NEW NATIONAL COMMITMENT REQUIRED:

The Changing Nature of Crime And Criminal Investigations

















POLICE EXECUTIVE RESEARCH FORUM

CRITICAL ISSUES IN POLICING SERIES

NEW NATIONAL COMMITMENT REQUIRED:

The Changing Nature of Crime And Criminal Investigations

January 2018



POLICE EXECUTIVE RESEARCH FORUM

This publication was supported by the Motorola Solutions Foundation. The points of view expressed herein are the authors' and do not necessarily represent the opinions of the Motorola Solutions Foundation or all Police Executive Research Forum members.

Police Executive Research Forum, Washington, D.C. 20036
Copyright © 2018 by Police Executive Research Forum

All rights reserved

Printed in the United States of America

ISBN: 978-1-934485-42-2

Graphic design by Dave Williams.

Photos by Matt Harman.

Contents

Acknowledgments 1

Crime Has Been Changing, and Police Agencies Need to Catch Up 4

By Chuck Wexler

Crime in the United States: What We Don't Know Is a Lot 9

Limitations of Current Crime Measures 10

What We Do Know about Computer-Enabled Crime 12

Sidebar: How Data on Computer-Enabled Crimes Are Collected 14

Sidebar: Recommendations of an NAS Panel on Modernizing the Nation's Crime Statistics 15

How Crime Is Changing 16

The Evolution of Computer-Related Crime 16

Sidebar: Sextortion: A New Type of Computer-Related Crime That Is Having a Dramatic Impact 19

New Ways to Commit Old Crimes 20

Sidebar: How Technology Is Changing Vehicle Thefts and Break-Ins 22

The Dark Web: The New Marketplace for Criminal Activity 22

Sidebar: The Surface Web, the Deep Web, and the Dark Web, Explained 24

The Surface Web and Crime 26

Sidebar: Justin Larson Case Study: How a 30-Year-Old Computer Scientist Used Encrypted Communications to Distribute Drugs 27

How Technology Is Changing Gang Activity 28

Sidebar: How a Brooklyn Street Gang Stole $1.5 Million Through a Fraudulent Money Order Scheme 29

Why Is the Shift in Gang Activity Occurring? 32

The New Crime Environment Presents New Investigatory Challenges for Police 33

The Growing Importance of Digital Evidence.....33
Sidebar: The Vanderbilt Rape Case: The Role of Digital Evidence in a High-Profile Investigation.....35

Encryption and Going Dark.....36
Sidebar: What Is Encryption?.....37

Addressing the Challenges of "Going Dark".....39
Sidebar: The National Domestic Communications Assistance Center.....39
Sidebar: Resources for Obtaining Data from ISPs.....41
Sidebar: Understanding the Harm Caused by the Microsoft Decision.....44

How Criminal Investigations Are Changing: What Agencies Are Doing to Address the Changing Nature of Crime 47

Using New Investigative Tools.....47
Sidebar: Peter the Great: A Case Study in New Investigative Techniques.....48

Rethinking the Organization and Operations of Investigative Units..... 54

New Approaches to Staffing.....56
Sidebar: How Washington, D.C. Police Are Using Civilian Specialists to Accelerate and Improve Criminal Investigations.....57

New Approaches to Training.....59
Sidebar: Free or low-cost training programs for state and local police agencies.....60

Cybersecurity and Officer Safety Concerns.....62

The Importance of Collaboration with Local, State, and Federal Partners.....62

Technologies that Could Shape the Future of Criminal Investigations 65

CONCLUSION: Catching Up with the Changes in How Crimes Are Committed: 9 Urgent Recommendations..... 68

About PERF.....73

About Motorola Solutions and the Motorola Solutions Foundation 75

APPENDIX A: Participants at the Critical Issues Meeting— "The Changing Nature of Crime and Criminal Investigations".....76

Acknowledgments

TO SAY THAT COMPUTERS, COMMUNICATION SYSTEMS, AND OTHER technologies are changing the policing profession is a vast understatement. In recent years, much of PERF's research and policy development work has focused on the impact of new technologies on crime analysis and police use of force. We have also studied new devices such as body-worn cameras and, most recently, the revolution that is occurring in 911 and emergency communications.

For this report, we stepped back and assessed the impact of computers and other technologies on the *nature of crime itself,* and on how technology is changing investigations. As part of our *Critical Issues in Policing* series, PERF assembled nearly 200 experts in criminal investigations, technology, and police operations and management to explore these issues during a day-long conference in Washington, D.C. We learned about new types of computer-related crimes, and also about criminals' use of technology to commit many old types of crime.

For law enforcement agencies to keep up in this new environment, their approaches to criminal investigations must change. Relying on physical evidence and witness statements is no longer sufficient in many cases. Investigators need to know how to access and secure data from mobile devices, social media, Fitbits and other devices that store computerized data, and the so-called "dark web."

The reality is that the science of criminal investigations is changing rapidly, and many law enforcement agencies are not prepared for the changes that are taking place. This report is a wake-up call for the policing profession. If we are to be successful in combating crime in the 21st century, agencies must have the training, tools, and skilled personnel to understand the changing nature of crime and to be resourceful in investigating new types of crime.

I am grateful to the PERF members and other subject matter experts who participated in our meeting and shared their experiences and insights. A complete list of meeting participants can be found in Appendix A, on page 76.

We are especially indebted to the Portland Police Bureau, Immigration and Customs Enforcement/Homeland Security Investigations, the U.S. Postal Inspection Service, and the Greenville, SC Police Department, who took the time to walk us through the "Peter the Great" case study (see page 48). This case demonstrated that when local and federal agencies work together, they

can operate safely in the dark web, and take down an online synthetic opioid operation that stretched around the world and claimed lives in the United States.

This report would not have been possible without the support of the Motorola Solutions Foundation, which has funded more than 30 *Critical Issues in Policing* projects. Because of Motorola Solutions' forward-thinking generosity, PERF has been able to explore issues that advance the profession and help to keep our communities safe.

Special thanks to Greg Brown, Motorola Solutions Chairman and CEO; Jack Molloy, Senior Vice President for Sales, North America; Jim Mears, Senior Vice President; Gino Bonanotte, Executive Vice President and Chief Financial Officer; Cathy Seidel, Corporate Vice President, Government Relations; Matt Blakely, Director of the Motorola Solutions Foundation; and Tracy Kimbo, Director of Government Marketing, who participated in the meeting. And Rick Neal, retired Vice President at Motorola Solutions and now President of the Government Strategies Advisory Group, continues to help with *Critical Issues* projects.

And once again, I thank the PERF staff members who planned and executed another successful *Critical Issues* project. They did excellent work in researching the issues, identifying experts to participate in the conference, and making sure we asked the right questions and covered the key topics.

This project was managed by Kevin Morison, Chief Operations Officer, and Jessica Toliver, PERF's Director of Technical Assistance. They developed the agenda, oversaw meeting preparations, and contributed to writing and editing of the final report. The report was drafted by Senior Research Assistant Madeline Sloan and Research Associate Margaret Brunner, who also conducted much of the background research. Research Associates Rachael Arietti and Elizabeth Miller also assisted with research. Sean Goodison, Deputy Director of PERF's Center for Applied Research and Management, provided expertise on digital evidence and presented findings at our conference from a recent PERF-RAND Corporation research project on digital evidence.

Senior Research Assistant Sarah Mostyn organized data and designed visuals for the meeting, and masterfully managed conference logistics, a significant undertaking for a meeting of this size and complexity. Assisting on the day of the conference were Research Assistant Allison Heider, Senior Research Assistant Matt Harman, Senior Office Coordinator Jennifer Brooks, and Senior Associate Dan Alioto. Among other duties, Matt was responsible for photography, and Allison and Dan assisted with live-tweeting the event. James McGinty, Assistant Director of Communications, managed visual presentations and assisted with report preparation. Communications Director Craig Fischer edited this report and assisted with writing. PERF's graphic designer, Dave Williams, designed and laid out the report. As always, Executive Assistant Soline Simenauer kept the project team on track, and Andrea Morrozoff, PERF's Chief Strategy Officer, provided overall direction for this *Critical Issues* project.

I'm grateful for the commitment and determination among forward-thinking police executives and investigators, who recognize the importance of new approaches to technology. Their resourcefulness in using technology to combat new types of computer-enabled crime provides direction to the entire law enforcement profession. This report should help police chiefs, sheriffs, and other leaders understand and prepare for the changes that are under way.

Chuck Wexler
Executive Director
Police Executive Research Forum
Washington, D.C.



Crime Has Been Changing, and Police Agencies Need to Catch Up

By Chuck Wexler

THE UNITED STATES IS EXPERIENCING A TRANSFORMATION IN how criminals are using technology to invent new types of crime, and are creating new methods for committing traditional crimes.

These developments are fundamental in nature. People who never committed crimes before are tempted when they learn how easy it can be to deal drugs or steal thousands of dollars, without ever having to confront a victim face-to-face. Criminal gangs that used to specialize in selling drugs on the street corner, or holding up pedestrians for the cash in their wallets, are switching to crimes they can commit in the privacy of their homes, by clicking keys on a keyboard.

Police departments will need to make significant changes to address these developments, but most agencies have not yet begun the process. Police agencies will need to hire people with new skills, provide new training to their officers and detectives, and in some cases restructure how they are organized.

First, a few facts that show the extent and the nature of this problem, and then our analysis of what we need to do. Consider the following:

- **The nation is experiencing an epidemic of drug abuse fatalities, fueled in part by the internet.** It's no longer just people on street corners selling drugs. Today, drug traffickers are ordering lethal drugs like fentanyl on the internet, having it delivered from China, and then selling it and shipping it to customers *through the U.S. mail!* The result is that thousands of people are dying of fentanyl overdoses.[1]

- **New types of crime, based on technology, are being invented.** For example, in just the last few years, "ransomware," a type of online attack that blocks victims' access to their computers until they pay a ransom, has become a billion-dollar-a-year enterprise. Even law enforcement agencies have been

1. See *The Unprecedented Opioid Epidemic: As Overdoses Become a Leading Cause of Death, Police, Sheriffs, and Health Agencies Must Step Up Their Response.* Police Executive Research Forum, 2017, pp. 15-18. http://www.policeforum.org/assets/opioids2017.pdf

victims of ransomware attacks, and in some cases police departments have paid the ransom.

- **Local gang members and other criminals have noticed that they can make more money, with less risk of getting caught, and smaller penalties if they do get caught, by using technology.** Why rob a convenience store if you can get on a computer, steal someone's identity (or create an entirely new, fictitious identify of a person who doesn't exist), and rip off major U.S. banks or credit card companies? It's a much "cleaner" way of profiting from crime, with no potentially dangerous face-to-face encounters with victims. The risk is lower and the payoff higher, with criminal penalties in some cases being essentially non-existent.

- **Crime statistics do not reflect most of these changes.** According to the FBI, there were 4,251 bank robberies in 2016—a 45-percent decrease compared to 2004. Meanwhile, the FBI reports that there were nearly 300,000 reports of people being victimized on the internet in 2016. In one famous incident, thieves working with computer experts in more than 20 countries stole $45 million from thousands of automated teller machines over a 10-hour period—which was more than the total losses from "traditional" physical robberies of banks over an entire year.[2]

  So we know that internet-based crimes are on the rise. But because the existing systems for measuring crime were created decades ago and have not kept pace with new developments, they only scratch the surface in measuring new crimes. "Only an estimated 15 percent of the nation's fraud victims report their crimes to law enforcement," the FBI said. So for every crime that is reported to the police, there are about six more crimes that are *not* reported. While the exact totals are not known, it is clear that "millions of people in the United States are victims of Internet crimes each year," the FBI said.[3]

- **Even when technologies are invented to prevent crime, criminals adapt.** For example, the electronic chips in car keys have made it almost impossible for a thief to start the engine and steal a car. So criminals developed key-fob jamming devices. As a car owner walks away from his car and clicks the key to lock the doors, the criminal uses an electronic device to disrupt the signal, so the car is not really locked. The criminal waits until the owner disappears from sight, and then gets in the car—usually not to steal it, but to look for the registration, insurance cards, or other paperwork such as credit card statements that can be used to commit identity theft.

---

2. See "Bank Crime Statistics." FBI. https://www.fbi.gov/investigate/violent-crime/bank-robbery/bank-crime-reports. See also "In Hours, Thieves Took $45 Million in A.T.M. Scheme." *New York Times*, May 9, 2013. http://www.nytimes.com/2013/05/10/nyregion/eight-charged-in-45-million-global-cyber-bank-thefts.html?pagewanted=all

3. *2016 Internet Crime Report*. FBI Internet Crimes Complaint Center, pp. 2-3. https://pdf.ic3.gov/2016_IC3Report.pdf.

