

SECURE IN OUR CONVICTIONS

USING NEW EVIDENCE TO STRENGTHEN PROSECUTION



January 2016

Copyright © 2016 Prosecutors' Center for Excellence. All rights reserved.

SECURE IN OUR CONVICTIONS: Using New Evidence to Strengthen Prosecution

By Kristine Hamann and Rebecca Rader Brown*

ABSTRACT

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.

The following is an overview of the forms of evidence increasingly used by prosecutors over the past several decades, including DNA, surveillance cameras, computers, cell phones, GPS, social media, and police body cameras. Each section provides a brief history of the technology, as well as a summary of the technology's current capabilities. The article also addresses emerging technologies that are likely to have an increasing impact on criminal investigations, including Next Generation DNA Sequencing, drones, facial recognition, and gunshot detection. Finally, the authors address challenges related to the increased use of cloud storage and the phenomenon of "going dark", which is limiting law enforcement access to smart phone and other digital evidence.

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 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.

INTRODUCTION

In May of 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 twelve-day trial and one day of deliberations, jurors convicted the roommate of first-degree murder and sentenced him to life in prison.¹

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 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.²

*Kristine Hamann is the Executive Director of Prosecutors' Center for Excellence. Rebecca Rader Brown is a Consulting Attorney with Prosecutors' Center for Excellence; her work is supported by Grant No. 2013-DB-BX-K005 awarded by the Bureau of Justice Assistance to the New York Prosecutors Training Institute (NYPTI). The authors would like to thank Georgetown law students Laura Donnelly, Daniel Kroepsch, and Elizabeth Paukstis for their assistance in researching and editing this article. Thanks also to Assistant District Attorneys Lois Raff and Robert Masters of the Queens District Attorneys Office in New York City for their insights and comments.

¹ For more information on the Colorado case, see: Ryan Hicks, CBS DENVER, <http://denver.cbslocal.com/tag/ryan-hicks/> (last visited Sept. 20, 2015).

² The authors are grateful to the many prosecutors who responded to requests for sample cases in the course of researching this paper. 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.³ In the 1960s and 1970s, the field of molecular genetics emerged as scientists learned to “read” DNA. Forensic DNA testing began in 1985.⁴ 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.⁵ In the years that followed, DNA emerged as “the most reliable physical evidence at a crime scene, particularly those involving sexual assaults.”⁶

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.”⁷ Additionally, twenty-three states require all convicted felons to provide DNA samples.⁸ 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).⁹ 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.

³ The History Channel, *This Day in History: Feb. 28, 1953 – Watson and Crick discover chemical structure of DNA*, THE HISTORY CHANNEL, <http://www.history.com/this-day-in-history/watson-and-crick-discover-chemical-structure-of-dna>.

⁴ Randy James, *A Brief History of DNA Testing*, TIME (June 19, 2009), <http://content.time.com/time/nation/article/0,8599,1905706,00.html>.

⁵ For more information on the *Andrews* case, see: Associated Press, *Rapist Convicted on DNA Match*, THE NEW YORK TIMES (Feb. 6, 1988), <http://www.nytimes.com/1988/02/06/us/rapist-convicted-on-dna-match.html>.

⁶ James, *supra* note 4.

⁷ Fact Sheet: Legislation to Advance Justice Through DNA Technology, The United States Department of Justice (Sept. 9, 2014), <http://www.justice.gov/ag/fact-sheet-legislation-advance-justice-through-dna-technology>.

⁸ *Id.*

⁹ Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System, Federal Bureau of Investigation, <https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet> (last visited Oct. 23, 2015).

As of May 2015, NDIS contains nearly twelve million offender profiles and more than 600,000 forensic crime scene profiles.¹⁰

DNA evidence must be collected, handled, and stored using sterile, environmentally controlled methods. Using cell samples (e.g., hair follicles or blood cells), technicians isolate, identify, and compare certain characteristics of an individual's genetic structure.¹¹ Testing is verified using "principles of statistics and population genetics to give statistical significance to the DNA match, by indicating the statistical frequency with which such matches might occur in the population."¹²

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.¹³ 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.¹⁴ Rapid testing is under development to enable creation of a profile compatible with DNA databases in one to two hours.¹⁵

A recent 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 and, without DNA evidence, the murder almost certainly would have remained unsolved.

