Fighting Crime with Mobile Technology

Mobile technology has become a powerful crime-fighting tool.

Cell phones contain call history, contacts, text messages, web browser history, email, a Global Positioning System (GPS), and other location information that police and law enforcement agencies find valuable. Evidence from cell phones can help investigators piece together motives and events and provide new leads.

“Smartphones and cell phones have become a regular part of criminal investigations because they are now owned by most people and provide information about a person’s whereabouts and a person’s contacts,” says Adam Pincus, a Legal instructor at South University, Online Programs. “This helps to jumpstart a criminal investigation.”

Digital forensics is a branch of science encompassing the recovery and investigation of material found in digital devices, including computers, cell phones, and digital cameras.

Tracking Criminals and Crime

Every time someone uses a cell phone, a signal is sent out that pinpoints where the user is. Cell towers and the GPS features in some smartphones track where a phone is at any moment. Cell phone carriers can provide authorities with a cell phone’s location via proper court documents.

Tracking subjects via their mobile devices has been utilized for many years and has become very much a part of many, if not all, investigations.

“Cell phone records can identify calls made and received. You also can obtain the cellular towers that were used in the conversation, SMS (short message service), or data communication,” says Lee Reiber, director of mobile forensics for AccessData, a provider of digital investigations, cyber security, and electronic discovery. “The cell phone records hold latitude and longitude information and can be used as a historical reference to where the mobile device was at a particular time.”

In addition to collecting cell phone communication records, police also encourage citizens to use their mobile devices to report crimes and send in tips.

“Police often reach out to the public and make it clear to them when they need help in an investigation,” Pincus says. “They will ask people who may have taken a picture that is related to the investigation to share it with them.”

People can send their digital photos and videos of crimes in progress to 911 call centers in some cities. New technology allows sent images to be directly added to the record of a related call, and be forwarded to emergency responders on their way to the scene. An example of such technology is CrimePush, a multiplatform smartphone app that allows users to report crimes quickly and efficiently. It also gives users the ability to send multiple, GPS-tagged distress messages to designated emergency contacts.

High-profile incidents throughout the world have proven how valuable mobile phone images can be to crime investigations.

The London bombings in July 2005 marked a turning point in news coverage and the role of camera phone images. Witnesses to the attacks used their cell phone cameras to record their experiences in the aftermath. Not only did it signal a new era of citizen journalism, but police in London were able to use the cell phone photos as clues to find the terrorists behind the bombings.

Just this April, investigators of the Boston Marathon bombings collected photos and video from cell phones and surveillance cameras to aid their investigation.
Seconds after the bombs exploded at the marathon, Jacksonville Beach, Fla., businessman and marathon runner David Green pulled out his smartphone and took a photo of the chaos developing. He then put his phone away and helped the injured. After officials released a surveillance video of the two bombing suspects, Green realized he had a picture of suspect Dzhokhar A. Tsarnaev walking away from the scene. Editors of The Associated Press were able to establish the authenticity of Green’s photo and established an exclusive arrangement for distribution of the photograph.

In addition to photos and video, text messages are proving to be helpful in investigations.

Text messages are more discreet and safer in some circumstances, such as kidnappings or burglaries. Many police departments throughout the country have text-a-tip programs that allow people to send anonymous text messages from their cell phones. In order to provide people with a confidential means of communication, text messages are sent to a separate third-party server where identifying information is removed and assigned an encrypted alias to ensure callers’ anonymity.

Crimes Using Cell Phones

Identity theft, stalking, fraud, pornography, illegal electronic surveillance, and theft of intellectual property are just some of the examples of crimes committed every day on mobile devices.

“A mobile device is simply a portable computing device, so any crime that can be perpetuated on a computer can be committed via a mobile device,” says Reiber, who was formerly a computer forensics specialist for the Boise (Idaho) Police Department.

The portability of mobile devices makes it difficult, but not impossible, to identify the source of an electronic crime, he adds.

“If a user is using a public wi-fi, a ‘burner’ prepaid phone, cloud storage, or any other anonymizing agent, difficulties in identification is compounded,” Reiber says.

Law enforcement agencies will continue to be challenged to obtain the tools and the training to perform competent digital forensics investigations and keep pace with criminal activity.