SECURE IN OUR CONVICTIONS

Using New Evidence to Strengthen Prosecution

KRISTINE HAMANN AND
REBECCA RADER BROWN

In May 2013, a Colorado man fails to show up to work. Concerned, the man's boss visits his house, where the man's roommate refuses to let the boss enter. The boss contacts the police, who launch a missing person investigation.

Using cell tower technology, police are able to approximate the missing man's location in the hours leading up to his disappearance. Cell phone data also suggests that the roommate's phone traveled to and from a remote area where, three weeks later, the man's body is discovered. On the day of the disappearance, bank ATM records show repeated mistaken entries of the victim's PIN before someone withdrew a large sum of money, and a bank surveillance video shows the victim's car present at the time of the transaction. That same day, surveillance video at a gas station shows the roommate driving the victim's car and wearing his jacket. Another supermarket surveillance video from the same day shows the roommate purchasing bleach.

Several decades earlier—without surveillance video, cell phone records, and electronic bank records—this crime might have gone unsolved. With no eyewitnesses and no one to contradict the roommate's alibi, prosecutors would have had difficulty filing charges and securing a conviction. Instead, armed with all of this evidence, prosecutors were prepared to bring murder charges against the victim's roommate with or without a body. After a 12-day trial and one day of deliberations, jurors convicted the roommate of first-degree murder and sentenced him to life in prison. (*See Ryan Hicks*, CBS Denver, http://tinyurl.com/ybs5dar9 (last visited Nov. 26, 2017).)

A prosecutor's job is, and has always been, to seek justice—for victims, families, communities, and the accused. Today, new types of evidence are helping law enforcement and prosecutors conduct more thorough and accurate investigations. Though the evidence used years ago continues to play a valuable part in a criminal case, the improvements in science and technology are enabling police and prosecutors to solve more crimes more reliably than ever before.

NEW FORMS OF EVIDENCE

The following is an overview of the forms of evidence increasingly used by prosecutors over the past several decades. Each section provides a brief history of the technology, as well as a summary of the technology's current capabilities. Though this article occasionally alludes to legal issues, it is not intended to address the legal standards for acquiring evidence and introducing it in court. Case examples are

KRISTINE HAMANN is the founder and executive director of Prosecutors' Center for Excellence, whose mission is to develop and support statewide nonpartisan best practices committees for prosecutors that are working to improve the criminal justice system. She can be reached at khamann@pceinc.org.

REBECCA RADER BROWN is an attorney in the commercial litigation and government & internal investigations groups with Finn Dixon & Herling LLP in Stamford, Connecticut. She can be reached at rbrown@fdh.com.

The writing of this article was supported in part by Grant No. 2013-DB-BX-K005 awarded by the Bureau of Justice Assistance to the New York Prosecutors Training Institute (NYPTI). Points of view or opinions in these materials are those of the authors and do not necessarily represent the official position or policies of the US Department of Justice.

given to illustrate how the evidence has proven helpful to prosecutors and law enforcement. Some examples are based on high-profile cases, while others are based on reports from prosecutors throughout the country. (The authors are grateful to the many prosecutors who responded to requests for sample cases in the course of researching this article. Wherever possible, we have cited to media coverage of the cases discussed.)

DNA EVIDENCE

In 1953, researchers identified DNA (deoxyribonucleic acid), the chemical source of genes. (*This Day in History: Feb. 28, 1953—Watson and Crick Discover Chemical Structure of DNA*, Hist. Channel, http://tinyurl.com/cwgxr6u (last visited Nov. 26, 2017).) In the 1960s and 1970s, the field of molecular genetics emerged as scientists learned to "read" DNA. Forensic DNA testing began in 1985. (Randy James, *DNA Testing*, Time (June 19, 2009), http://tinyurl.com/j54nzqe.) Three years later, Tommie Lee Andrews became the first person in the United States to be convicted due to DNA evidence in his rape trial. DNA from semen found in the victim matched his blood sample, ensuring his conviction. (*See Rapist Convicted on DNA Match*, N.Y. Times, Feb. 6, 1988, http://tinyurl.com/y7c43euy.) In the years that followed, DNA emerged as "the most reliable physical evidence at a crime scene, particularly those involving sexual assaults." (James, *supra*.)

DNA databases are now widespread. "All 50 states and the federal government have laws requiring that DNA samples be collected from some categories of offenders." (*Advancing Justice through DNA Technology: Using DNA to Solve Crimes*, U.S. Dep't of Justice, http://tinyurl.com/kss9p3e (last updated Mar. 7, 2017).) Additionally, 23 states require all convicted felons to provide DNA samples. (*Id.*) State and federal laws determine the types of criminal offenders required to submit DNA samples to each database. The FBI manages the Combined DNA Index System (CODIS), which supports state criminal justice DNA databases and software, and the National DNA Index System (NDIS), which links state and federal databases together, allowing efficient comparison of DNA profiles.