Now consider a few of the challenges that police are facing:

- **The work of criminal investigators is becoming more complex.** Not very long ago, detectives responding to a homicide or other serious crime had a clear focus: quickly get to the scene, collect physical evidence, and interview any witnesses. Today, investigators must retrieve smartphones from victims and suspects and scour their social media accounts for clues; access nearby security camera feeds, automated license plate readers, and traffic enforcement cameras; and try to obtain data from other devices such as Fitbits, GPS devices, and video cameras in the victims' or suspects' cars. And investigators must do all this work quickly, before the digital trail gets cold.

  "I was a homicide detective for 10 years, and the way homicide cases are done now is completely different," said Major Richard Perez of the Fairfax County, VA Police Department. "Back in the day, a homicide investigation was all about doing an interview, going to the victim's job, talking to the family, etc. Nowadays, victims typically have one to three smart devices, and witnesses and suspects do too. So if I want to trace a victim's movements, I have to download cell records, obtain subpoenas to review text messages, look at phone logs and social media accounts, and review all other forms of digital evidence. You need a minimum of three support people behind each homicide detective."

  Chief Daniel Slaughter of the Clearwater, FL Police Department said, "We need to be recruiting for different skill sets and educational experiences than a typical boots-on-the-ground guy. We need to develop the future leaders of our department into this specialty."

- **Police are not getting a lot of help from the technology sector.** Criminals are using the "dark web" to make themselves anonymous online. Even when police obtain court orders allowing them to get into a cell phone in order to find out who a victim or suspect was communicating with, they often find that there is no way to get past the user's passcode. Smartphone manufacturers argue that they cannot build a special "backdoor" for police to access the data in these devices, because criminals inevitably would hack into the backdoor, making everyone's phones less safe.[4]

- **Technology is changing the environment every day, and most police agencies are far behind the curve.** Because policing in the United States is decentralized, there are thousands of small and medium-size agencies that lack the resources to respond to the changes cited above. Even large, well-funded agencies have a lot of work to do—finding and hiring technology experts; training officers to understand the basics of crime-related technologies; and rethinking the traditional structure of a police agency. The old "silos," such as special units for organized crime, gangs, and narcotics, are becoming less relevant as cybercrime becomes a part of all these traditional categories.

- **Crime data systems have not kept pace with changes in crime:** A major challenge facing the profession is that we do not have an accurate picture

4. "How an Apple passcode has foiled the FBI." *Los Angeles Times*, February 17, 2016. http://www.latimes.com/business/technology/la-fi-0218-apple-encryption-20160218-story.html

of the problem we are facing. The FBI's Uniform Crime Reporting (UCR) system has traditionally focused on commonly reported "street crimes," and has not kept pace with new trends involving computer-enabled crime. The UCR's property crime categories—burglary; larceny/theft; motor vehicle theft; and arson—do not reflect today's realities. In December 2017, the FBI announced that its National Incident-Based Reporting System (NIBRS), a more sophisticated database than the traditional UCR, was updated to include new definitions of "hacking computer invasion" and "identity theft" in the fraud category.[5] This is a step in the right direction, but we are still a long way from having accurate, detailed data about computer-facilitated crimes.

- **In many cases, it's not clear how, or even if, local police are prepared to take reports and investigate offenses like identity theft and credit card fraud.** In 2000, the FBI created the Internet Crime Complaint Center (IC3), whose mission is "to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected internet-facilitated criminal activity."[6] Yet 17 years later, the IC3 reports that "only an estimated 15 percent of the nation's fraud victims report their crimes to law enforcement." If local police agencies were ahead of the curve on Internet-facilitated crime, the reporting rate would certainly be higher than 15 percent.

  In many cases, there is little incentive to report internet crime. Banks and credit card companies routinely cancel fraudulent charges made against a victim's account, so there is no need for the victim to report the crime to be reimbursed. By contrast, victims of "traditional" crimes such as burglary often must obtain a police report in order to file insurance claims, so there is more reporting such crimes.

  So the true extent of this problem is hidden. But we do know that the total financial losses due to just one type of internet crime—identity theft—totaled more than $15 billion in 2014, according to a crime victimization survey conducted by the Bureau of Justice Statistics.[7]

  Data collection is more than just an academic undertaking to support research. The fact that we don't know the true nature of crime in our country should be a concern. Data helps to drive policy, resources, and operations.

PERF convened the experts: To better understand the changing nature of crime in the United States, and what those changes mean for police agencies and their investigative functions, PERF brought together a cross-section of experts in Washington, DC on August 9, 2017. This report summarizes the wide-ranging discussions that took place at the meeting. It also captures

5. "2016 NIBRS Crime Data Released." FBI news media release, Dec. 11, 2017. https://www.fbi.gov/news/stories/2016-nibrs-data-released. See also "NIBRS Offense Definitions." https://ucr.fbi.gov/nibrs/2016/resource-pages/nibrs_offense_definitions-2016_final.pdf

6. *2016 Internet Crime Report*, p. 2. https://pdf.ic3.gov/2016_IC3Report.pdf.

7. *Victims of Identity Theft, 2014.* U. S. Department of Justice, Bureau of Justice Statistics. Sept. 2015; revised November 2017, page 7. https://www.bjs.gov/content/pub/pdf/vit14.pdf

interviews conducted with attendees before the conference and other background research and follow-up.

Here is what our project taught us:

The status quo is completely unacceptable. Today's crime-fighting challenges are far greater than in the past, but most local police agencies are nowhere near being prepared to meet the challenges. Only a small fraction of internet-based crimes are even being reported to police, much less investigated. And when a crime *is* reported, often it is not clear which law enforcement agency is responsible for investigating it, because the victim may be located thousands of miles away from the perpetrator, in a different city, state, or even nation. And the crime often involves a bank or other institution that may be headquartered in another location. Work does not get done when nobody knows whom the job belongs to.

Local police agencies must become significantly more involved, because these crimes are far too numerous to be handled solely by the FBI and other federal agencies. But in most of the United States' 18,000 local police agencies, policies and protocols are not being written, cyber experts and analysts are not being hired, and officers are not receiving the training they need to investigate these crimes.

The conclusion to this report contains specific steps that law enforcement agencies can take today to prepare themselves for the more complex criminal investigations of tomorrow. Here is what needs to be done:

- The United States needs a new national commitment to address the growing threat of computer-based crime, similar to the nation's response to the terrorist attacks of 9/11. Existing systems for measuring, preventing, and investigating crime are obsolete.
- We need to hire police officers and analysts with new skills, and give them the continuous training they will need to keep up with constantly changing crime patterns. Detectives in particular will need to adjust how they do their jobs.
- We need better systems for gathering data about these new types of crime.
- We need a new national approach to who "owns" these crimes. The first step in solving a crime is deciding which police agency is responsible for investigating it.
- We need to find a way of getting local law enforcement agencies up to speed, because the FBI and other federal agencies can investigate only a small fraction of these crimes.

Most importantly, we need a sense of urgency about this issue. The people committing these new types of crime, or committing old types of crime in new ways, realize that their risk of being caught is minuscule. Law enforcement agencies at all levels—federal, state, and local—must step up and take on new responsibilities for identifying these crimes and investigating them. The national UCR figures that indicate very low historical crime rates are not conveying the whole truth when millions of crimes are under the radar.

Crime in the United States: What We Don't Know Is a Lot

"We don't know the true nature of crime in the U.S., because we don't have the systems in place to capture all—or even most—crime types.

"The harm may be much greater for the crimes we don't know about than for the crimes we do know about."

— Nola Joyce, former Deputy Commissioner and Chief Administrative Officer, Philadelphia Police Department



Nola Joyce, former Deputy Commissioner, Philadelphia Police Dept.

AS MEASURED BY TRADITIONAL REPORTING SYSTEMS, CRIME IN THE United States has declined sharply in recent decades. But even as rates of homicide, robbery, burglary, and other crimes have fallen since the 1990s (albeit with significant upticks in violent crime in 2015 and 2016), new types of crimes—many of them enabled by computer technology—have begun to proliferate. In 2016, the most recent year for which data are available, there were nearly 300,000 internet crimes reported to a federal database, with losses totaling more than $1.4 billion, and only an estimated 15 percent of these crimes are reported to law enforcement, according to the FBI. While the actual totals are unknown, it is clear that "millions of people in the United States are victims of Internet crimes each year," the FBI said.[8] If the losses from unreported crimes are similar in magnitude to the crimes that *are* reported, the total costs may approach $10 billion per year.

What do we know about the nature and extent of these computer-enabled crimes? Are increases in these types of crimes offsetting the dramatic reduction in "street crimes" that have been recorded and celebrated?

These are important questions not just for researchers and statisticians. They are important for law enforcement executives as well. As the Compstat era in policing has demonstrated, statistical information is a key factor that drives policies, resources, and operations. Participants at the *Critical Issues*

8. "2016 Internet Crime Report." FBI Internet Crimes Complaint Center, pp. 2-3. https://pdf.ic3.gov/2016_IC3Report.pdf.

meeting said that having accurate and complete data is especially important now, because the nature of crime and criminal investigations is changing dramatically.

Limitations of Current Crime Measures

Since 1930, the Federal Bureau of Investigation (FBI) has compiled and published crime data in the United States through the Uniform Crime Reporting (UCR) Program. The UCR and the National Crime Victimization Survey (NCVS), which is managed by the Bureau of Justice Statistics, serve as the primary measures of crime in the country.[9] The two systems focus largely on a set of violent and property crimes that are defined and reported.

Since the early 1990s, the news about the crime measured by the UCR and NCVS has been encouraging. According to UCR data, from 1993 to 2015, the violent crime rate declined by 50 percent. The decrease was even larger—77 percent—when measured by the NCVS. Similarly, property crimes dropped by 48 percent according to UCR data—and 69 percent per the NCVS—during the same period.[10] (UCR and NCVS statistics generally move in the same direction over time, but they can differ, for a number of reasons. One major difference is that the UCR measures crimes that have been reported to local police agencies, while NCVS is a survey that asks respondents about criminal victimizations they have experienced, whether or not they reported them to the police.)

As promising as these trends are, experts point out one glaring deficiency: traditional crime measurement systems, especially the UCR, do not adequately measure new and evolving types of crime. Thus, they do not provide a complete and accurate picture of crime in the United States.[11]

> "Without a more comprehensive set of crime statistics, we cannot know whether the large-scale declines in the 1990s in traditional and well-measured violent and property crimes reflect broader declines in crime, or whether these recorded changes were offset by notable increases in alternative and newly-emerging forms of crime that are not captured in current data systems."[12]
>
> **— Janet Lauritsen and Daniel Cork, Panel on Modernizing the Nation's Crime Statistics**



Daniel Cork, Study Director, Panel on Modernizing the Nation's Crime Statistics

In recent decades, new technologies have led to new types of crimes, such as identity theft and credit card fraud. Many of these crime types do not fit easily into the UCR framework. For example, the UCR categorizes most

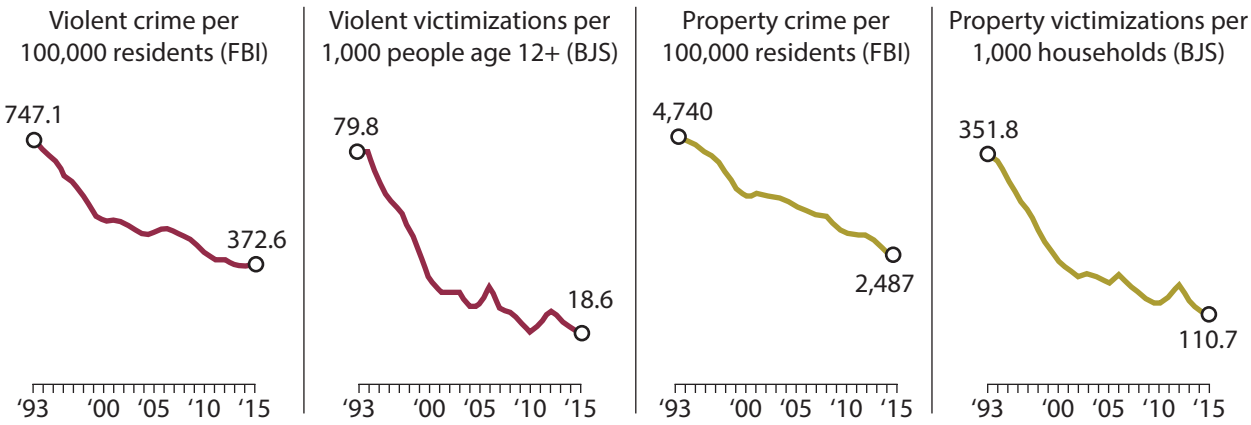
9. "The Nation's Two Crime Measures." Bureau of Justice Statistics. January 26, 2017. https://www.ucrdatatool.gov/twomeasures.cfm