¹⁰ The FBI website includes many useful factsheets pertaining to DNA databases and analysis. *See* Combined DNA Index System (CODIS), Federal Bureau of Investigation, <https://www.fbi.gov/about-us/lab/biometric-analysis/codis> (last visited Sept. 20, 2015).

¹¹ Jennifer M. Romeika and Fei Yan, *Recent Advances in Forensic DNA Analysis*, FORENSIC RESEARCH (2013), <http://www.omicsonline.org/recent-advances-in-forensic-dna-analysis-2157-7145.S12-001.pdf>.

¹² *Arnold v. State*, 807 So. 2d 136, 140 (Fla. 4th Dist. Ct. App. 2002) (reversed and remanded as failure to give defendant an opportunity to present conflicting evidence at Frye hearing before admission of evidence violated Due Process rights).

¹³ Romeika, *supra* note 11.

¹⁴ *Id.*

¹⁵ Rapid DNA or Rapid DNA Analysis, The Federal Bureau of Investigation, <https://www.fbi.gov/about-us/lab/biometric-analysis/codis/rapid-dna-analysis> (last visited Oct. 23, 2015).

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 2015 Michigan case demonstrates how effective DNA databases can be at solving cold cases. A man was convicted 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.¹⁶

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 1971.¹⁷ Improvements in the technology in the eighties and nineties 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.¹⁸ Cameras are now commonplace in less populous cities, as well as in suburban and rural communities throughout

¹⁶ Agar, J., *DNA links suspect to cold-case rape, victim 'relieved' by arrest, police say*, MLIVE.COM (Sept. 8, 2015, 1:48 PM), http://www.mlive.com/news/grand-rapids/index.ssf/2015/09/dna_links_suspect_to_cold-case.html.

¹⁷ 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), <http://stetson.edu/law/lawreview/media/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-ba.pdf>.

¹⁸ William M. Bulkeley, *Chicago's Camera Network Is Everywhere*, THE WALL STREET JOURNAL (Nov. 17, 2009, 12:01 AM), <http://www.wsj.com/articles/SB10001424052748704538404574539910412824756>.

the United States.¹⁹ 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 that 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.²⁰ In a recent 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.²¹

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

Computers

Personal computers 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 8.2 percent in 1984 to 83.8 percent in 2013.²²

In 1984, the FBI Magnetic Media Program (later Computer Analysis and Response Team) formed.²³ 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

¹⁹ One Assistant District Attorney with whom we spoke explained that “[t]he proliferation of these devices has altered the old-fashion, 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.”

²⁰ The *New York Times* published the following account of how surveillance images were introduced at trial: Jo Thomas, *Jurors See Chilling Images of Truck Before Bombing*, THE NEW YORK TIMES (May 15, 1997), <http://www.nytimes.com/1997/05/15/us/jurors-see-chilling-images-of-truck-before-bombing.html>.

²¹ For more on the Kenneth Peters trial: See Cortney Ofstad, *Peters murder trial continues*, YOUR DAILY GLOBE (Apr. 24, 2013), <http://www.yourdailyglobe.com/story/2013/04/24/news/peters-murder-trial-continues/387.html>.

²² The United States Census records data on household computer and Internet use. See Computer and Internet Use: Latest Releases, United States Census Bureau, <http://www.census.gov/hhes/computer/> (last visited Sept. 20, 2015).

²³ NIST Forensic Science News, National Institute of Standards and Technology, NIST Forensic Sciences News: Vol. 1, Issue 2 (Fall 2013), <http://www.nist.gov/forensics/upload/NFSN-Fall-2013-final.pdf>.

computer. The technicians then use the copy to avoid damaging or altering the original.²⁴ Evidence can be captured onscreen 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.