State DNA databases include at least two categories of profiles: samples collected directly from known offenders or detainees (offender profiles), and those gathered at crime scenes (forensic profiles). (*Frequently Asked Questions on CODIS and NDIS*, FBI, http://tinyurl.com/hjkxu5w (last visited Nov. 26, 2017); *see also Combined DNA Index System (CODIS)*, FBI, http://tinyurl.com/yc5vtjta (last visited Nov. 26, 2017).) By collecting and cross-referencing samples, investigators can solve crimes more effectively than ever before. For example, a sample collected at a crime scene might match the profile of a known offender. Likewise, a sample collected from a suspect could match biological material from an old crime scene, allowing investigators to solve a cold case. As of October 2017, NDIS contains over 13 million offender profiles, nearly three million arrestee profiles, and more than 800,000 forensic crime scene profiles. (*CODIS-NDIS Statistics*, FBI, http://tinyurl.com/ya6bzckq (last visited Nov. 26, 2017).)

Advances in DNA analysis techniques have reduced the required body fluid or tissue sample size, allowed for extraction of DNA from degraded or mixed samples, and cut down the time needed to create a DNA profile. (Jennifer M. Romeika & Fei Yan, *Recent Advances in Forensic DNA Analysis*, S12 J. Forensic Res. 1 (2013).) For example, a process known as DNA amplification allows scientists to test degraded samples by finding and replicating the sample's untainted regions and thus generate more usable amounts of DNA. (*Id.*) Rapid testing is under development to enable creation of a profile compatible with DNA databases in one to two hours. (*Rapid DNA*, FBI, http://tinyurl.com/yalzpr9p (last visited Nov. 26, 2017).)

A murder case in Virginia is an excellent example of how DNA collection can prove useful. In 2009, a man was fatally stabbed and robbed on his way to work. Police swabbed the man's pockets, which had been turned inside out during the robbery, and created a new DNA profile in the state's crime scene database. The profile did not initially match any known offender, but police were able to solve the crime a year later when the profile matched a man added to the offender database. From the DNA, the police identified the suspect, who confessed to the crime and testified against his accomplice. Neither of the perpetrators had any ties to the victim, so without DNA evidence the murder almost certainly would have remained unsolved.

DNA evidence is particularly useful in solving cold cases involving rape, because rape kits collected from victims often provide DNA evidence from the attacker. Forensic profiles created from the rape kit can be stored for decades, allowing law enforcement to cross-reference forensic profiles with new offender profiles added to the database. A Michigan case demonstrates how effective DNA databases can be at solving cold cases. A man was convicted in 2015 of felony drug charges and, pursuant to state law, was required to submit a DNA sample to the Michigan Convicted Offender Database. The DNA sample matched the forensic profile from a 2001 Michigan rape case, as well as profiles from two rape cold cases in Texas from the early 2000s. (John Agar, *DNA Links Suspect to Cold-Case Rape, Victim "Relieved" by Arrest, Police Say*, MLive.com (Sept. 8, 2015), http://tinyurl.com/y7wustmj.)

SURVEILLANCE CAMERAS

Due to the widespread use and sophistication of surveillance technology, it is one of the most common and useful forms of digital evidence available today. Law enforcement officers, business owners, and private individuals have installed surveillance cameras in many places of business, public spaces, traffic lights, and private homes.

Video surveillance was first used in the 1950s, long before the technology was digital. Public surveillance by police departments began in Hoboken, New Jersey, in 1966, and Mount Vernon, New York, in 1971. (Robert D. Bickel et al., *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?*, 33 Stetson L. Rev. 299 (2003).) Improvements in the technology in the 1980s and 1990s led to its increased use, but the images were low-resolution and grainy, making them difficult to use.

Digital surveillance cameras, which produce clearer, higher-quality images, were first installed on street corners in major urban areas like New York, Chicago, and Washington, D.C. In 2006, Chicago launched Operation Virtual Shield, which linked together a vast network of police and private cameras estimated to number in the tens of thousands. (William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, Wall St. J., Nov. 17, 2009, http://tinyurl.com/y947u4yg.) Cameras are now commonplace in less populous cities, as well as in suburban and rural communities throughout the United States. One assistant district attorney with whom we spoke explained that the proliferation of these devices "has altered the old-fashioned,

shoe-leather techniques employed by detectives. Where previously cops canvassed the vicinity of a crime in search of a witness who may have observed anything, now the canvass is as much focused on retrieving any evidence from surveillance equipment—evidence which often proves to be the most significant information gathered during the course of an investigation."

In one well-known example, surveillance cameras captured the Ryder truck used by the Oklahoma City bombers in the moments before the explosion, producing footage that later became trial evidence. (Jo Thomas, *Jurors See Chilling Images of Truck before Bombing*, N.Y. Times, May 15, 1997, http://tinyurl.com/y94qjgtx.) In another case, when an elderly Michigan woman went missing, police and prosecutors used surveillance footage from a nearby gas station, a hotel, and highway cameras to contradict her husband's alibi. The evidence showed the husband traveling to and from the area where his wife's body was later discovered, and he was convicted of her killing. (*See* Cortney Ofstad, *Peters Murder Trial Continues*, Your Daily Globe (Apr. 24, 2013), http://tinyurl.com/y982f86n.)