10. "5 facts about crime in the U.S." Pew Research Center, February 21, 2017. http://www.pewresearch.org/fact-tank/2017/02/21/5-facts-about-crime-in-the-u-s/

11. National Academies of Sciences, Engineering, and Medicine. (2016). *Modernizing Crime Statistics—Report 1: Defining and Classifying Crime.* Washington, DC: The National Academies Press. https://www.nap.edu/read/23492/chapter/2

12. From an upcoming paper to be published in *Criminology and Public Policy*.

Trends in Violent Crime and Property Crime, 1993–2015



Source: Pew Research Center, February 2017, compilation of data from the Uniform Crime Reporting program (FBI) and the National Crime Victimization Survey (BJS). http://www.pewresearch.org/fact-tank/2017/02/21/5-facts-about-crime-in-the-u-s/

"white-collar crimes" as fraud, forgery/counterfeiting, embezzlement, or the catch-all "all other offenses."[13]

Current crime-reporting structures present other challenges for police officials in determining how to categorize certain complex crimes. For example, if a credit card is stolen from a victim in one jurisdiction, but the credit card is used to make purchases in another jurisdiction, which agency reports the crime? In reporting many computer-related crimes, it is often difficult to define the criminal action, identify victims, and determine where the offense took place.[14]

Victims of these crimes often face challenges in reporting the offenses to the police. Which agencies are supposed to accept reports of identity theft, credit card fraud, and other computer-enabled crimes? And who conducts the follow-up investigation? These questions are further complicated by the fact that in some instances, the victims are banks and other financial institutions, which may be reluctant to report these crimes because of the bad publicity they can generate. If these crimes are never reported to local police agencies, they will never be adequately captured by current crime reporting systems.

> "We have yet to put a face on intellectual crimes and cyber-crimes. By tracking offenses, identifying victims, and calculating financial losses, we can illustrate how these crimes are impacting our communities."
>
> **— Captain Craig Buckley, City of Fairfax (VA) Police Department**



Fairfax, VA Police Captain Craig Buckley

The FBI's National Incident-Based Reporting System (NIBRS) is improving the quality and completeness of crime data. For example, while UCR captures

13. Barnett, C. "The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data." FBI Criminal Justice Information Services Division. https://ucr.fbi.gov/nibrs/nibrs_wcc.pdf.

14. Ibid, 9-10.

only the most serious offense committed during a single incident, NIBRS collects information on multiple offenses within the same incident. (For example, if an armed robbery also includes an aggravated assault, UCR would record only the robbery, while NIBRS would capture both crimes.) NIBRS also captures additional information about victims, offenders, arrestees, and property involved in the crimes.[15]

In December 2017, the FBI announced that newly released NIBRS data for 2016, for the first time, includes data on the fraud offenses of identity theft and hacking/computer invasion.[16]

However, NIBRS has its limitations. Only 37 percent of U.S. law enforcement agencies participating in the UCR program in 2016 submitted their crime data via NIBRS (although the FBI plans to fully transition from UCR to NIBRS by 2021).[17] And although NIBRS captures more detailed information on many crimes, the system still does not fully account for a full range of internet-enabled crimes. As the Panel on Modernizing the Nation's Crime Statistics noted, "NIBRS' core development work and structuring took place in the late 1980s, and it is not clear that its design has kept pace with the times."[18]

What We Do Know about Computer-Enabled Crime

Without UCR or NIBRS data to provide complete data on computer-enabled crime, law enforcement executives and the public have had to rely on other sources, including reports collected by the FBI's Internet Crime Complaint Center (IC3) and the Federal Trade Commission's Consumer Sentinel Network. Not surprisingly, these sources suggest that crimes such as identity theft are on the rise, although the data itself is not comprehensive.

The IC3 collects more than 800 complaints per day from members of the public who suspect they are victims of internet-facilitated criminal activity. The number of complaints received by IC3 increased 14 percent between 2013 and 2016, to nearly 300,000. The monetary losses associated with those internet-related crimes surpassed $1.4 billion in 2016.[19]

And for every Internet crime that is reported to law enforcement, the FBI estimates that there may be approximately 6 more such crimes that are not reported.[20]

---

15. "NIBRS Overview." FBI. https://ucr.fbi.gov/nibrs-overview

16. "FBI Releases 2016 NIBRS Crime Statistics in Report and CDE, Promotes Transition of Agencies." FBI news media release, Dec. 11, 2017. https://ucr.fbi.gov/nibrs/2016/resource-pages/nibrs-2016_summary.pdf

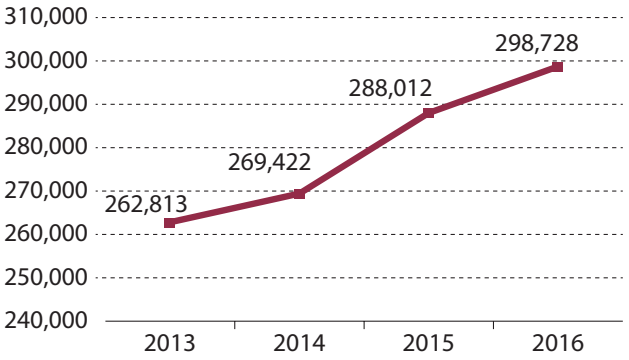
17. Ibid.

18. National Academies of Sciences, Engineering, and Medicine. (2016). *Modernizing Crime Statistics—Report 1: Defining and Classifying Crime.* Washington, DC: The National Academies Press. Page 8. https://www.nap.edu/read/23492/chapter/2.

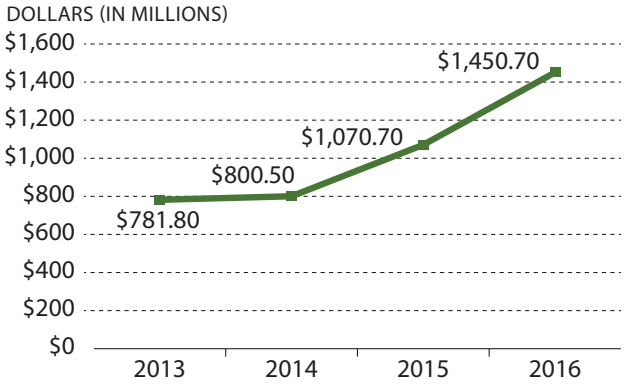
19. Ibid.

20. "2016 Internet Crime Report." FBI Internet Crimes Complaint Center, p. 3. https://pdf.ic3.gov/2016_IC3Report.pdf.

Total Internet Crime Complaints



Total Monetary Losses



Source: Federal Bureau of Investigation, Internet Crime Complaint Center: 2016 Internet Crime Report, p. 2. https://pdf.ic3.gov/2016_IC3Report.pdf

Identity Theft Complaints



Source: Federal Trade Commission, "Consumer Sentinel Network: Consumer Sentinel Network Data Book." March 2017. Page 5. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

Identity theft is on the rise: The specific crime of identity theft also appears to be on the rise. In 2016, the Federal Trade Commission received 399,225 complaints of identity theft, a 59 percent increase from 2010.[21] Supplemental data from the Justice Department's National Crime Victimization Survey in 2014 indicate that 17.6 million people, or about 7 percent of U.S. residents age 16 and older, were victims of identity theft.[22] Eighty-six percent of those victims reported fraudulent use of financial account information, such as credit cards or bank accounts. The losses are costly, with $15.4 billion in

21. "Consumer Sentinel Network Data Book for January-December 2016." Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf

22. "Victims of Identity Theft, 2014." U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf

cumulative loss attributed to identity theft in 2014 alone, according to NCVS data. Although the number of identity theft victims is large and growing, these crimes are vastly underreported. Fewer than 1 in 10 victims report the incident to the police.[23]

Given the lack of comprehensive data collection systems and the severe underreporting of computer-enabled crimes, there is currently no way to accurately measure the number of these offenses or their monetary impact on victims and on the national economy. This lack of data also makes it difficult for law enforcement agencies to formulate strategies and devote the resources needed to combat the problem.

How Data on Computer-Enabled Crimes Are Collected

The United States lacks a robust, consistent system for collecting data about computer-enabled crimes. Currently, police agencies and the public rely on valuable but incomplete data sources. There are three primary sources of this information:

FBI Internet Crime Complaint Center (IC3). The IC3 accepts complaints from victims or third parties who suspect internet-facilitated criminal activity. Crime reports are investigated, and the data is summarized in annual reports to increase public awareness.[24]

Federal Trade Commission Consumer Sentinel Network (CSN). The CSN collects data on consumer complaints filed to the Federal Trade Commission, state law enforcement organizations, federal agencies, and non-governmental organizations. The CSN publishes data on fraud, identity theft, and other consumer complaints in an annual report.[25]

In addition, the **National Crime Victimization Survey Data Supplement** in 2014 captured one-time information on identity theft victimizations from NCVS respondents age 16 and older, but only for that year.[26]

23. Ibid.

24. Federal Bureau of Investigation Internet Crime Complaint Center. IC3 Mission Statement. https://www.ic3.gov/about/default.aspx.

25. "Consumer Sentinel Network Data Book for January-December 2016." Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

26. "Victims of Identity Theft, 2014." U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/vit14.pdf.

Recommendations of an NAS Panel on Modernizing the Nation's Crime Statistics

> "Crime continues to evolve and take different shapes. Accordingly, there is a need for an expansive framework for crime classification that is amenable to periodic revision."
>
> **— Panel on Modernizing the Nation's Crime Statistics, National Academy of Sciences, Engineering, and Medicine**

In 2013, the National Academies of Sciences, Engineering, and Medicine formed the Panel on Modernizing the Nation's Crime Statistics, within the National Research Council. Composed of researchers and practitioners, this 15-member body spent more than three years assessing and making recommendations for the development of a modern set of crime measures in the United States, and for the best means for obtaining them.[27]

One resource the panel explored was the International Classification of Crime for Statistical Purposes (ICCS). The ICCS was organized by the United Nations Office of Drugs and Crime to serve as a shared, international framework for crime classification. A key feature of the ICCS is that it allows police officials to provide essential characteristics of an offense, which is particularly useful for noting internet-enabled crimes.[28]

In its report, the National Academies panel advocated a modified ICCS approach that combines a detailed list of crime categories with an extensive set of attributes, or tags, to describe pertinent details of the offense.[29] For example, a "cybercrime-related" tag would allow crime reporting officials to identify various forms of crime committed with the use of a computer.[30] The panel noted that this type of approach has the potential to more accurately capture the number and nature of internet-enabled crimes and, as a result, present a more comprehensive picture of crime in the United States.

27. "Modernizing the Nation's Crime Statistics: Project Scope." The National Academies of Sciences, Engineering, and Medicine. http://sites.nationalacademies.org/dbasse/cnstat/currentprojects/dbasse_085946.

28. United Nations Office on Drugs and Crime. "International Classification of Crime for Statistical Purposes (ICCS)." http://www.unodc.org/unodc/en/data-and-analysis/statistics/iccs.html.

29. National Academies of Sciences, Engineering, and Medicine. (2016). "Modernizing Crime Statistics—Report 1: Defining and Classifying Crime." Page 133. https://www.nap.edu/read/23492/chapter/2

30. United Nations Office on Drugs and Crime. (2015). "International Classification of Crime for Statistical Purposes (ICCS), Version 1.0." http://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_English_2016_web.pdf.

How Crime Is Changing

> "Technology and social media have opened up a new variety of potential ways for criminals to get tasks accomplished."
>
> **— Arlington County, VA Police Department Deputy Chief Charles Penn**

COMPUTERS, COMMUNICATIONS PLATFORMS, AND OTHER TYPES OF new technology are changing crime in two important ways. First, the variety of computer-related crimes continues to grow. In addition to cyber-crimes that already have become familiar to most people, such as identity theft and credit card fraud, newer types of offenses have emerged, including "sextortion" (sexual exploitation, in some cases by blackmailing victims with the threat of disseminating sexual images of them) and synthetic identity theft (creating an entirely new fictitious identity).

Second, technology is changing how some long-established types of crimes are committed today. For example, drug dealers are discovering they can move larger quantities of illegal drugs more easily and with less risk via "dark web" internet marketplaces and the U.S. mail than they can by selling drugs on the streets.