Searching a hard drive is one of the most difficult tasks for a computer forensics team – it is where science and art intersect. An industry has arisen to support this analysis, and a host of proprietary and free software is now available to scan, analyze, and search computer drives.²⁵ These tools also enable investigators to search deleted, temporary, and back-up files, all of which can remain on a hard drive unbeknownst to the user.²⁶

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.²⁷ 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 prepared for or tried to conceal his 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.²⁸ The prosecution also relied heavily upon browsing history from the defendant's computer, which included al Qaeda literature and instructions on how to make a bomb.²⁹ The prosecution's computer evidence ultimately helped to secure the defendant's conviction.

²⁴ Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 280 (2005).

²⁵ The Belkasoft Evidence Center bills itself as compatible with law enforcement needs, including complying with industry standards of reliability and allowing for presentation of the software's reports in court. See BELKASOFT, <https://belkasoft.com/en/> (last visited Sept. 20, 2015). Another example is Guidance Software's EnCase Forensic, which has a portable version allowing for collection and review of evidence from computers found in the field. See Overview, EnCase Forensic v7, Guidance Software, <https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx> (last visited Sept. 20, 2015).

²⁶ Jay M. Zitter, *Authentication of Electronically Stored Evidence, Including Text Messages and E-mail*, 34 A.L.R.6TH 253.

²⁷ C.M. Whitcomb, *The Evolution of Digital Evidence in Forensic Science Laboratories*, THE POLICE CHIEF (Nov. 2007), http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1321.

²⁸ Jon Kamp, *Jury Not Swayed by Defense Argument Brother Influenced Dzhokhar Tsarnaev*, THE WALL STREET JOURNAL (May 15, 2015, 8:04 PM), <http://www.wsj.com/articles/jury-not-swayed-by-defense-argument-brother-influenced-dzhokhar-tsarnaev-1431734675>.

²⁹ Ann O'Neill, *The 13th Juror: The radicalization of Dzhokhar Tsarnaev*, CNN (Mar. 30, 2015, 4:17 PM), <http://www.cnn.com/2015/03/27/us/tsarnaev-13th-juror-jahar-radicalization/>.

Cell Phones

In 1983, the first commercial cellular phone system began operation in Chicago.³⁰ By 1990, cellular subscriptions surpassed five million; that number doubled within two years.³¹ 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 smart phone. As of 2014, 90 percent of American adults owned a cell phone, and 64 percent owned a smart phone.³²

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 smart phones, the methods used to extract evidence and the evidence itself often resemble the evidence gleaned from personal computers.³³

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.³⁴ 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, helping to prove or disprove the whereabouts of a person involved in the investigation.³⁵ 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 either by using cell tower signals ("triangulation") or GPS (Global Positioning System), a feature of smart phones.³⁶ Triangulation is possible when a phone transmits signals to two cell towers simultaneously. The two cell towers serve as two

³⁰ Wireless History Foundation, Wireless History Timeline, <http://www.wirelesshistoryfoundation.org/wireless-history-project/wireless-history-timeline> (last visited Oct. 23, 2015).

³¹ *Id.*

³² See Mobile Technology Fact Sheet, Pew Research Center (Oct. 2014), <http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/>.

³³ Cellebrite is one provider of cell phone forensic software. See CELLEBRITE, <http://www.cellebrite.com/Mobile-Forensics> (last visited Sept. 20, 2015).

³⁴ Matt Blaze, *How Law Enforcement Tracks Cellular Phones*, MATT BLAZE'S EXHAUSTIVE SEARCH: SCIENCE, SECURITY, CURIOSITY (Dec. 13, 2013), <http://www.crypto.com/blog/celltapping/>.

³⁵ *Id.*

³⁶ Alexandra Wells, *Ping!: The Admissibility of Cellular Records to Track Criminal Defendants*, 33 ST. LOUIS U. PUB. L. REV. 487, 489-95, http://www.slu.edu/Documents/law/PLR/Archives/XXXIII-2-14/Wells_Article_0.pdf; Chandra Steele, *How Police Track Your Phone*, PC MAGAZINE (May 16, 2012), <http://www.pcmag.com/article2/0,2817,2404494,00.asp>.