Likewise, surveillance footage may also be used on behalf of someone wrongfully accused. In a Tennessee case, prosecutors used surveillance videos to determine that a witness had mistakenly identified a defendant, thereby exonerating him.

COMPUTERS

Personal computers (PCs) became increasingly popular in the 1980s, leading to the use of computer evidence in criminal investigations. The rise of the Internet in the 1990s similarly boosted sales of the PC. The number of American households with a computer jumped from 8 percent in 1984 to 79 percent in 2015. (Camille Ryan & Jamie M. Lewis, U.S. Census Bureau, Computer and Internet Use in the United States: 2015 (2017), http://tinyurl.com/yaahqtdu.)

In 1984, the FBI Magnetic Media Program (later Computer Analysis and Response Team) formed. (*Key Dates in Computer Forensics at NIST*, 1 NIST Forensic Sci. News, no. 2, Fall 2013, at 3, http://tinyurl.com/ybolg7rt.) Investigators ordinarily seize a computer and bring it to a laboratory for analysis, and computer technicians begin by creating a duplicate copy of everything on the computer. The technicians then use the copy to avoid damaging or altering the original. (Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 280 (2005).) Evidence can be captured on-screen or in print. When retrieving evidence from local storage, computer technicians use recovery software to extract the data and check the accuracy of the results. (Jay M. Zitter, Annotation, *Authentication of Electronically Stored Evidence, Including Text Messages and E-Mail*, 34 A.L.R.6th 253 (2008).)

Many modern-day crimes are committed using computers and the Internet, and computer forensics can be crucial in prosecuting these cybercrimes, as well as traditional criminal activities. (C.M. Whitcomb, *The Evolution of Digital Evidence in Forensic Science Laboratories*, Police Chief, Nov. 2007, at 41.) Stored computer files may provide evidence of a crime, such as financial or other business records. A defendant's Internet browsing history can also demonstrate, for example, how he or she prepared for or tried to conceal his or her actions.

The 2015 Boston Marathon bomber trial is a perfect example of how both prosecutors and defense attorneys use computer evidence to make their cases. In that case, the defense used evidence from the defendant's brother's computer to argue that the brother, rather than the defendant, masterminded the attacks. (Jon Kamp, *Jury Not Swayed by Defense Argument Brother Influenced Dzhokhar Tsarnaev*, Wall St. J., May 15, 2015, http://tinyurl.com/ydz2fsj8.) The prosecution also relied heavily on browsing history from the defendant's computer, which included al Qaeda literature and instructions on how to make a bomb. (Ann O'Neill, *The 13th Juror: The Radicalization of Dzhokhar Tsarnaev*, CNN (Mar. 30, 2015), http://tinyurl.com/yaq8wy8z.) The prosecution's computer evidence ultimately helped to secure the defendant's conviction.

CELL PHONES

In 1983, the first commercial cellular phone system began operation in Chicago. (*Wireless History Timeline*, Wireless Hist. Found., http://tinyurl.com/yc4jlyxe (last visited Nov. 26, 2017).) By 1990, cellular subscriptions surpassed five million; that number doubled within two years. (*Id.*) In the 2000s, the cell phone became increasingly data-centric, with more text and media messages, and then voice-over-Internet calls, and eventually the smartphone. As of January 2017, 95 percent of American adults owned a cell phone, and 77 percent owned a smartphone. (*Mobile Fact Sheet*, Pew Res. Ctr. (Jan. 12, 2017), http://tinyurl.com/hxzkjlo.)

Cell phone evidence can be obtained when police have physical custody of the phone or by requesting historical or real-time data from the phone company. Evidence found on a cell phone can include contacts, call history, text messages, deleted text messages, photos, calendar entries, notes, media storage, web browsing history, app metadata, and e-mail. Because of the enhanced sophistication of smartphones, the methods used to extract evidence and the evidence itself often resemble the evidence gleaned from PCs. (Cellebrite is one provider of cell phone forensic software.)

Call detail records (CDRs) are historical data obtained from a cell service provider and can include logs of incoming and outgoing calls, as well as the originating and terminating cell towers used to make each call. (Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, Matt Blaze's Exhaustive Search (Dec. 13, 2013), http://tinyurl.com/myl6x9p.) CDRs are often used to prove a pattern of communication by a defendant, victim, or witness. Location data from cell towers may be used to approximate a cell phone's historical location and thus the whereabouts of a person involved in the investigation. (*Id.*) These records may be offered to prove or disprove a defendant's alibi or presence at the scene.