These changes have significant implications for police agencies throughout the country. Technology is changing the policies, procedures, and organizational structures that police must adopt to fight crime, as well as the resources police must obtain.

This chapter explores how crime is changing. Subsequent chapters examine how police agencies are responding to these changes.

The Evolution of Computer-Related Crime

> "The shift from street crimes to cyber-crime is not specific to any one group or crime. We are seeing a large-scale change affecting everything from child exploitation to distribution of narcotics. I believe this large shift is occurring because of the anonymity the internet provides."
>
> **— Captain Paul Kammerer, Volusia County (FL) Sheriff's Office**

Computer-related crime—"cyber-crime"—is not new. Since the advent of the public internet in the early to mid-1990s, criminals have tried to exploit the technology for financial gain through a variety of schemes. In recent years, the variety of these crimes has grown, with new offenses such as ransomware, revenge porn, and sextortion becoming more prevalent.

Ransomware: In just a few years, for example, ransomware (a type of online attack that blocks a user's access to his or her computer system until a ransom is paid) has become a billion-dollar-a-year criminal enterprise.[31] Even law enforcement agencies have been victims of ransomware.

Synthetic identity theft: As technology becomes more sophisticated, so have computer crime schemes. One example is a twist on identity theft, called "synthetic identity theft." Typically, identity theft involves stealing personally identifiable information, such as a Social Security Number or credit card number, from a single individual, and using that information to make purchases, apply for credit, file fraudulent tax returns in the name of that individual in order to receive a tax refund, or otherwise benefit financially.

Synthetic identity theft involves taking pieces of information from multiple people to create an entirely new, fictional identity that can often be exploited for long periods of time.[32] Synthetic identity theft is more complex, often more difficult to detect, and designed to provide a much larger, long-term yield.

> "In synthetic identity theft, the criminal obtains a social security number, usually a child's, and will then attach a fake name/address to it and piggy-back on another person's credit to establish credit. The criminals build up credit, secure mortgages, take out loans, and then cash them all out. It is a long-term scam. It takes time, but the profits are high."
>
> **— Chicago Police Department Detective Patricia Dalton**



Chicago Police Detective Patricia Dalton

Children are especially vulnerable to synthetic identity theft because their credit profiles are blank slates. Since credit reports are not typically run on children, many victims do not discover that their identity has been compromised until they are in their late teens or early 20s and are applying for a student loan or their first credit card.

Why computer-related crime is attractive to criminals: Experts cite at least four reasons why computer-related crime is so attractive to today's offenders:

1. **Anonymity.** The internet provides a high degree of anonymity and cover. This is particularly true in the heavily encrypted part of the internet known as the "dark web."

---

31. See, for example, "Ransomware: Now a Billion Dollar a Year Crime and Growing." *NBC News*, Jan. 9, 2017. https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646.

32. "Why are fraudsters targeting your child's identity?" *CBS News,* July 30, 2014. https://www.cbsnews.com/news/synthetic-id-theft-why-are-fraudsters-targeting-your-childs-identity/.

2. **Potential for large financial gains, with reduced risk.** With only a modest, up-front investment in computer equipment and basic technical skills, cybercriminals can steal significantly more money with a few clicks of the mouse than what a robber can get from the cash register at a convenience store — and without the risk of directly encountering their victims or the police. The monetary losses associated with the 298,728 internet-related crimes reported to IC3 in 2016 totaled approximately $1.45 billion, or $4,857 per crime on average.[33]

   Considering that most of the internet-based crimes did not require the offenders to ever face their victims, witnesses, or the police, it becomes clear why internet crimes are so common: The risk of being apprehended is small, and the "take" is large.

3. **Investigation and prosecution are more difficult.** Many computer-enabled crimes cross multiple jurisdictional boundaries. The offender may be in one jurisdiction, the victim in another, and the offenses (such as fraudulent online purchases) in yet another location.

   Participants at PERF's *Critical Issues* meeting noted that the multi-jurisdictional nature of computer-related crime is one of the biggest challenges in identifying and prosecuting cyber criminals, because it is difficult for an investigation to begin when there is no clarity about who "owns" the crime. How can a police department assign an investigator to interview a victim and make other inquiries if the department doesn't know whether it has jurisdiction over the crime?

   "The national and international nature of internet crime makes it much harder for us to track down," said Fayetteville, NC Police Captain James Nolette.



Fayetteville, NC Police Captain James Nolette

4. **The lag between technology and the law.** Because it takes time for legislators to recognize and write laws that address complex, technical matters, some cyber-crimes can go on for years before they become illegal. Sergeant Sylvan Altieri, with the Metropolitan Police Department of Washington, D.C., cited the example of revenge porn. "Revenge porn has been a phenomenon ever since the internet came into existence, but it took years and years for 'unlawful publication' legislation to become law," he said.

   And even when laws against specific cyber-crimes are enacted, the criminal penalties are often low, relative to the amount of damage inflicted by the crime.[34] As a result, the threat of criminal penalties may not be a significant deterrent.

   Internet-related crime is often more lucrative; it is harder to detect and quantify; and it results in fewer criminal penalties than many

>> continued on page 20

33. "2016 Internet Crime Report." FBI Internet Crimes Complaint Center, p. 2. https://pdf.ic3.gov/2016_IC3Report.pdf.

34. See "The Utah Model: A Path Forward for Investigating and Building Resilience to Cyber Crime." Police Executive Research Forum and U.S. DOJ, Bureau of Justice Assistance. Pages 21-23. http://www.policeforum.org/assets/UtahModel.pdf

Sextortion: A New Type of Computer-Related Crime That Is Having a Dramatic Impact

"Sextortion" is an emerging type of online sexual exploitation in which offenders coerce or blackmail victims into providing sexually explicit images or videos of themselves. These demands often come from the offender's threat to publicly post sexual images or to send them to the victim's friends and family.[35] Experts, calling sextortion a kind of "remote sexual assault," have noted that it is a vicious crime that causes severe psychological harm to victims.[36] Sextortion cases often involve victims and offenders who are in different, even faraway jurisdictions, and there are often multiple victims for each offender.

A sextortion case often begins with a computer hacker gaining access to a person's email account, which contains nude photographs of the victim. Using social engineering,[37] the hacker is able to gain access to the victim's social media accounts, including their contacts. The hacker then contacts the victim on several different platforms, demanding that the victim send additional sexually explicit photos or video. If the victim does not comply, the hacker threatens to send the content to all of the victim's friends on Facebook, or to the victim's family or employer. The victim sends the hacker the material according to his demand. The hacker then increases the requests until the victim is constantly bombarded with demands to make even more graphic material. This is a classic example of sextortion.

Researchers and activists say that sextortion has increased dramatically in recent years.

In 2016, the Brookings Institute released the first comprehensive study to attempt to quantify sextortion in the United States.[38] Researchers discovered 80 reported cases of sextortion through court documents and news articles. The cases involved what the researchers conservatively estimated to be 3,000 victims.[39] This figure may be severely underreported as well. For example, a survey of sextortion victims conducted in 2016 discovered that one in three victims never tells *anyone* (let alone the police) about the crime, due to embarrassment, shame, or self-blame.[40]

The true extent of sextortion is particularly difficult to quantify because of the lack of government data and the slow pace of legislation to prohibit it. Very few states have codified sextortion as a distinct crime,[41] leading many prosecutors to charge these cases under a wide variety of statutes. For example, if the victim is a minor, prosecutors can attempt to charge the case under child exploitation statutes.

>> continued on page 20

35. "The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress, April 2016." U.S. Department of Justice. Pp. 74-76. https://www.justice.gov/psc/file/842411/download.

36. Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera, "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault," The Brookings Institute (May 2016). https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.

37. Social engineering is a form of cyberattack that involves using human interaction or deception to get people to divulge personal information or access to a network. See SANS Institute, *Social Engineering: A Means to Violate a Computer System*. https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

38. Wittes, Poplin, Jurecic & Spera.

39. Ibid.

40. Janis Wolak & David Finkelhor. *Sextortion: Findings from a Survey of 1,631 Victims.* The Crimes Against Children Research Center, University of New Hampshire (June 2016). https://27l51l1qnwey246mkc1vzqg0-wpengine.netdna-ssl.com/wp-content/uploads/2016/08/Sextortion_Report.pdf.

41. See, e.g., "'Sextortion' Criminalized in Two States." *Courthouse News*, April 5, 2017. https://www.courthousenews.com/sextortion-criminalized-statute-two-states/.

Devastating impacts, including suicide risks: The impact on victims can be devastating. Researchers estimate that one in eight victims move out of their homes out of fear of further victimization.[42] An FBI analysis of 43 sextortion cases involving child victims found that "at least two victims committed suicide, and at least 10 more attempted suicide."[43] Sextortion disproportionately impacts women and minors. The Department of Justice reports that "sextortion cases tend to have more minor victims per offender than all other child sexual exploitation offenses."[44] Offenders have created online forums accessible on the dark web, to discuss tips and techniques to perpetrate these crimes.

continued from page 18

long-established street crimes. Together, these factors have created a rich environment for crime fueled by technology to grow.

"Online financial crimes are exploding right now, because there is a lot less risk for perpetrators. They do not have to be face-to-face with their victims, and they can commit crimes across jurisdictions, complicating matters for law enforcement."

— Captain Michael Ward, Montgomery County (MD) Police Department

New Ways to Commit Old Crimes

"Our criminal perpetrators have moved from committing traditional crimes with traditional methods to simply doing them through a different method."

— Prince George's County (MD) Sheriff Melvin High



Prince George's County, MD Sheriff Melvin High

In addition to committing new types of computer-related crimes, offenders are increasingly using technology to commit offenses that have been unlawful for many decades, including drug trafficking, motor vehicle theft, harassment, and crimes against children. "Nobody robs a bank with a note anymore," said Daniel Mahoney, Deputy Director of the Northern California Regional Intelligence Center. "There is a technological component to every crime."

Technology has always played a role in the crimes of theft and fraud. In the past, these schemes may have involved the telephone or U.S. mail. Offenders usually targeted one victim at a time, and the monetary gains were typically limited. Modern technology—the internet, email, social media, and computer hardware devices such as "skimmers" that criminals attach to ATM machines to steal victims' debit card information—have dramatically reshaped these crimes.

42. Wolak & Finkelhor.

43. "The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress, April 2016." U.S. Department of Justice. Page 76. https://www.justice.gov/psc/file/842411/download

44. Ibid., page 75.

Technology has made it easier for even modestly intelligent or competent criminals to target large numbers of victims and steal larger sums of money.



Roanoke County, VA Chief of Police Howard Hall

Credit card "skimmers": One example cited by participants at PERF's *Critical Issues* conference was the growing use of skimming devices to steal credit card and ATM card information from large numbers of unsuspecting victims. "We are seeing a great deal of credit card fraud through skimmers at gas pumps, ATMs, and grocery stores," said Roanoke County, VA Police Chief Howard Hall.

Skimmers are small, surreptitious card readers that are attached to credit or debit card payment devices and ATM machines. Without interfering with the functionality of the host machine, the skimmer captures data from the card's magnetic stripe every time customers use their cards. The thief later returns to the compromised machine to retrieve the device that now contains the stolen data. With that information in hand, the offender can create cloned cards to make purchases or withdrawals, sell the information to others, or open additional accounts in the victim's name.

Even as consumers and police become more alert at spotting skimmers, the technology continues to become more sophisticated. "New devices that are smaller and more difficult to detect—known as "shimmers" or "slimmers"—are also starting to pop up," said D.C. Metropolitan Police Sergeant Sylvan Altierri. "These are difficult cases, because the computer chips are encrypted and are hard to trace back to the suspect." Shimmers allow thieves to intercept the radio-frequency identification (RFID) information stored on the chips of modern credit, debit, and ATM cards, and then use Bluetooth technology to transmit the information wirelessly.

Harassment, stalking, and child exploitation: Technology—in particular, the internet—is also changing the crimes of harassment, stalking, and child exploitation. In the past, these offenses involved face-to-face contacts between the offender and the victim. Now, through social media apps, emails, and text messaging, offenders can make initial contact with their victims electronically, before engaging in in-person criminal behavior.