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 towers and phone can reveal the cell phone's approximate location.³⁷ Using GPS, a service provider can "ping" a person's smart phone and provide real-time location information for the phone.³⁸ Accuracy and usefulness of this data depend upon 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.³⁹ These methods record data from calls, text messages, and e-mail but do not record the content of the communications.⁴⁰ 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 ten minutes).⁴¹ Between 2001 and 2011, trap and trace authorizations jumped from 5,683 cases to 37,616.⁴²

Two recent 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.

³⁷ Wells, *supra* note 36.

³⁸ Blaze, *supra* note 34.

³⁹ For statutory language regarding pen registers and trap and trace devices, see 18 U.S.C. §§ 3121-3127 (2015).

⁴⁰ The Patriot Act expanded the use of trap-and-trace devices to include "all "dialing, routing, addressing, or signaling information." See 18 U.S.C.S. § 3127 (2015); see also Amy Baggio, *21st Century Investigations and Motions Practice* (June 2011), <http://www.fd.org/docs/select-topics/search-and-seizure/generally/21st-century-investigations-and-motions-practice.pdf?sfvrsn=6>.

⁴¹ 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. See 18 U.S.C.A. §§ 3121-3123 (2001).

⁴² Documents released by the Department of Justice in 2012 showed the increase; See Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, THE AMERICAN CIVIL LIBERTIES UNION (Sept. 27, 2012, 1:32 PM), <https://www.aclu.org/blog/new-justice-department-documents-show-huge-increase-warrantless-electronic-surveillance>.

GPS Devices

Inspired by Sputnik, the first artificial Earth satellite launched by the Soviet Union in 1957, GPS technology was designed for U.S. 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.⁴³

Law enforcement can obtain information from GPS tracking devices placed on vehicles or items, or can obtain the information from devices already GPS-enabled, such as cell phones. Two kinds of tracking devices include data-loggers, which store locations on the device's internal memory to be retrieved later, and data-pushers, which transmit location data in real time.⁴⁴ Prosecutors can also subpoena GPS data from third parties, such as GPS service providers or telephone companies, as discussed above.

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 non-compliant offenders and those with stay away orders have been subject to GPS monitoring twenty-four hours a day.⁴⁵

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.⁴⁶ In another high-profile case, a man

⁴³ Mark Sullivan, *A brief history of GPS*, TECHHIVE (Aug. 9, 2012), <http://www.techhive.com/article/2000276/a-brief-history-of-gps.html>.

⁴⁴ Nathan J. Buchok, *Plotting a Course for GPS Evidence*, 28 QUINNIPIAC L. REV. 1019 (2010), [http://www.quinnipiac.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/37_28QLR1019\(2009-2010\).pdf](http://www.quinnipiac.edu/prebuilt/pdf/SchoolLaw/LawReviewLibrary/37_28QLR1019(2009-2010).pdf).

⁴⁵ Court Services and Offender Supervision Agency, *GPS Tracking of Criminal Offenders in Washington, D.C.*, DC PUBLIC SAFETY BLOG (Apr. 12, 2012), <http://media.csosa.gov/blog/2012/04/gps-tracking-of-criminal-offenders-in-washington-d-c/>.

⁴⁶ Buchok, *supra* note 44.

was arrested for abducting a woman off of a Philadelphia street after police obtained data from a GPS device showing that the car dealership, concerned about poor credit, had placed in his car at the time of purchase.⁴⁷

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 Six Degrees, Friendster launched in 2002 and grew to three million users within three months. 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. Smart phones 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.⁴⁸

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.⁴⁹

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.⁵⁰ Social media are used at trial by both the prosecution and the defense to discredit witnesses, track down additional evidence, or establish associations between

⁴⁷ Abby Ohlheiser, *The controversial GPS device that helped police catch Carlesha Freeland-Gaither’s alleged abductor*, THE WASHINGTON POST (Nov. 7, 2014), <https://www.washingtonpost.com/news/post-nation/wp/2014/11/06/the-controversial-gps-device-that-helped-officials-catch-an-alleged-philadelphia-abductor/>.