With the proper authority, police also can work with mobile phone service providers to track a person's whereabouts in real time by using either cell tower signals (triangulation) or GPS (Global Positioning System), a feature of smartphones. (Alexandra Wells, *Ping!: The Admissibility of Cellular Records to Track Criminal Defendants*, 33 St. Louis U. Pub. L. Rev. 487, 489–95 (2014); Chandra Steele, *How Police Track Your Phone*, PC Mag. (May 16, 2012), http://tinyurl.com/y76fsptp.) Triangulation is possible when a phone transmits signals to two cell towers simultaneously. The two cell towers serve as two known points of a triangle, and the location of the cell phone is the unknown third point. In some instances, trigonometry involving the angles and distances between the towers and phone can reveal the cell phone's approximate location. (Wells, *supra*, at 492.) Using GPS, a service provider can "ping" a person's smartphone and provide real-time location information for the phone. (Blaze, *supra*.) Accuracy

and usefulness of this data depend on the geographical location and population density of the region where the phone is located, but law enforcement officials with whom we spoke said GPS is typically accurate within 50 to 100 feet.

Pen registers, which track data from outgoing phone communications, and "trap and trace" devices, which track data from incoming communications and other identifying information, are also common in narcotics and other investigations to show ongoing criminal activity. (*See* 18 U.S.C. §§ 3121–3127.) These methods record data from calls, text messages, and e-mails but do not record the content of the communications. (The Patriot Act expanded the use of trap and trace devices to include all "dialing, routing, addressing, and signaling information." *Id.* § 3127(4).) Under a pen register, law enforcement can also request that the service provider send location information, latitude, longitude, and degree of error (e.g., plus or minus 100 feet) for the cell phone at a set interval (e.g., every 10 minutes). Government attorneys must obtain a court order before using pen registers and trap and trace devices by showing that they are critical to an ongoing criminal investigation, but the government need not show probable cause or get a warrant. *Id.* §§ 3121–3123.) Between 2001 and 2011, trap and trace authorizations jumped from 5,683 cases to 37,616. (Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, Am. C.L. Union (Sept. 27, 2012), http://tinyurl.com/ycf9s8dz.)

Two Tennessee cases demonstrate the versatility of cell phone data as evidence. In the first, a defendant was convicted of murder in part because of a photograph of the murder weapon lying on his bed hours before the crime was committed. The photo and timestamp were found on his cell phone. In another case, police used a court-ordered trap and trace device to investigate a suspected narcotics ring and show a pattern of movement consistent with drug trafficking. Police later stopped one of the suspects, who was caught with large amounts of cash and drugs.

GPS DEVICES

Inspired by Sputnik, the first artificial Earth satellite launched by the Soviet Union in 1957, GPS technology was designed for US military and intelligence applications. Between 1974 and 1985, the military launched satellites that would serve as the first generation of GPS, completed in 1995. In 1983, GPS became available to civilian commercial aircraft to improve navigation and air safety, and in 1998, the government allowed GPS satellites to transmit signals specifically for civilian use. In 1989, mobile GPS devices were first marketed to consumers in the United States, followed by the first GPS phone a decade later. Starting in 2005, a new generation of GPS satellites began to transmit dedicated signals for commercial and civilian use. (Mark Sullivan, *A Brief History of GPS*, PCWorld (Aug. 9, 2012), http://tinyurl.com/yczy9kvc.)

With a warrant, police and prosecutors can plant GPS devices on a car or other vehicle to establish a suspect's location. Devices already equipped with GPS, such as cell phones and navigational systems, record and store historical location data that may later be retrieved by investigators. GPS devices can also supervise sex offenders, pretrial defendants, probationers, and parolees, and are sometimes used as alternatives to incarceration. For example, starting in 2003 in Washington, D.C., high-risk or noncompliant offenders and those with stay-away orders have been subject to GPS monitoring 24 hours a day. (Leonard A. Sipes Jr., *GPS Tracking of Criminal Offenders in Washington, D.C.*, DC Pub. Safety Blog (Apr. 12, 2012), http://tinyurl.com/ya76xygv.)

The use of GPS in criminal prosecutions drew national attention in the 2004 murder trial of Scott Peterson. At trial, the judge admitted data from a GPS device indicating that Peterson had been near the place where his wife's body was found. (Nathan J. Buchok, *Plotting a Course for GPS Evidence*, 28 Quinnipiac L. Rev. 1019 (2010).) In another high-profile case, a man was arrested for abducting a woman off of a Philadelphia street after police obtained data from a GPS device that the car dealership, concerned about poor credit, had placed in his car at the time of purchase. (Abby Ohlheiser, *The Controversial GPS Device That Helped Police Catch Carlesha Freeland-Gaither's Alleged Abductor*, Wash. Post, Nov. 7, 2014, http://tinyurl.com/y9fkotkz.)