The U.S. Department of Justice noted this alarming trend in its National Child Exploitation Threat Assessment of 2016. It found that technology is contributing to three disturbing trends:

- **New and evolving threats.** New methods of child sex abuse continue to emerge in the online environment.
- **Evolving means of exploitation.** Mobile devices have fundamentally changed the way offenders can target and abuse children. Mobile apps, in particular, can be used to target, recruit, groom, and coerce children to engage in sexual activity.
- **Large number of victims, easily targeted.** Offenders are adept at tricking and/or coercing children who are online, and offenders typically target many children.[45]

45. Ibid., pages 9-10.

How Technology Is Changing Vehicle Thefts and Break-Ins

From 1997 to 2016, the motor vehicle theft rate in the United States decreased by 53 percent.[46] This dramatic decline has been attributed largely to the growing use and sophistication of anti-theft technology. For example, engine immobilizers, which prevent a car from starting unless the key needed to start the engine is recognized electronically by the vehicle's on-board computer, have become standard in most new vehicles sold over the last decade.[47]

Thwarting car-locking key fobs: As anti-theft measures have become more sophisticated, criminals have adopted new technologies to circumvent them. Some car burglars have begun using key fob jamming devices. As a victim walks away from his or her car and attempts to lock it with a key fob, the thief uses the jamming device to disrupt the signal, preventing the car from locking. After the owner walks away, the criminal can enter the car and steal any valuables that were left inside.[48]

Stealing vehicle registration cards, rather than radios: Technology is also changing what criminals are seeking when they break into vehicles. In the past, thieves targeted vehicles with items of high cash value, such as sound systems and GPS mapping devices. Today, many thieves are targeting items that can yield a greater, long-term return: vehicle registration and insurance cards. Personally identifiable information obtained from the documents can then be used to commit identity theft and fraud.

Frank Fernandez, Director of Public Safety for the City of Coral Gables, Florida, said that criminal organizations in south Florida are increasingly recruiting children to break into cars and obtain documents with identifying information. (The groups use juveniles because they are less likely to face serious consequences if they are caught.) The organizations then use the personal information to commit identity theft and related offenses. Director Fernandez said that often, criminals involved in these schemes target low-income neighborhoods, because their victims are less likely to be protected by subscription-based credit monitoring services.

The Dark Web: The New Marketplace for Criminal Activity

Perhaps the most significant technology that is facilitating criminal activity in the United States today is the so-called "dark web"—a largely hidden part of the internet that is encrypted, allowing users to remain anonymous and untraceable. The dark web has legitimate purposes, such as allowing journalists and political dissidents in repressive nations to communicate with each other and with the world, with less fear of exposure and reprisals. In recent years, however, the dark web has also emerged as a major platform for trafficking in drugs, weapons, sex workers, hacking tools, and even violent crime. The dark web is fundamentally changing how and where many of these types of crimes

46. "2016 Crime in the United States, Table 1." FBI Criminal Justice Information Services Division. https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/tables/table-1

47. "Technology making car theft obsolete." *Boston Globe,* September 8, 2014. https://www.bostonglobe.com/business/2014/09/07/how-tech-making-car-theft-obsolete/4qzCXHQHiQPvcjqewQWIZJ/story.html

48. "Could thieves use jamming technology to steal your car?" *The Guardian,* May 26, 2015. https://www.theguardian.com/technology/2015/may/26/high-tech-thieves-jamming-technology-steal-car

are committed, moving them from street corners to the internet and, often, the U.S. mail.

What does the dark web provide? Anonymity and ease of use. Several factors make the dark web an attractive platform for individuals engaged in criminal activities. First, with users' online identities effectively masked, the dark web is largely anonymous. It is also vast and multi-faceted, offering a variety of marketplaces for buying and selling an array of illegal goods. And, with a computer, an internet connection, and special (but readily available) browsing software, the dark net is easy to access and use. Some commentators have used the term "Amazon Effect" to describe the dark web, because individuals can make purchases online and have the product delivered directly to them, eliminating the need for in-person transactions.



Deputy Assistant Administrator Fred Smith, DEA Office of Investigative Technology

Online drug trafficking: Experts say the dark web is having a marked impact on illegal drug trafficking, with sales transitioning from street corners to dark markets. "Over the last five to 10 years, we have seen an increase of narcotics cases involving the dark web," said Fred Smith, Deputy Assistant Administrator of the DEA's Office of Investigative Technology. "Many drug dealers feel safer on the dark web, so they are using this approach more frequently."

While it is difficult to quantify the extent of illegal drug activity taking place on the dark web, a 2016 study by the RAND Corporation estimated that across eight major dark web marketplaces, revenue from illegal drug sales could be as high as $25 million per month.[49] Experts also note that while the dark web still accounts for a relatively small share of total drug sales, especially regarding cocaine and marijuana, it has emerged as a major source for sales of highly lethal synthetic opioids, such as fentanyl and U-47700.[50]

Online gun trafficking: Illegal gun sales on the dark web also have become a growing concern. While it is generally legal for individuals to buy guns online in the United States, the Bureau of Alcohol, Tobacco, Firearms, and Explosives has increased its focus on large-scale illegal gun-running operations, including many investigations that target customers in Europe and other parts of the world. Over the last two years, the ATF has dismantled dark web gun-running operations led by individuals using nothing more than a computer to start their illegal busineses.

In Manhattan, Kansas, for example, Michael Ryan used Tor software to conceal his identity as he shipped dozens of semi-automatic rifles, handguns, and hundreds of rounds of ammunition to customers around the world, under the name "Gunrunner," according to his plea agreement.[51] He was sentenced to more than four years in federal prison.

>> continued on page 25

49. Kruithoff, Kristy, et.al. RAND Corporation (2016). "Internet-facilitated drug trade: An analysis of the size, scope and the role of the Netherlands." https://www.rand.org/pubs/research_reports/RR1607.html.

50. "Opioid Dealers Embrace the Dark Web to Send Deadly Drugs by Mail." *The New York Times*, June 10, 2017. https://www.nytimes.com/2017/06/10/business/dealbook/opioid-dark-web-drug-overdose.html?_r=0.

51. "Inside the Illegal Online Weapons Trade." *CNN,* August 11, 2016. http://www.cnn.com/2016/08/10/us/declassified-illegal-online-weapons-trade/index.html.

The Surface Web, the Deep Web, and the Dark Web, Explained

The "surface web" is what most people are familiar with: Many people's interactions with the internet are limited to what is known as the "surface web," which is defined as all websites and web pages that are indexed and searchable by Google, Yahoo, and other search engines. This includes news media sites, social media such as Facebook and Twitter, online stores and business websites, government agencies and private-sector websites, special-interest websites and blogs, and other web pages that are publicly available. The indexed, searchable surface web consists of billions of pages,[52] but it is a relatively small portion of the entire internet, by some estimates less than 1 percent.[53]

The "deep web" includes private networks of organizations that may not be public: A much larger portion of the internet is called the "deep web," which includes large databases maintained by government agencies and private organizations, some of which are publicly available, either free or for a charge, and others of which are private to the organizations that operate them. Private networks operated by government and private organizations are also part of the deep web.[54]

The "dark web" is accessible only with software that masks users' identities: By contrast, the "dark web" is a layer of the World Wide Web that is not searchable, and is accessible only through special software that masks the user's Internet Protocol (or IP) address. An IP address is a numerical label assigned to each computer or other device connected to the internet. The IP address is a ready way to identify an internet-connected device, and often its user. The dark web has an interface to the surface web, allowing users to access websites and browse services, but the dark web interface effectively masks the user's identity.

To access the dark web, users need special software to mask their IP address and, therefore, their identity. A common method used to access the dark web is The Onion Router (or TOR) software. TOR conceals users' identities and online activity through multiple layers of encrypted connections. Most dark web activity is anonymized, making detection and identification challenging for law enforcement.[55]

The dark web is home to a number of "darknet markets," where individuals can buy and sell illicit goods and services, such as drugs, firearms, and professional hacking services. Transactions on these markets occur through the exchange of crypto-currencies, a form of digital currency. Although many variations of crypto-currencies exist, Bitcoin is the most popular.

Federal authorities, in conjunction with international partners, have aggressively targeted darknet markets in recent years. In 2013, federal agents seized Silk Road, an online marketplace for narcotics, murderers, and other illegal goods and services. Authorities arrested Ross Ulbricht, a 29-year-old American physicist, who owned and operated the site since 2011. Ulbricht was sentenced to life in prison without parole after being convicted of drug distribution and other charges. In its 30 months of operation, the FBI estimated that Silk Road generated $1.2 billion in sales.[56]

Following the takedown of Silk Road, two other sites, Alphabay and Hansa, emerged as large markets on the dark web. In the summer of 2017, however, an international investigation led by the FBI

52. "WorldWideWebsize.com." http://www.worldwidewebsize.com/

53. "Combatting Crime on The Dark Web: How Law Enforcement And Prosecutors Are Using Cutting-Edge Technology To Fight Cyber Crime." Prosecutors' Center for Excellence, December 2016. http://pceinc.org/wp-content/uploads/2016/01/20161219-Combatting-Crime-on-the-Dark-Web-How-Law-Enforcement-and-Prosecutors-are-Using-Cutting-Edge-Technology-to-Fight-Cyber-Crime-PCE-Altvater.pdf.

54. Ibid., pp. 1-3.

55. The Tor Project, Inc. "Overview." https://www.torproject.org/about/overview.html.en.

56. "Feds Seize 'Silk Road' Online Drug Site." *USA Today*, October 2, 2013. https://www.usatoday.com/story/news/nation/2013/10/02/fbi-shuts-down-silk-road-website/2909023/.

and Dutch authorities seized and shut down both Alphabay and Hansa. Servicing more than 200,000 users and 40,000 vendors, Alphabay had transactions exceeding $1 billion in digital currencies in its two years of operation. The site facilitated the exchange of stolen identities, hacking tools, and other illegal goods and services. The darknet market was also a major source of heroin and fentanyl and has been linked to multiple overdose deaths.[57]

Authorities acknowledge that even as major dark net markets such as Silk Road and AlphaBay are shut down, new ones tend to emerge quickly and fill the void.

continued from page 23

ATF recently created an Internet Investigations Center (IIC). Staffed by federal agents and intelligence and operations specialists, the IIC "conducts and coordinates multi-jurisdictional operations and provides investigative direction to disrupt and dismantle online criminal activity within the enforcement and regulatory jurisdiction of ATF."[58]

The dark web has also created a market for a broader range of individuals to engage in a variety of white-collar crimes. "The increase of dark marketplaces is enabling non-technical criminals to utilize online means to conduct fraud, whether through money laundering and usage of digital currency, or actually using malware," said Albert Murray, Assistant Section Chief of the FBI's Cyber Division.



Albert Murray, Assistant Section Chief, FBI Cyber Division

> "Considering the difference in purity, we are seizing more fentanyl in the mail than we are at the Southwest Border."
>
> **— Chief Customs and Border Protection Officer Stephen McConachie**

Just a few years ago, many of the illegal drugs entering the United States came across the Southwest border. Today, with the emergence of the dark web as a major trafficking portal, drugs—especially fentanyl and other synthetic opioids—are increasingly entering the country through the mail.

Traffickers are using the U.S. Postal Service (USPS) both to import drugs from overseas and to repackage and ship them domestically. For example, an individual from the United States can purchase fentanyl from China, advertise the product on the dark web, and redistribute the drug through parcels sent to domestic buyers. (For an example of how these types of distribution networks operate, see the sidebar on the "Peter the Great" case, page 48.)



Stephen McConachie, Chief Customs and Border Protection Officer

57. Federal Bureau of Investigation. "Darknet Takedown: Authorities Shutter Online Criminal Market AlphaBay." July 20, 2017. https://www.fbi.gov/news/stories/alphabay-takedown.

58. Fact Sheet – Internet Investigations Center. ATF, August 2016. https://www.atf.gov/resource-center/fact-sheet/fact-sheet-internet-investigations-center.

The Surface Web and Crime

The dark web is not the only online technology that is impacting crime. The so-called "surface web"—the part of the internet that is visible to everyday users—is also changing how some crimes are being committed. Experts at the *Critical Issues* conference discussed how social media, mobile apps, and other web-based systems are changing the nature of crime.

Social media like Facebook can help criminals find victims: As the popularity of social networking sites such as Facebook, Twitter, Instagram, and Snapchat has exploded over the past several years, criminals are turning to social media to identify and exploit victims.[59] For crimes such as prostitution and human trafficking, social media provides an extensive population of potential victims who can be easily identified through their personal profiles and the content about themselves that they share online (pictures, videos, friends, activities, locations where they can be found, and other personal information).