⁴⁸ Digital Trends, *The History of Social Networking*, DIGITAL TRENDS (Aug. 5, 2014), <http://www.digitaltrends.com/features/the-history-of-social-networking/>.

⁴⁹ Justin P. Murphy and Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 11 (2013).

⁵⁰ Wayne Hanson, *How Social Media Is Changing Law Enforcement*, GOVERNMENT TECHNOLOGY (Dec. 2, 2011), <http://www.govtech.com/public-safety/How-Social-Media-Is-Changing-Law-Enforcement.html>.

people.⁵¹ Some attorneys also use social media profiles to investigate potential jurors during *voir dire*, thereby affecting the composition of juries.⁵²

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.⁵³ Zimmerman was ultimately acquitted of second-degree murder.⁵⁴

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 2014.⁵⁵ In May of 2015, the Justice Department announced plans to spend \$20 million on a pilot program implementing body cameras nationwide.⁵⁶ Sixty-six of the 100 most populous cities now require or plan to adopt body cameras for their police departments.⁵⁷ The number of jurisdictions using body worn cameras will surely continue 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

⁵¹ *Id.*

⁵² Murphy & Fontecilla, *supra* note 50, at 25-9; 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* (May 1, 2014), [http://www.fjc.gov/public/pdf.nsf/lookup/jurors-attorneys-social-media-trial-dunn-fjc-2014.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/jurors-attorneys-social-media-trial-dunn-fjc-2014.pdf/$file/jurors-attorneys-social-media-trial-dunn-fjc-2014.pdf).

⁵³ Lizette Alvarez, *Social Media, Growing in Legal Circles, Find a Role in Florida Murder Case*, THE NEW YORK TIMES (Nov. 6, 2012), http://www.nytimes.com/2012/11/07/us/social-media-finds-a-role-in-case-against-zimmerman.html?_r=1.

⁵⁴ Lizette Alvarez and Cara Buckley, *Zimmerman Is Acquitted in Trayvon Martin Killing*, THE NEW YORK TIMES (July 13, 2013), <http://www.nytimes.com/2013/07/14/us/george-zimmerman-verdict-trayvon-martin.html>.

⁵⁵ Press Release, The White House, Fact Sheet: Strengthening Community Policing (Dec. 1, 2014), <https://www.whitehouse.gov/the-press-office/2014/12/01/fact-sheet-strengthening-community-policing>.

⁵⁶ Press Release: Justice Department Announces \$20 Million in Funding to Support Body-Worn Camera Pilot Program, United States Department of Justice (May 1, 2015), <http://www.justice.gov/opa/pr/justice-department-announces-20-million-funding-support-body-worn-camera-pilot-program>.

⁵⁷ Abigail Tracy et al., *Is Your Police Force Wearing Body Cameras?*, VOCATIV (Nov. 15, 2014, 10:11 AM), <http://www.vocativ.com/usa/justice-usa/police-force-wearing-body-cameras/>.

“non-evidentiary” 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 store the footage.⁵⁸

In Oakland, California, police-worn body cameras recently 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.⁵⁹ 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.⁶⁰

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 2005.⁶¹ 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.⁶² The scientific community has embraced NGS for medical and other scientific research, but forensic scientists continue to use the Sanger method, which is

⁵⁸ One model policy endorsed by the Prosecutors’ Center for Excellence addresses issues including: when to turn on the camera, how long to retain footage, how to store footage, who is authorized to view footage, and how to handle open records requests. See Antonia Merzon, *Body-Worn Cameras: A Report for Law Enforcement*, <http://pceinc.org/wp-content/uploads/2015/06/Digital-Evidence-Body-Worn-Cameras-A-Report-for-Law-Enforcement.pdf>.

⁵⁹ Henry K. Lee, *Police body cameras and store security caught fatal Oakland cop shooting*, SFGATE (Aug. 13, 2015, 5:18 PM), <http://www.sfgate.com/crime/article/Police-body-cameras-and-store-security-caught-6443269.php>.

