. “Realistically,” says Morrissey, “we use it now on a daily basis.”

—Nick Taborek

The bottom line The U.S. government spent $5.7 million on “forensic extraction” technology in fiscal 2011, up 1,066 percent from five years ago.