Again, the anonymity of the internet provides cover for offenders who, in the past, had to identify and solicit potential victims face-to-face. Instead, human traffickers and pimps are using sites such as Instagram, Kik, and Snapchat to recruit vulnerable social media users, who are often lured with the promise of a job or are fooled into believing they are in an online relationship.[60]

The Fayetteville, NC Police Department recently investigated a case in which a woman was using social media to recruit teenage girls to participate in prostitution. "We determined that three girls, ages 15, 16, and 17, were pimped out by a 21-year-old female who recruited them via Facebook and took them to other cities," said Analyst Rachael Songalewski. To lure customers, the woman took provocative pictures of the girls and posted them on the Backpage.com website in order to advertise them for prostitution.[61]

Mobile apps also can facilitate crime: Some criminals are using applications downloaded on smartphones and other mobile devices to lure victims to a variety of crimes, including robberies and assaults. For example, when the Pokémon Go app became popular in the summer of 2016, criminals exploited the game's geolocation features to lure unsuspecting players to secluded areas, whether they were robbed and assaulted. Several dozen of these crimes were reported.[62]

---

59. "Criminal Use of Social Media (2011)." National White Collar Crime Center. https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Criminal percent20Use percent20of percent20Social percent20Media.pdf.

60. "How traffickers use social media to lure vulnerable teenagers into sex work." *VentureBeat*, November 15, 2015. https://venturebeat.com/2015/11/15/how-traffickers-use-social-media-to-lure-vulnerable-teenagers-into-sex-work/.

61. Backpage is an online classified advertising site that has listings for a wide variety of consumer goods and services. Following complaints that the site was being used to support prostitution and human trafficking, Backpage took down its "adult services" section in early 2017, but some allege that the site still facilitates prostitution. See "Backpage's Sex Ads Are Gone. Child Trafficking? Hardly." *The New York Times*, March 11, 2017. https://www.nytimes.com/2017/03/11/us/backpage-ads-sex-trafficking.html.

62. "Pokemon Go dangerous? Every crime, accident, death linked to game so far." *Syracuse.com*, July 26, 2016. http://www.syracuse.com/us-news/index.ssf/2016/07/pokemon_go_dangerous_every_crime_accident_death_shooting_linked_to_game.html.

Justin Larson Case Study: How a 30-Year-Old Computer Scientist Used Encrypted Communications to Distribute Drugs

In June 2017, a U.S. district judge in Maryland sentenced Justin Larson to life in prison for distributing acetyl fentanyl, resulting in death.[63] Larson hardly fit the profile of an international narcotics distributor. The 30-year-old Gaithersburg, Maryland man held a computer science degree from the University of Maryland. "The defendant was highly intelligent and had conducted extensive internet research to learn his trade craft, to study the classification of drugs, and to learn the techniques of other criminals distributing drugs through the internet," said Sergeant Michael Yu of the Montgomery County, Maryland Police Department's Electronic Crimes Unit.

Investigators first came into contact with Larson over a domestic call, and received a tip about his alleged drug activity. An FBI task force that included the Montgomery County Police Department and Immigration and Customs Enforcement/Homeland Security Investigations pursued the case for almost three years before making an arrest. An important part of the investigation was uncovering how Larson communicated with his supplier.

That supplier was a fentanyl dealer in China, with whom Larson connected over the dark web. All communications between Larson and his supplier went through multiple layers of encryption. Larson would type out all messages in an encrypted platform that would generate a self-destructing link and then send the link through an encrypted web-based email. When the supplier or Larson read messages from each other, they were destroyed forever. In order to unravel these communications, investigators had to perform detailed forensic digital examinations on Larson's mobile devices and work with web-based email providers to find people connected to Larson.

Larson's case demonstrates how the internet has fueled changes in drug trafficking and how suppliers and distributors communicate. "Traditionally, people needed a large network for that kind of drug trafficking operation," Sergeant Yu said. "But in this case, the defendant was simply importing fentanyl from overseas using encrypted communications. Nowadays with technology, you don't need a gang or a special connection to get involved in drug trafficking. You can just do it from your computer."

Criminals are also using ads on app-based platforms to find victims. Offenders post fake advertisements on the sites, or respond to legitimate ads, then set up meetings with victims. During a homicide investigation, the DeKalb County, Georgia Police Department discovered that a group was posting fake ads on the app, OfferUp. "The suspects were luring people in and robbing them," said Lieutenant Timothy Donahue. "In one case, they murdered the person." Similarly, the Suffolk County, NY Police Department arrested a man who allegedly responded to ads on the app, Letgo, and robbed sellers on three separate occasions.[64]

63. "Montgomery County Man Sentenced To Life In Federal Prison For Distributing Acetyl Fentanyl Resulting In Death." U.S. Attorney's Office for the District of Maryland, June 30, 2017. https://www.justice.gov/usao-md/pr/montgomery-county-man-sentenced-life-federal-prison-distributing-acetyl-fentanyl

64. "Letgo app used by Myandanch man to rob sellers, police say." Newsday, May 31, 2016. http://www.newsday.com/long-island/crime/letgo-app-used-by-wyandanch-man-to-rob-sellers-police-say-1.11858674.

Police also are seeing criminals increasingly use dating apps to arrange meeting with victims. In Dallas, at least seven men have been arrested for committing sexual assaults against victims they found through dating apps or social media.[65] In Daytona Beach, Florida, an 18-year-old woman received a 20-year prison sentence for using the app, Meet Me, to set up a robbery that ended with a victim being shot.[66]

Encrypted messaging thwarts investigations: Email and other messaging platforms allow users to communicate with each another across the country and around the globe. Criminal offenders are turning to encrypted communications services to discuss their illegal activities. "We have investigations where we have wiretaps to listen to phone calls, and as soon as we're about to hear important details, the conversation moves to an encrypted messaging service," said Camden County, NJ Deputy Police Chief Joseph Wysocki. (For more information on encryption, see pp. 36–43.)



Chicago Deputy Police Chief Steve Caluris

How Technology Is Changing Gang Activity

> "Street gangs thrive off anonymity, so the dark web provides a very lucrative environment for them to operate."
>
> **— Deputy Chief Steve Caluris, Chicago Police Department**

In cities across the country, criminal activity among street gangs is evolving. Several participants at the *Critical Issues* meeting noted that gangs in their jurisdictions are moving away from street crimes and are engaging in more sophisticated criminal enterprises that include fraud, identity theft, and other computer-enabled crimes. These crimes are often less dangerous, have lower criminal penalties, and can be more profitable than crimes such as street-level drug dealing.

This shift does not mean that gangs are abandoning intimidation and violence against rivals. But some gangs are searching for a steadier, more reliable source of funding for their ongoing operations.



NYPD Chief of Detectives Robert Boyce

Gangs Are Committing Financial Fraud

> "We used to say, 'If there's drugs, there's guns.' Now, wherever there's *money*, you'll find guns."
>
> **— Chief of Detectives Robert Boyce, New York City Police Department**

Historically, most young gang members got their start in the low-level drug trade. Recently, however, police report seeing more gang members, especially

65. "Rapists increasingly using dating apps, social media to lure victims, Dallas police warn." *Dallas Morning News,* February 2, 2016. https://www.dallasnews.com/news/crime/2016/02/01/rapists-increasingly-using-dating-apps-social-media-to-lure-victims-dallas-police-warn.

66. "Central Florida woman gets 20 years in dating app shooting." Orlando.com, June 28, 2017. https://www.clickorlando.com/news/central-florida-woman-gets-20-years-in-dating-app-shooting.

How a Brooklyn Street Gang Stole $1.5 Million Through a Fraudulent Money Order Scheme

In July 2015, federal authorities in New York City indicted 12 members of the Van Dyke Money Gang (VDMG) on charges of bank fraud and aggravated identity theft. Banks along the East Coast had lost more than $1.5 million as a result of the gang's elaborate money order scheme.[67]

The gang members, who ranged in age from 20 to 30 and who pleaded guilty, fraudulently obtained blank Postal Money Orders and Western Union Money Orders. Members of VDMG printed relatively small dollar amounts, typically under $1,000, on the money orders. The men recruited bank account holders to deposit the fraudulent money orders into their accounts. The account holders then withdrew money from the accounts and turned it over to VDMG members. The scheme involved over 350 accounts from banks in New York, Massachusetts, and Washington, D.C.

The scheme was uncovered and indictments returned following a multi-agency investigation that included Immigration and Customs Enforcement/Homeland Security Investigations, the United States Secret Service, the U.S. Postal Inspection Service, and the New York City Police Department. In announcing the indictments, U.S. Attorney Preet Bharara said: "Today's allegations suggest that members of street gangs, like the Van Dyke Money Gang, have expanded their criminal repertoire to include white collar crimes like bank fraud and identity theft."

young ones, getting involved in a variety of financial schemes. NYPD Deputy Chief Michael Baldassano noted, "We're seeing less sophisticated gangs and crews move away from drug sales and use the dark web to get involved in grand larceny."

One common fraud involves gang members obtaining credit card information from darknet markets and using the proceeds to facilitate other, sometimes violent crimes. "Individuals can purchase a credit card number for $20 on the dark web, put it on to a counterfeit credit card, create a fake ID, and recruit people to go shopping for them," said NYPD Deputy Inspector Christopher Flanagan. In some cases, the fraudulent credit cards are used to rent vehicles to be used in drive-by shootings or other crimes.

Check fraud is another financial scheme increasingly employed by street gangs. Gang members steal checks or money orders or create counterfeits. Then they recruit individuals, often college students or transients, and pay them to open a legitimate bank account. The account holder deposits the fraudulent checks into the account and quickly makes cash withdrawals. "Over a weekend, gangs will set up a person's account, put bad checks in, and start withdrawing the money. The banks do not catch the activity until Monday or Tuesday, and then these people go to the next person," Philadelphia Police Captain Roland Lee explained. In some cases, these criminal organizations relocate to another jurisdiction when local police begin to figure out their scheme.



NYPD Deputy Chief Michael Baldassano



Philadelphia Police Captain Roland Lee, Jr.

67. "Twelve Members and Associates of Brooklyn Gang Indicted for Committing Bank Fraud Involving More Than 350 Bank Accounts and More Than $1.5 Million in Loss." U.S. Attorney's Office for the Southern District of New York, July 14, 2015. https://www.justice.gov/usao-sdny/pr/twelve-members-and-associates-brooklyn-gang-indicted-committing-bank-fraud-involving

Gangs are becoming far more sophisticated about developing expertise: Enticed by the large financial returns from financial crimes, gangs are recruiting educated and financially sophisticated individuals into their ranks to help commit offenses such as mortgage fraud, tax fraud, and other intricate schemes. "Street gangs are financially supporting their members in obtaining law degrees and other specialized education," said Deputy Chief Steve Caluris of the Chicago Police Department. He added that gangs are willing to make these investments because financial crimes yield high returns.

Gang members are also using the internet to recruit and train others on how to commit various fraud offenses. Experts note that this type of recruitment, investment, and training is an indicator of some gangs' commitment to a more sophisticated, long-term focus for financing their operations.



NYPD Deputy Inspector Christopher Flanagan

Identity Theft Can Be a Short-Term Tactic

Some gangs are also relying on short-term schemes, such as identity theft, to fund their operations. These tend to be less sophisticated and produce a more immediate return. In some cases, gangs form specifically for the purpose of committing financial crimes such as identity theft.

For example, in November 2017, the U.S. Attorney's Office for the District of Maryland announced guilty pleas and sentencing of members of a nationwide group called the Felony Lane Gang. "These individuals traveled from Florida to Maryland and other states, broke into vehicles parked at recreation areas, sports fields, gyms, fitness centers, and other locations, and stole wallets, purses and other items left in the vehicles," the U.S. Attorney's Office said in a media release. "The defendants then used the victims' stolen checks, credit cards and identifications to conduct fraudulent financial transactions. Traveling groups generally consisted of two to four managers and one to six 'faces' (sometimes called 'sliders' or 'workers') or persons who passed the fraudulent and stolen checks. They traveled in rental cars and stayed in hotels, sometimes using victims' identities and credit cards…. Over the course of the scheme, the defendants fraudulently obtained and attempted to obtain over $1 million from more than a dozen financial institutions, using the identification of hundreds of individual victims."[68]

Gangs Are Becoming More Subtle about Money Laundering

Gangs have long relied on money laundering to hide the illegal profits from drug trafficking and other crimes. Recently, gangs are becoming more sophisticated in creating elaborate money laundering operations to conceal their criminal activity. Quovella Spruill, Chief of Detectives for the Essex County, NJ, Prosecutor's Office, explained, "Gangs have to hide their money. They are

68. "Member of the 'Felony Lane Gang' Sentenced in $1 Million Bank Fraud Conspiracy." U.S. Attorney's Office for the District of Maryland, Nov. 3, 2017. https://www.justice.gov/usao-md/pr/member-felony-lane-gang-sentenced-1-million-bank-fraud-conspiracy

now smart enough to know not to buy flashy cars. Instead, they are trying to start businesses and buy property to make the money look legitimate."