⁶⁰ Ford, D., *University Cop Indicted for Murder in shooting of Motorist Samuel DuBose*, CNN (Jul. 30, 2015, 12L18 AM), <http://www.cnn.com/2015/07/29/us/ohio-sam-dubose-tensing-indictment/>.

⁶¹ Yaran Yang et al., *Application of Next-generation Sequencing Technology in Forensic Science*, SCIENCE DIRECT (Oct. 2014), <http://www.sciencedirect.com/science/article/pii/S1672022914001053>.

⁶² Sandra Porter, *Basics: How do you sequence a genome? part III, reads and chromats*, SCIENCEBLOGS (Jan. 28, 2007), <http://scienceblogs.com/digitalbio/2007/01/28/basics-how-do-you-sequence-a-g-2/>; Yang et al., *supra* note 61.

more expensive and far less efficient.⁶³ A move by the forensics community to implement NGS would have large initial costs, 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.⁶⁴

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.⁶⁵ The Federal Aviation Administration (FAA) recently proposed rules that would allow drones for commercial use and would require federal agencies to disclose where they fly drones within the United States.⁶⁶ The FBI has adopted a drone program for domestic surveillance,⁶⁷ and local police departments currently use drones for search-and-rescue missions or for photographing and investigating crime scenes.⁶⁸ But there are Fourth Amendment concerns about using drones for unwarranted surveillance. Fourteen states have passed legislation requiring police to obtain a warrant before using drones for surveillance.⁶⁹

The first arrest based upon 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 sixteen-hour police standoff,

⁶³ Yang et al., *supra* note 61.

⁶⁴ *Id.*

⁶⁵ Kimberly Dvorak, *Homeland Security increasingly lending drones to local police*, THE WASHINGTON TIMES (Dec. 10, 2012), <http://www.washingtontimes.com/news/2012/dec/10/homeland-security-increasingly-loaning-drones-to-1/>.

⁶⁶ Craig Whitlock, *FAA rules might allow thousands of business drones*, THE WASHINGTON POST (Feb. 15, 2015), https://www.washingtonpost.com/world/national-security/faa-releases-proposed-rules-for-domestic-drone-use/2015/02/15/6787bdce-b51b-11e4-a200-c008a01a6692_story.html.

⁶⁷ Dan Roberts, *FBI admits to using surveillance drones over US soil*, THE GUARDIAN (June 19, 2013, 4:20 PM), <http://www.theguardian.com/world/2013/jun/19/fbi-drones-domestic-surveillance>.

⁶⁸ Dvorak, *supra* note 65.

⁶⁹ Kaveh Waddell, *Few Privacy Limitations Exist on How Police Use Drones*, NATIONAL JOURNAL (Feb. 5, 2015), <http://www.nationaljournal.com/tech/few-privacy-limitations-exist-on-how-police-use-drones-20150205>.

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.⁷⁰

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.⁷¹

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. Its database was expected to contain fifty-two million photos by 2015.⁷² The FBI program reports 85 percent accuracy when using images with people facing forward "no more than 15 degrees off the center axis."⁷³ 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.⁷⁴

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

⁷⁰ For more on this story, visit: See Jason Koebler, *First Man Arrested With Drone Evidence Vows to Fight Case*, U.S. NEWS AND WORLD REPORT (Apr. 19, 2012, 5:00 PM), <http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case>.

⁷¹ Face Recognition, Biometric Center of Excellence, Federal Bureau of Investigation, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/face-recognition.pdf (last visited Oct. 28, 2015).

⁷² See Fingerprints and Other Biometrics: Next Generation Identification, Federal Bureau of Investigation, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Sept. 20, 2015); see also Jennifer Lynch, *FBI Plans to Have 52 Million in its NGI Face Recognition Database by Next Year*, ELECTRONIC FRONTIER FOUNDATION (Apr. 14, 2014), <https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year>.