SOCIAL MEDIA

During the 1980s and 1990s, website bulletin board systems, AOL community and member profiles, and sites like GeoCities were precursors to modern social media. On the heels of early sites like Classmates.com and SixDegrees.com, Friendster launched in 2002 and grew to three million users within a year. A year later, both LinkedIn and Myspace emerged; in another year Facebook surfaced, initially only for college students. Other modern social media followed: Flickr for pictures, YouTube for video, Tumblr for blogging, and Twitter for microblogging. Smartphones have revolutionized social media, with "old" services, like Facebook, adapting to the mobile platform, and new services, like photo and video messaging apps Snapchat and Instagram, entering the market. (*The History of Social Networking*, Digital Trends (May 14, 2016), http://tinyurl.com/y7pshjjs.)

Police and prosecutors increasingly use social media not only to investigate crimes, but also to prevent crimes before they occur. Many social media profiles are open to the public, exposing them to law enforcement and attorneys alike. Even when the profiles are private, the police may enlist cooperating witnesses who are "friends" or "connections" of a suspect to help them gain access to information on the suspect's profile. Police and prosecutors may also subpoena social media records from the website or app. (Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 Rich. J.L. & Tech. 11 (2013).)

Criminals sometimes brag about their crimes on social media, and sexual predators have been located and arrested based on their online activities, such as sharing photos and videos of sexual acts involving children. (Wayne Hanson, *How Social Media Is Changing Law Enforcement*, Gov't Tech. (Dec. 2, 2011), http://tinyurl.com/oqmdodg.) Social media are used at trial by both the prosecution and the defense to discredit witnesses, track down additional evidence, or establish associations between people. (*Id.*) Some attorneys also use social media profiles to investigate potential jurors during voir dire, thereby affecting the composition of juries. (Meghan Dunn, Jurors' and Attorneys' Use of Social Media during Voir Dire, Trials, and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management (2014), http://tinyurl.com/y9pkk5uq; Murphy & Fontecilla, *supra*, at 25–29.)

The Trayvon Martin case, in which a neighborhood watch volunteer killed a Florida teen, illustrates how social media can aid or complicate a prosecutor's job. Defense counsel created Facebook and Twitter profiles for George Zimmerman's defense to boost public

perception of their client, and the attorneys scanned Facebook profiles to exclude potentially problematic jurors. Both Martin's Facebook profile and a witness's Twitter account were admitted as evidence during the trial. (Lizette Alvarez, *Social Media, Growing in Legal Circles, Find a Role in Florida Murder Case*, N.Y. Times, Nov. 6, 2012, http://tinyurl.com/y8cjqnjs.) Zimmerman was ultimately acquitted of second-degree murder. (Lizette Alvarez & Cara Buckley, *Zimmerman Is Acquitted in Trayvon Martin Killing*, N.Y. Times, July 13, 2013, http://tinyurl.com/jq7ndte.)

POLICE BODY CAMERAS

Police departments began experimenting with police body-worn cameras as early as 2005 in the United Kingdom and 2010 in the United States. Prompted by the events in Ferguson, Missouri, and Staten Island, New York, President Obama proposed federal funding for body cameras in late 2014. (Press Release, White House, Fact Sheet: Strengthening Community Policing (Dec. 1, 2014), http://tinyurl.com/yc53hy7q.) The number of jurisdictions using body-worn cameras is continuing to grow, as departments of all sizes consider adopting them.

Body camera evidence is obtained from portable cameras typically worn on the chest or glasses. Data are retrieved from the camera and stored either by a third party or by the department itself. Video designated as "evidentiary" may be retained for longer periods, while "nonevidentiary" evidence is deleted after a shorter period of time. Department procedures vary in terms of when officers must turn on the cameras, as well as how and for how long they must store the footage. (*See, e.g.*, Antonia Merzon, Colo. Best Practices Comm. for Prosecutors, Body-Worn Cameras: A Report for Law Enforcement (2015), http://tinyurl.com/yaomkxvs.)

In Oakland, California, police-worn body cameras captured a robbery suspect pointing a gun at a police officer before police shot and killed him. The police department used the footage, which showed the suspect's actions from the officers' perspectives, to demonstrate that they justifiably responded with deadly force. (Henry K. Lee, *Police Body Cameras and Store Security Caught Fatal Oakland Cop Shooting*, SFGate (Aug. 13, 2015), http://tinyurl.com/yb26hqtc.) In a contrasting case in Cincinnati, Ohio, a police officer shot a man during a routine traffic stop. The officer told investigators that he feared for his life, but footage from the officer's body camera contradicted that narrative. The officer was fired from his job and indicted on murder charges. (Dana Ford, *University Cop Indicted for Murder in Shooting of Motorist Samuel DuBose*, CNN (July 30, 2015), http://tinyurl.com/pcg93t3.)

EMERGING TECHNOLOGY

Although law enforcement officers now commonly use the technologies discussed above, many would have been unimaginable just a decade or two ago. Below are four examples of emerging technologies that are likely to increasingly impact criminal prosecutions in the future.