Experts note that some gangs are developing fake businesses, or shell companies, through which illegally obtained money is routed. Jeff Lybarger, Director of the National White Collar Crime Center, cited a recent case in New Jersey in which gang members bought several car-wash businesses to launder money. Although this was not part of the initial investigation by police, investigators made the discovery when they subpoenaed financial records from the car washes.



Jeff Lybarger, Director of Training, National White Collar Crime Center

Gangs Are Hiring Contract Workers

Experts also note that gangs and other criminal organizations are increasingly modeling their operations on those of legitimate businesses. One example cited by participants at the *Critical Issues* meeting was the use of "contract workers." Some gangs are now contracting out some of their criminal activities to non-gang members, many of whom have only a loose affiliation with the gang.

"Recently, we were collaborating on a case with several FBI task forces," said Los Angeles Police Department Captain Charles Hearn. "While they were on site, several cars belonging to FBI investigators were broken into. The suspects took body armor, radios, and personal information from the investigators. We solved the case, and we arrested the suspects. We discovered that these were just two or three ladies—young women with kids, living in an apartment complex—who were loosely associated with the gang. They were sent to break into the cars, get the information, and create dossiers of the investigators, all in furtherance of the gang. It's not the actual gang members themselves."



Los Angeles Police Capt. Charles Hearn

Gangs often target transients and young females for these types of assignments. If they are arrested and prosecuted, these contract workers are likely to face lower criminal penalties than the gang members themselves, who often have a criminal history. In addition, these arrangements can serve to distance the gang from the crimes, and reduce the likelihood that they will be caught.

Gangs remain violent: Experts note that although technology has driven many gangs to diversify their criminal repertoires, gang members remain engaged in violence, narcotics offenses, and other street crimes, just as they have done for decades. In many cases, the computer-related crimes are a means to raise money to purchase weapons, vehicles, and other items used in violent crimes.

> "People who were involved in traditional crimes and are now transitioning into fraud-related crimes still have their old ways of violence in them. We find credit card mills, and we'll find guns too. Gangs can transition into different crimes, but there will still be violence. There's always a gun."
>
> **— NYPD Deputy Chief Joseph Dowling**
> **Commanding Officer, Grand Larceny Division**



NYPD Deputy Chief Joseph Dowling

Why Is the Shift in Gang Activity Occurring?

> "Why would gang members stand on the corner and sell drugs when they can make thousands of dollars every month with a credit card factory? Gangs can make proceeds just as high as they did with the narcotics trade, but they know they won't receive a lengthy prison sentence or get shot. So why not commit identity theft and rake in a couple thousand dollars?"
>
> **— Chicago Police Detective Patricia Dalton**

Less danger, higher profits, lower penalties: Why are gangs becoming increasingly engaged in fraud, identity theft, money laundering, and other financial crimes? Participants at the *Critical Issues* meeting gave three primary reasons: White-collar crimes are (1) less dangerous; (2) they often yield higher profits, and (3) they typically carry lower criminal penalties than street crimes. Although statutes for financial crimes vary from state to state, participants at PERF's conference agreed that relatively lax criminal penalties for most computer-related crimes make them an attractive alternative to many drug and violent offenses, which carry substantial penalties.

For example, penalties for grand larceny often mandate only probation for an offender with no prior criminal history. Criminals charged with financial crimes often face no jail time and are mandated only to pay restitution. Most violent crimes and narcotics violations, on the other hand, carry much harsher sentences. "Depending on the amount of drugs involved, the offender will do 15 years," said NYPD Deputy Chief Joseph Dowling.

Several participants at the *Critical Issues* meeting noted that laws and penalties for white-collar crimes have not kept pace with the changing nature of crime and criminal activity, especially as it relates to gang involvement in these crimes. "At a minimum, criminal statutes for computer-enabled crimes are 5 to 10 years behind technology," said Gainesville, Florida Police Captain Anthony Ferrara.



Gainesville, FL Police Captain Anthony Ferrara

Captain Ferrara described a recent series of fraud cases his agency investigated in which victims were sent a letter on IRS letterhead instructing them to send money in order to release their tax refund. *Even though the offenders were posing as federal tax officials, the offense did not carry an enhanced penalty.* "Extorting money by posing as a government agent carries no enhancements," Ferrara explained. "It is just under the heading of fraud."

Others meeting participants said that judges and other criminal justice officials should be educated about how gang crime is changing, and how it is impacting victims and larger communities. In grand larceny cases, for example, judges appear reluctant to impose tough sentences for first-time offenders, despite the immense impact that financial crimes can cause to victims.

"Judges need to be educated on how gangs are moving into these types of crimes, and they must work with the legislature to increase penalties," said NYPD Deputy Chief Dowling. "The penalties for these crimes do not measure up to the impact on the victims' lives."

The New Crime Environment Presents New Investigatory Challenges for Police

THE CHANGING NATURE OF CRIME IN THE UNITED STATES HAS CREATED a challenging environment for police investigators. They are facing not only an increase in the number of cyber-crimes that are being committed, but also the emergence of entirely new types of computer-related offenses.

Police are also seeing the expanded use of technology to commit many street crimes. The dark web, in particular, has emerged as a vast and largely anonymous marketplace for trafficking in drugs, guns, prostitution, and more. Technology has opened up crimes such as drug trafficking to a wide range of new criminals, many of whom have little experience and are unaffiliated with gangs or other criminal organizations. Technology is also impacting how some street gangs operate; they are becoming more sophisticated and tech-savvy, even as they remain engaged in violence.

Police agencies are facing a number of operational challenges when it comes to investigating new types of crime and new types of criminals. Effectively managing digital evidence and dealing with issues such as encryption are two issues of critical importance in this environment.

The Growing Importance of Digital Evidence

> "Digital evidence is everywhere. It's not just computer cases, it's all cases."
>
> **— Sean Goodison, Deputy Director, PERF Center for Applied Research**

> "A smartphone, a laptop, an e-reader, a Fitbit — where data is stored, digital evidence is stored."
>
> **— Commander Richard Perez, Fairfax County (VA) Police Department**



Commander Richard Perez, Fairfax County, VA Police Department

Nearly every type of crime today has a digital component. Searching the smartphone of a suspect, or a crime victim, can yield text messages, emails, photos, videos, social media postings, names of persons recently contacted, and

internet searches that the suspect or victim made, such as a Google map search for directions to an address, all of which can be important digital evidence.

And smartphones are by no means the only source of digital evidence. Investigators today are encountering a wide array of digital data captured by a variety of devices—laptops and tablets, GPS systems, Fitbits and other wearable technologies, closed-circuit television, and the growing body of "Internet of Things" devices.

According to the National Forensic Science Technology Center, digital evidence has four defining characteristics:

- Digital evidence is latent, or "hidden," like fingerprints or DNA;
- It can cross jurisdictional borders quickly and easily;
- It can be altered, damaged, or destroyed with little effort;
- It can be time-sensitive.

Police use digital evidence much as they use traditional physical evidence—to connect people, places, and events in order to establish causality for crimes. Unlike traditional physical records, however, digital evidence is wider in scope, it may encompass more personally sensitive information, and is often more difficult to obtain.[69] These characteristics of digital evidence present many challenges for police in modern criminal investigations.

Volume of data is exploding: Compounding those challenges is the sheer volume of data that is being generated today, and how data creation will continue to accelerate in the future. By 2020, the number of internet-connected devices is expected to reach an average of 4.3 per person, or roughly 33 billion devices worldwide.[70] Individuals are using those devices to create vastly more data than ever before, much of it "life-critical" data necessary for the smooth functioning of modern daily life. These trends are expected to accelerate in the future, with an expected 10-fold increase in the amount of data worldwide by 2025.[71]

For police investigators, the volume and breadth of data has important implications, now and especially in the future. More devices mean more data, and more potential digital evidence for investigators to uncover and use. But these trends also mean greater challenges for investigators in accessing and analyzing the growing body of potential evidence, and distinguishing the "signal" from the "noise."

>> continued on page 36

69. Goodison, S., Davis, R., & Jackson, B. (2015). *Digital Evidence and the U.S. Criminal Justice System*. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

70. "33 Billion Internet Devices by 2020: Four Connected Devices for Every Person in World." *Strategy Analytics.* https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer&a0=5609.

71. Reinsel, David, et.al. "Data Age 2025: The Evolution of Data to Life-Critical." April 2017. International Data Corporation. https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

The Vanderbilt Rape Case: The Role of Digital Evidence in a High-Profile Investigation

Criminal investigators are increasingly turning to information from digital devices to connect people, places, and events, just as they do in traditional criminal investigations that rely on witness statements and physical evidence.

The investigation of a high-profile sexual assault case on the campus of Vanderbilt University illustrates how critical digital evidence can be in cases where physical evidence is not readily available. Officials with the Metropolitan Nashville Police Department described the investigation during the *Critical Issues* meeting.

Cell phone messages and photos were at the heart of the case: On June 23, 2013, a 21-year-old female student was raped while she was unconscious, in a residence hall on the Vanderbilt campus. Eventually, hallway surveillance camera footage was discovered that showed four university football players carrying the woman into a dorm room, where multiple sexual assaults occurred. The men took pictures and videos of the incident, sending them to at least one other player. Several text messages were also exchanged, discussing a plan to delete the evidence and cover up the rape.[72]

The investigation began with an unrelated crime: a damaged door in one of the university's freshman residence halls. Administrative personnel reviewed surveillance camera footage with hopes of discovering who caused the damage. While reviewing the video, administrators saw footage of an unconscious woman being taken into a room and later carried out, undressed and abandoned in the hallway.

Administrative personnel notified the police of their discovery, and the Metropolitan Nashville Police Department (MNPD) immediately initiated an investigation, but as Chief Steve Anderson recalled, "By that time, any physical evidence was gone." The victim was unconscious during the encounter and was unaware of what had occurred. Although police believed the victim had been given a date-rape drug, too much time had elapsed for that to be proved. With limited physical evidence, investigators would need to rely on digital evidence to solve the case.



Metropolitan Nashville Police Captain Jason Reinbold

Using the surveillance video, detectives were able to begin identifying persons of interest, who were brought in for questioning. During an interview, one of them admitted to taking pictures during the incident, but said the photos had been deleted. When investigators conducted a forensic analysis of the suspect's cell phone, they confirmed that the pictures, as well as text messages during that time, had been deleted. However, investigators were able to uncover remnants of seven text messages that were clearly related to the rape. "The language was atrocious, and it was during the same time frame in which the woman was in that room," MNPD Captain Jason Reinbold said.

Investigators knew that text messages existed, but they did not know to whom they had been sent. "So we looked at the call log, and determined who the suspect had spoken with during the same time frame of the rape," Reinbold explained. It was discovered that that calls were made to two friends of the suspect, who lived in Riverside, California.

During the investigation, police discovered that the suspect had flown to California to retrieve and

>> continued on page 36

72. Vanderbilt Rape Case: Timeline of Key Events. June 15, 2017. *The Tennessean*. http://www.tennessean.com/story/news/crime/2015/06/23/vanderbilt-rape-case-timeline-of-investigation-and-case/29183041/.

destroy a cell phone belonging to one of the friends. The suspect purchased the friend a new phone and threw the old phone into a river in an attempt to destroy evidence of the rape.

Messages were inadvertently stored on the cloud: An MNPD detective traveled to Riverside and worked with local police to execute four search warrants for digital devices belonging to the suspect's friends. Police recovered a laptop from the friend for whom the suspect had purchased a new phone. Unbeknownst to the owner, the laptop contained iMessages that were linked to his iCloud account. Although the messages from the suspect were not accessible through the destroyed phone, investigators were able to retrieve them from the laptop. "We were able to acquire all of the video and messages about the rape that the suspect at Vanderbilt University had sent to his friends in Riverside County, California," Captain Reinbold explained. In all, police were able to recover from the laptop 40 pictures and three videos that captured the incident.

Digital evidence played a critical role in the prosecution of the Vanderbilt rape case. Juries have found three of the four defendants guilty on charges of aggravated rape and aggravated sexual battery. Each has been sentenced to 15 years or more in prison. A fourth suspect is awaiting trial.[73]

continued from page 34

Encryption and Going Dark

> "Most digital evidence will be encrypted a decade from now. So we need to think about how we will retrieve it, where we will store it, and how we'll analyze it."
>
> **— Major Frederick Fife, New Jersey State Police**



New Jersey State Police Major Frederick Fife

The basic process for obtaining digital evidence is much like the process for gathering physical evidence. In general, police must first obtain a search warrant or subpoena to lawfully seize digital evidence.