⁷³ Brianna Ehley, *FBI's Billion Dollar Facial Recognition Falls Short of Facebook's*, THE FISCAL TIMES (Jul. 11, 2014), <http://www.thefiscaltimes.com/Articles/2014/07/11/FBI-s-Billion-Dollar-Facial-Recognition-Falls-Short-Facebook-s>.

⁷⁴ Ben Sobel, *Facial recognition technology is everywhere. It may not be legal.*, THE WASHINGTON POST (Jun. 11, 2015), <https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/>.

fraud.⁷⁵ 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 identities by using an alias.”⁷⁶

Gunshot Detection

Seismologists developed gunshot detection technology in the early 1990s, and introduced it to police departments soon after.⁷⁷ 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, and New York have started using gunshot detection technology to identify and locate gunfire as it happens. In D.C., the city’s network of 300 microphones has documented 39,000 shooting incidents in eight years.⁷⁸ While the information is not frequently used at trial, it 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.⁷⁹

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 recent 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,

⁷⁵ Jenni Bergal, *States Crack Down on Driver’s License Fraud*, STATELINE, THE PEW CHARITABLE TRUSTS (July 14, 2015), <http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/07/14/states-crack-down-on-drivers-license-fraud>.

⁷⁶ *Id.*

⁷⁷ U.S. Geological Survey, *Earthquake Technology Fights Crime*, U.S. GEOLOGICAL SURVEY, <http://earthquake.usgs.gov/learn/publications/gunshots/> (last visited Oct. 28, 2015).

⁷⁸ Andras Petho et al., *ShotSpotter detection system documents 39,000 shooting incidents in the District*, THE WASHINGTON POST (Nov. 2, 2013), http://www.washingtonpost.com/investigations/shotspotter-detection-system-documents-39000-shooting-incidents-in-the-district/2013/11/02/055f8e9c-2ab1-11e3-8ade-af23cda135e_story.html.

⁷⁹ Daniel Rivero, *Is NYC’s new gunshot detection system recording private conversations?*, FUSION (Mar. 20, 2015, 3:34 PM), <http://fusion.net/story/107298/is-nycs-new-gunshot-detection-system-recording-private-conversations/>.

virtualized environments, often hosted and managed by third parties.”⁸⁰ 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.”⁸¹ This can create a problem when executing a search warrant, particularly if the data is stored in a foreign country.⁸² 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.”⁸³ 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.⁸⁴

The second concern arises from recent 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.⁸⁵ 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 recent 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

⁸⁰ George Grispos et al., *Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics*, 4 INTERNATIONAL JOURNAL OF DIGITAL CRIME AND FORENSICS 28, 28-48 (2012), <http://arxiv.org/pdf/1410.2123.pdf>.

⁸¹ John M. Cauthen, *Executing Search Warrants in the Cloud*, FBI LAW ENFORCEMENT BULLETIN (Oct. 7, 2014), <https://leb.fbi.gov/2014/october/executing-search-warrants-in-the-cloud>.

⁸² *Id.*; see also Jennifer Daskal, *Case to Watch: Microsoft v. U.S. on the Extraterritorial Reach of the Electronic Communications Privacy Act*, JUST SECURITY (Mar. 6, 2015), <https://www.justsecurity.org/20780/case-watch-microsoft-v-united-states-extraterritorial-reach-electronic-communications-privacy-act/> (discussing ongoing litigation between Microsoft and United States over the government’s ability to access data stored on foreign servers).

⁸³ Cauthen, *supra* note 81.

⁸⁴ *Id.*

⁸⁵ James B. Comey, Director, Federal Bureau of Investigation, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Address Before the Brookings Institution (Oct. 16, 2014), <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

her four-digit passcode. Apple is unable to access the phone's data without Mills' password, and the case remains unsolved.⁸⁶

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 ten-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.⁸⁷

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

⁸⁶ Danielle Maddox, *The Brittney Mills murder case has put Baton Rouge in the middle of the national cellphone encryption debate*, THE ADVOCATE (Aug. 30, 2015), <http://theadvocate.com/news/13122948-123/the-brittney-mills-murder-case>.