NEXT-GENERATION DNA SEQUENCING

The technology now referred to as next-generation DNA sequencing (NGS) first emerged in 2005. (Yaran Yang et al., *Application of Next-Generation Sequencing Technology in Forensic Science*, 12 Genomics Proteomics & Bioinformatics 190 (2014).) Over the next several years, multiple companies developed competing NGS systems, which allow for much cheaper, faster, and more detailed sequencing of a high volume of "reads" or nucleotide sequences. (*Id.*; Sandra Porter, *Basics: How Do You Sequence a Genome? Part III, Reads and Chromats*, Scienceblogs.com (Jan. 28, 2007), http://tinyurl.com/yamjrgw9.) The scientific community has embraced NGS for medical and other scientific research, but forensic scientists continue to use the Sanger method, which is more expensive and far less efficient. (Yang et al., *supra*.) A move by the forensics community to implement NGS would have large initial costs but could solve many of the current challenges in crime scene investigations, such as partial or mixed DNA samples. In a case where a DNA sample does not produce a match from the offender database, NGS analysis could tell law enforcement important physical or geographical information to track down a suspect. (*Id.*)

DRONES

Unmanned aerial vehicles, commonly known as drones, have been used extensively in military operations abroad. In 2012, the Department of Homeland Security launched a program to accelerate adoption of drone technology by local police departments. (Kimberly Dvorak, *Homeland Security Increasingly Lending Drones to Local Police*, Wash. Times, Dec. 10, 2012, http://tinyurl.com/y8uav9b4.) In 2016, the Federal Aviation Administration (FAA) released the first operational rules for routine commercial use of small unmanned aircraft systems, including aiding in certain rescue operations. (Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,064 (June 28, 2016).)

The federal government has adopted a drone program for domestic surveillance (Gregg Zoroya, *Pentagon Report Justifies Deployment of Military Spy Drones over the U.S.*, USA Today (Mar. 9, 2016), http://tinyurl.com/y7ss6qrd), and local police departments currently use drones for search and rescue missions or for photographing and investigating crime scenes (Dvorak, *supra*). But there are Fourth Amendment concerns about using drones for unwarranted surveillance. Eighteen states have passed legislation requiring police to obtain a warrant before using drones for surveillance. (*2016 Unmanned Aircraft Systems (UAS) State Legislation Update*, Nat'l Conf. of St. Legislatures (Mar. 20, 2017), http://tinyurl.com/y8uko26d.)

The first arrest based on drone evidence occurred in North Dakota in 2011, when police borrowed a drone from the Department of Homeland Security. In this case, a herd of cows wandered onto a cattle rancher's property, and when the rancher refused to return them to his neighbor, the police called for SWAT team assistance. There was a 16-hour police standoff, which was resolved when the SWAT team flew a drone over the property to identify the man's location and ascertain when it was safe to approach him for arrest. (*See* Jason Koebler, *First Man Arrested with Drone Evidence Vows to Fight Case*, U.S. News & World Rep. (Apr. 19, 2012), http://tinyurl.com/y9qvdos4.)

FACIAL RECOGNITION

Facial recognition, which identifies people by comparing an image from a photograph or video frame to a database of facial coordinates, was first studied in the 1960s and developed through the 1970s and 1980s, but it initially required an administrator's manual input. In 1988, a scientific breakthrough revealed that accurate facial analysis required identification of less than 100 points of a human's face,

and in 1991, facial recognition reached full automation in real time. (*Face Recognition*, FBI, http://tinyurl.com/ycwyb4jo (last visited Nov. 26, 2017).)

Achieving full operational capability in 2014, the FBI's Next Generation Identification (NGI) program offers state-of-the-art biometric identification services to be shared with participating state agencies. Although the NGI database contains nearly 30 million photos, the FBI also has access to selected states' driver's license photos, the State Department's visa and passport database, and the biometric database maintained by the Defense Department—for a total of over 411 million images. (U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy 47–48 (2016).) The FBI program reports 85 percent accuracy when using images with people facing forward "no more than 15 degrees off the center axis." (*Id.* at 25–26; Russell Brandom, *Why Facebook Is Beating the FBI at Facial Recognition*, Verge (July 7, 2014), http://tinyurl.com/y77ctzge.) With access to front-facing images uploaded by users, the private industry's technology is even better: Facebook's recognition technology (which detects a user's appearance in a photograph to suggest "tagging" them) has 97.25 percent accuracy; Google's is 99.63 percent. (Ben Sobel, *Facial Recognition Technology Is Everywhere. It May Not Be Legal*, Wash. Post, June 11, 2015, http://tinyurl.com/o6gxyx2.)

Several states, including New York, New Jersey, Nebraska, and Iowa, are using images from department of motor vehicles (DMV) databases to crack down on identity theft and fraud. (Jenni Bergal, *States Crack Down on Driver's License Fraud*, Stateline (July 14, 2015), http://tinyurl.com/ycf9lpxl; David Kravets, *Drivers' License Facial Recognition Tech Leads to 4,000 New York Arrests*, Ars Technica (Aug. 22, 2017), http://tinyurl.com/y9pucef6.) In some instances, DMV images are shared with law enforcement agencies to help track down "wanted felons or criminals, such as sex offenders, who are trying to hide their identity by using an alias." (Bergal, *supra*.)

GUNSHOT DETECTION

Seismologists developed gunshot detection technology in the early 1990s, and introduced it to police departments soon after. (John C. Lahr et al., *Earthquake Technology Fights Crime*, U.S. Geological Surv. (1996), http://tinyurl.com/y97ysq3t.) The technology utilizes a network of microphones to detect a gun's unique explosive sound, and then triangulates the source of the sound using GPS. These microphones can then be integrated with video surveillance so that when a gunshot is detected, a camera turns to the source. Washington, D.C., Boston, New York, and Chicago, among other cities, have used gunshot detection technology to identify and locate gunfire as it happens. (*See ShotSpotter Fact Sheet*, ShotSpotter (June 2017), http://tinyurl.com/yc2emvtp.) In D.C., the city's network of 300 microphones documented 39,000 shooting incidents in eight years. (Andras Petho et al., *ShotSpotter Detection System Documents 39,000 Shooting Incidents in the District*, Wash. Post, Nov. 2, 2013, http://tinyurl.com/hteguvc.) The information can help prosecutors establish the number or sequence of shots, the time of the shots, and whether multiple guns were fired. The microphones can also record sounds, like speech, that occur immediately after a gunshot is detected. These voice recordings have been introduced as evidence at trial. (Daniel Rivero, *Is NYC's New Gunshot Detection System Recording Private Conversations?*, Splinter (Mar. 20, 2015), http://tinyurl.com/yd298qwd.)

THE CLOUD AND "GOING DARK"

Despite the growing quantity of digital evidence available to improve the accuracy of prosecutors' and law enforcement's investigations, two technological developments have the potential to significantly limit access to digital data.

The first development involves the growing use of cloud storage for PC and cell phone data. Rather than storing data on an individual device or local server, people and businesses increasingly use cloud computing, a system in which digital files are stored in "remote, virtualized environments, often hosted and managed by third parties." (George Grispos et al., *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*, 4 Int'l J. Digital Crime & Forensics 28, 28-48 (2012), http://tinyurl.com/y9ktcnxa.)

The cloud model poses two major challenges for digital forensics. The first is that "little, if any, data pertaining to a computer user is found in a single geographic location." (John M. Cauthen, *Executing Search Warrants in the Cloud*, FBI L. Enforcement Bull. (Oct. 7, 2014), http://tinyurl.com/y9rd7wpm.) This can create a problem when executing a search warrant, particularly if the data is stored in a foreign country. (*Id.*; *see also In re* Matter to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 855 F.3d 53 (2d Cir. 2017), *cert. granted*, No. 17-2 (U.S. Oct. 16, 2017).)

The second concern is that, even when investigators are able to recover data from the cloud, they may be unable to covert the data into a "format understandable to a human reader." (Cauthen, *supra*.) Data may be encrypted pursuant to a service-level agreement with the customer, and the service provider may be limited in its ability to search or recover the data. (*Id.*) The second concern arises from decisions by Apple and Google to encrypt information on the iPhone and Android operating systems by default—a phenomenon known as "going dark." With encryption, the companies themselves cannot retrieve data without a user's passcode and, therefore, are unable to cooperate with criminal investigations even after a search warrant is issued. (James B. Comey, Dir., FBI, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, Address before the Brookings Institution (Oct. 16, 2014), http://tinyurl.com/orr6exf.) Cell phone apps such as Snapchat, a messaging app in which photos and text messages disappear after mere seconds, also demonstrate the trend toward making user data inaccessible.

Going dark may create the greatest roadblock for prosecutors, as a Louisiana murder case illustrates. In April 2015, Brittney Mills, a 29-year-old pregnant woman, was fatally shot when an unknown individual came to her front door. Although doctors delivered her baby, he died a week later. The police suspect that the perpetrator was someone she knew. Investigators found the victim's iPhone, but were unable to access the information on it without her four-digit passcode. Citing protections for customers' privacy, Apple would not provide access to the phone's data without Mills's password. A private company hired by the district attorney was able to access the encrypted data, but the case remains unsolved. (Grace Toohey, *Two Years Later, Brittney Mills Murder Case Still Unsolved after DA Hired Private Company to Crack iPhone*, Advocate (May 8, 2017), http://tinyurl.com/yaj6rgru.)