⁸⁷ For more on the Missouri case, see Kathee Baird, *Final Suspect in Carl Anderson's Murder Sentenced to 23 Years*, THE STONE COUNTY CHRONICLE, <http://stonecountychronicle.com/final-suspect-in-carl-andersons-murder-sentenced-to-23-years/> (last visited Sept. 20, 2015).

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.⁸⁸ 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. Prosecutors must gain the skills to find the evidence and to explain it to jurors, victims, state legislatures, media, and the community at large. In any given case, they must be prepared to use or examine one or more of the types of evidence discussed above, and to review the evidence for possible exculpatory information. This is becoming increasingly overwhelming, as digital evidence is voluminous and device storage capacities continue to increase.⁸⁹

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. Local, state, and national trainings⁹⁰ are essential, though not every busy prosecutor has the resources or time to attend.

⁸⁸ 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, 8:09 AM), <http://www.cnn.com/2011/CRIME/03/26/jailhouse.calls.recordings/>.

⁸⁹ Lucas Mearian, *Data storage – then and now*, COMPUTERWORLD (Mar. 14, 2014, 6:00 AM), <http://www.computerworld.com/article/2473980/data-storage-solutions/data-storage-solutions-143723-storage-now-and-then.html> - slide 1.

⁹⁰ The National District Attorneys Association and National White Collar Crime Center offer trainings on handling digital evidence and a host of other topics relevant to prosecutors and law enforcement. See NATIONAL DISTRICT ATTORNEYS ASSOCIATION, http://www.ndaa.org/upcoming_courses.html (last visited Oct. 28, 2015); see also NATIONAL WHITE COLLAR CRIME CENTER, <https://www.nw3c.org/> (last visited Oct. 28, 2015).

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.⁹¹ Inter-agency 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 inculcate 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.

Prosecutors' Center for Excellence (PCE) works with prosecutors to improve the criminal justice system and to address emerging issues. A core mission of PCE is to develop and support statewide Best Practices Committees for prosecutors. These non-partisan committees, which consist of prosecutors from all regions of a state, provide a process for prosecutors to proactively address the issues of the day and to strive to improve the criminal justice system. PCE provides technical assistance, training, materials, expert advice, and research on policy issues relevant to the work of these committees.

The writing of this article is supported in part by Grant No. 2013-DB-BX-K005 awarded by the [Bureau of Justice Assistance](#) to the [New York Prosecutors Training Institute \(NYPTI\)](#). The [Bureau of Justice Assistance](#) is a component of the [Department of Justice's Office of Justice Programs](#), which also includes the [Bureau of Justice Statistics](#), the [National Institute of Justice](#), the [Office of Juvenile Justice and Delinquency Prevention](#), the [Office for Victims of Crime](#), and the [SMART Office](#). Points of view or opinions in these materials are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.

⁹¹ As of this publication, 21 states have formed statewide Best Practices Committees for prosecutors, and several others are considering committees as well. See Prosecutors' Center for Excellence, *Best Practices Committees*, <http://pceinc.org/committees/> (last visited January 23, 2016).

ADDITIONAL REFERENCES (by topic)

DNA

Dennis Harris, *New DNA Advances*, EVIDENCE TECHNOLOGY MAGAZINE, http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1114.

Computers

Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 BOSTON BAR JOURNAL 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, <http://jolt.richmond.edu/v18i1/article3.pdf>.

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*, THE NEW YORKER (June 26, 2014), <http://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police>.

Police-Worn Body Cameras

Working Paper, David A. Harris, *Picture This: Body Worn Video Devices ("Head Cams") as Tools for Ensuring Fourth Amendment Compliance by Police* (April 2010), <http://www.nlg-npap.org/sites/default/files/Harris-Video.pdf>.

Harvard Law Review, *Chapter Four: Considering Police Body Cameras*, 128 HARV. L. REV. 1794 (Apr. 2015), <http://harvardlawreview.org/2015/04/considering-police-body-cameras/>.