LOOKING FORWARD

Used effectively and lawfully, existing and emerging evidence can benefit even the smallest of jurisdictions. In 2012, prosecutors in a Missouri town of 35,000 people convicted two defendants of second-degree murder without a body, cause of death, murder weapon, eyewitness, or defendant statement. The case involved a missing person who was last seen with one of the defendants. A search warrant for one defendant's house revealed blood spatter evidence. Cell phone records were also used to track the movements of the defendants in the days after the disappearance, leading police to a small pond in a remote area. Cadaver dogs signaled the pond, which was drained and revealed a charred human liver. DNA from the liver matched the blood spatters in the defendant's house. Surveillance footage and credit card receipts also showed the defendants purchasing cleaning supplies and other relevant items. Prosecutors in the 10-person Missouri office used DNA, cell tower records, cell phone forensics, and surveillance videos to convict two defendants in a case that could have remained unsolved forever. (*See* Kathee Baird, *Final Suspect in Carl Anderson's Murder Sentenced to 23 Years*, Crime Scene (Nov. 23, 2014), http://tinyurl.com/ychogpw9.)

These sample cases demonstrate how much a prosecutor's job has changed in a relatively brief period of time. Just two or three decades ago, prosecutors were significantly more limited in their ability to procure the evidence that links a perpetrator to his crime. Many of the tragic instances of wrongful conviction took place prior to the arrival of sophisticated DNA and digital evidence. With better evidence at their disposal, prosecutors today can avoid some of the mistakes of the past and be more confident when proceeding with charges against a defendant. Surveillance footage and GPS surveillance could also help law enforcement to keep communities safer by preventing criminal activity.

In addition to these opportunities, the massive growth of DNA and digital technology presents many new challenges for prosecutors. First, those who are unfamiliar with new technologies may view them with fear or skepticism. As more and more digital data become available, it is important to remember that all evidence, whether it has existed for decades or only a few years, is subject to the same procedures and safeguards before it may be introduced in court. Using all traditional legal standards, police and investigators must find, preserve, and authenticate new forms of evidence before using them to make their case.

Furthermore, district attorneys' offices must find the manpower, technical knowledge, and funds to keep pace with changing technologies. Prosecutors are now confronted with a deluge of digital evidence and must make strategic decisions about how to efficiently and effectively sort through the files, often in the face of budget cuts and diminishing labor pools. (In addition to digital evidence discussed above, prosecutors now routinely monitor jailhouse phone calls for admissions by defendants. *See* Susan Candiotti & Sally Garner, *Recorded Calls Keep Inmates Locked Up*, CNN (Mar. 26, 2011), http://tinyurl.com/yaufw745.) Despite the demonstrated effectiveness of new technologies like police body cameras, not all jurisdictions have the resources to keep up with their acquisition and use. Prosecutors, who support the use of the cameras, are struggling with finding the personnel to review the recordings and the funds to store them. As more police departments are buying cameras, these concerns are only increasing.

Despite limited resources, prosecutors still must find ways to stay informed about changes in technology and the growing body of evidence available to them. There are many ways to accomplish these goals and overcome the challenges. Increased funding for personnel and training for prosecutors can go a long way toward ensuring that prosecutors can access and use the new evidence appropriately. Collaborations, such as the statewide best practices committees of prosecutors that have formed around the country, provide forums for prosecutors to share strategies and information about upcoming technologies and issues to promote the best ways to use the evidence. As of November 2017, 20 states have formed statewide best practices committees for prosecutors, and others are considering forming committees. (*Best Practices Committees*, Prosecutors' Ctr. for Excellence, http://pceinc.org/committees/ (last visited Nov. 26, 2017).)

Interagency communication among police departments, forensic laboratories, and prosecutors through regular meetings and discussions is also fundamental to help ensure that evidence is properly collected and handled.

The criminal justice system is undergoing a period of reflection and improvement. The availability of the new evidence described in this article is an important aspect of that improvement. If prosecutors, police, and forensic laboratories have the necessary resources to recover, test, and use the new evidence, they can use it effectively in criminal cases to inculpate the guilty and exculpate the innocent. Prosecutors must take the lead, embrace the new technology, and push for more. The new evidence will allow prosecutors to be secure in the validity of their convictions and will promote justice for the victim of the crime, the accused, and the community at large. ■

ADDITIONAL REFERENCES

DNA

Dennis Harris, *New DNA Advances*, Evidence Tech. Mag. (Jan. 2013), http://tinyurl.com/y9la6v9h.

COMPUTERS

Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 Bos. B.J. 10 (2003).

CELL PHONES

Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 Rich. J.L. & Tech. 3 (2011).

Martin A. Dolan et al., *Improving Your Criminal Practice: Use of Cell Phone Records and GPS Tracking*, 24 CBA Rec. 38 (2010).

Douglas Starr, *What Your Cell Phone Can't Tell the Police*, New Yorker (June 26, 2014), http://tinyurl.com/ycqa6xsl.

POLICE-WORN BODY CAMERAS

David A. Harris, *Picture This: Body Worn Video Devices ("Head Cams") as Tools for Ensuring Fourth Amendment Compliance by Police* (Univ. of Pittsburgh Sch. of Law, Working Paper No. 2010-13, Apr. 2010), http://tinyurl.com/ycoahzyl.

Considering Police Body Cameras, 128 Harv. L. Rev. 1794 (2015).