However, the development of new technologies and network security protocols has made it increasingly difficult for police to gain access to digital evidence, even when executing judicially approved orders.[74] Many digital devices use encryption methods to prevent unauthorized access to the digital data stored on the device. Unlocking these devices is becoming more difficult for criminal investigators. The phrase "going dark" refers to the inability of police to access digital evidence due to encryption.

Historically, law enforcement agencies have been able to access most digital data through legal processes with the assistance of telecommunications companies. Today, however, new encryption technology often restricts data access

73. "Brandon Banks sentenced to 15 years in prison in Vanderbilt rape case." *The Tennessean,* August 17, 2017. http://www.tennessean.com/story/news/2017/08/17/brandon-banks-faces-friday-sentencing-vanderbilt-rape-case/565194001/

74. "Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence." IACP, 2016. Pp. 14-15. http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf.

What Is Encryption?

Encryption is a method of protecting digital information as it is stored on a device or transmitted across the internet or other computer networks. When data is encrypted, it is converted to another form or code to prohibit unauthorized access. A decryption key, such as a password or numeric passcode, must be submitted to retrieve the protected information.[75]

There are many legitimate and necessary uses for encryption. For example, encryption is vital for protecting online commerce and safeguarding government records, and it is a vital tool for preventing many types of online crimes. Some criminal offenders, however, are using encryption methods to prevent police from accessing incriminating digital evidence. For instance, perpetrators are increasingly using encryption software on devices storing images of child pornography.

No way to give police "backdoor access"? Officials at the FBI and other agencies have advocated giving police "backdoor access" (i.e., a special decryption key) to encrypted data stored on the devices of criminal suspects. Many tech companies and privacy advocates, however, argue that a method for backdoor access could be exploited and compromise users' privacy.

For example, Apple Inc. CEO Tim Cook, in a letter to Apple customers, said,

> Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation [of the 2015 San Bernardino mass shooting incident]. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession.... Building a version of [an Apple product operating system] that bypasses security in this way would undeniably create a backdoor. And while the government may argue that its use would be limited to [the San Bernardino] case, there is no way to guarantee such control.[76]

solely to the user. Even with the assistance of service providers and a court order, police may not be able to access encrypted data.[77]

In 2014, Apple announced that it could no longer extract data from devices running on iOS 8 and later versions. "For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction, as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key. All iPhone 6 and later device models are manufactured running iOS 8.0 or a later version of iOS," the company has said.[78]

Shortly after Apple's announcement, other companies followed suit. Google revealed that its Android devices would be protected by default encryption similar to the iPhone. (Together, iOS and Android operating systems account for

75. "What Is Data Encryption?" *Digital Guardian,* Dec. 7, 2017. https://digitalguardian.com/blog/what-data-encryption.

76. "A Message to Our Customers." Tim Cook, February 16, 2016. https://www.apple.com/customer-letter/

77. "Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence." IACP, 2016. Page 2. http://www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf.

78. *Legal Process Guidelines: Government & Law Enforcement within the United States.* Apple Inc. See Section I, "Extracting Data from Passcode Locked iOS Devices." https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

more than 99 percent of all new smartphones worldwide.) Similarly, Facebook has announced that the company's Messenger service, with approximately 900 million users, would include an opt-in feature permitting users to encrypt their messages. Encrypted data is a built-in feature of several popular messaging services, including WhatsApp, which has more than 1 billion users.

Gangs are using encryption: The move toward greater encryption of mobile devices and messaging services has created new opportunities for online criminals, and new challenges for law enforcement investigators. Participants at the *Critical Issues* meeting reported that some criminals are using encrypted services. "We've seen a big change in the sophistication of gangs. They are communicating through encrypted messaging apps like Skype, WhatsApp, and Instagram to conceal their illicit activity," said New Jersey State Police Major Frederick Fife, who is assigned to the New Jersey Regional Operations Intelligence Center. Minneapolis Police Lieutenant Jeff Rugel added, "A lot of criminal activity is taking place on SnapChat, and we never see most of it because of the nature of the app."



Minneapolis Police Lt. Jeff Rugel

The new reality is that investigators need to presume that much of the digital evidence they seek from mobile devices and online apps will be encrypted.

The number of lawfully seized devices across the country that remain inaccessible due to encryption is unknown. However, a number of major agencies have reported on backlogs in their jurisdictions. The FBI estimates that during the 11-month period from October 2016 through August 2017, it could not access the contents of more than 6,900 mobile devices connected with criminal investigations because of encryption. "To put it mildly, this is a huge, huge problem," FBI Director Christopher Wray said. "It impacts investigations across the board—narcotics, human trafficking, counterterrorism, counterintelligence, gangs, organized crime, child exploitation."[79]

In New York City, the Manhattan District Attorney's Office publishes an annual "Smartphone Encryption and Public Safety" report. The latest report shows that since 2014, the prosecutor's office had recovered and obtained court-ordered warrants or consent to search 3,882 devices running Apple or Android operating systems.[80] More than half, 2,147, were locked using encryption. During the first 10 months of 2017, more than 700 of the nearly 1,300 devices recovered were encrypted.

Smartphone Encryption Statistics
October 1, 2014 – October 31, 2017

	2014	2015	2016	2017	Grand Total
iOS					
Unlocked	40	145	171	199	555
Locked	59	382	538	466	1,445
iOS Total	**99**	**527**	**709**	**665**	**2,000**
ANDROID					
Unlocked	103	324	371	382	1,180
Locked	19	188	259	236	702
ANDROID Total	**122**	**512**	**630**	**618**	**1,882**
Grand Total	**221**	**1,039**	**1,339**	**1,283**	**3,882**

Source: Manhattan District Attorney's Office.

79. "FBI couldn't access nearly 7K devices because of encryption." Associated Press, Oct. 22, 2017. https://apnews.com/04791dfbe30a4d3596e8d187b16d837e.

80. "Smartphone Encryption and Public Safety." Manhattan District Attorney's Office, November 2017. http://manhattanda.org/sites/default/files/2017 percent20Report percent20of percent20the percent20Manhattan percent20District percent20Attorney percent27s percent20Office percent20on percent20Smartphone percent20Encryption_0.pdf.

Similarly, police officials in Los Angeles reported more than 300 encrypted devices associated with criminal investigations that were unable to be searched.

Addressing the Challenges of "Going Dark"

> "We have an enormous problem with encryption. About 97 percent of the market of new phones, and about 40 percent of the phones we have as evidence, are encrypted. Our labs are filled with phones related to homicides and shootings that can't be accessed because we don't have the passwords. We are hoping that, on a national level, this can be legislated to help us get into these devices."
>
> **— Colonel Joseph Fuentes, New Jersey State Police**



New Jersey State Police Colonel Joseph Fuentes

Participants at the *Critical Issues* meeting discussed a number of strategies for addressing the "going dark" issue, detailed below:

In Rare Cases, Contracting with Technical Experts

Frustrated by tech companies' inability or unwillingness to grant access to contents of criminal suspects' devices, some law enforcement agencies have begun to contract with private technical experts to help unlock those devices. The most famous instance of this followed the December 2015 mass shooting in San Bernardino, California. Syed Rizwan Farook and his wife, Tashfeen Malik, opened fire at a holiday party where Farook had worked, killing 14 people and injuring 22.

Because the shooting involved domestic terrorism, the FBI moved to access data stored on Farook's iPhone in the hopes of identifying any accomplices, determining motives, and uncovering any plans for other attacks. However, their efforts were thwarted because of the default encryption on the device. The FBI sued Apple to unlock the phone, but eventually dropped the suit after the

The National Domestic Communications Assistance Center

The U.S. Justice Department's National Domestic Communications Assistance Center (NDCAC) serves as a hub for technical knowledge management and information-sharing among law enforcement agencies.[81] NDCAC seeks to collect data to quantify the impact of "going dark."

Through an online portal, law enforcement agencies can submit information on the number of impenetrable devices they encounter and share examples of investigations that have been curtailed by encryption. As more agencies provide information, NDCAC will develop a deeper understanding of the scope and impact of encryption, and share its findings with law enforcement agencies.

81. National Domestic Communications Assistance Center. "A hub for technical knowledge management." https://ndcac.fbi.gov/.

Bureau paid an undisclosed vendor more than $1 million to unlock the gunman's device.

Although contracting with outside vendors has been used in cases such as the San Bernardino mass shooting, experience suggests it may not be a sustainable method to access encrypted data for several reasons:[82]

- **Cost:** It is cost-prohibitive for most police agencies, especially smaller departments.
- **Time:** It takes too much time, often weeks or months. In cases such as a missing person or a possible terrorist threat, waiting for encrypted data is problematic.
- **Ad-hoc nature:** "Hacking" methods are not always replicable across models or operating systems, so there is seldom a quick fix.
- **Solutions are short-lived:** Methods for hacking have a short shelf-life, as manufacturers are constantly looking to identify and correct identified security flaws.
- **Admissibility questions:** Evidence recovered through hacking may be difficult to introduce at trial.

In June 2017, the Department of Justice requested $21.6 million in federal funding to address the issue of encryption. With the funding, the FBI intends to develop in-house expertise and acquire tools for analyzing encrypted electronic devices. In testimony to a Senate Appropriations subcommittee, Deputy Attorney General Rod Rosenstein stated, "The seriousness of this threat cannot be overstated…. This phenomenon is severely impairing our ability to conduct investigations and bring criminals to justice."[83]

Working with Tech Companies

> "We are not trying to circumvent formal legal procedures to go after individual privacy. What we are trying to do is conduct criminal investigations based on proper legal process, approved by an independent judge."
>
> **— Minnesota Bureau of Criminal Apprehension Superintendent Drew Evans**



Superintendent Drew Evans, Minnesota Bureau of Criminal Apprehension

Another avenue for addressing encryption is for law enforcement agencies to work directly with the technology sector. Participants at the *Critical Issues*

82. "Smartphone Encryption and Public Safety." Manhattan District Attorney's Office, November 2017. Pp. 8-10. http://manhattanda.org/sites/default/files/2017 percent20Report percent20of percent20the percent20Manhattan percent20District percent20Attorney percent27s percent20Office percent20on percent20Smartphone percent20Encryption_0.pdf

83. "Deputy Attorney General Rod J. Rosenstein Testifies Before the U.S. House of Representatives and U.S. Senate Appropriations Subcommittees on Commerce, Justice, Science and Related Agencies." U.S. Department of Justice, June 13, 2017. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-testifies-us-house-representatives-and-us-senate

Resources for Obtaining Data from ISPs

SEARCH, the National Consortium for Justice Information and Statistics, offers several resources to criminal justice partners for obtaining data from Internet Service Providers (ISPs). The following tools are accessible through the organization's website, www.search.org.

- **Internet Service Provider List:** The ISP List is a database of Internet service and other online content providers that can assist investigators in obtaining data needed for an investigation. For each ISP, there is a listing of legal contact information and instructions for serving subpoenas, court orders, and search warrants.
- **Training:** SEARCH offers both instructor-led and self-paced online courses centered on high-tech crime investigations, public safety and emergency communications, and justice information sharing.
- **Quick Access ISP Information:** Through a simple online request form, SEARCH provides law enforcement investigators with documents to aid in data requests to ISPs. These files include legal process policies and law enforcement compliance guides for major companies, such as Apple, Snapchat, and Uber.
- **The National Domestic Communications Assistance Center (NDCAC)** maintains a database with documents to aid in law enforcement agencies' data requests to ISPs. These files include point-of-contact information and search warrant templates for more than 100 applications. https://ndcac.fbi.gov/

meeting reported mixed success in obtaining digital evidence from tech companies. While some departments described positive working relationships with certain tech companies, others have faced resistance to data requests despite having followed proper legal procedures. Ames, Iowa Police Commander Geoff Huff explained, "Each company has varying levels of willingness to help police."

Delays are a problem: Participants discussed several challenges when working with tech companies. Some companies take a substantial amount of time to provide the requested data, even in time-sensitive cases. While investigating a homicide, for example, detectives from the Roanoke County, VA Police Department secured a search warrant for the on-board GPS in the car of a person of interest. According to the vehicle manufacturer, the device recorded the car's location for 30 days. "To date, nearly 18 months later, we still have not received the requested information from the GPS," Police Chief Howard Hall said. Philadelphia Police Inspector Jim Smith said, "Even under exigent circumstances, it can often take 10 days for the tech companies to respond to our requests."

In some cases, tech companies will provide "jumbled" (or highly coded) data to the police in response to records requests. "It is sometimes presented in an unreadable code, which is totally useless to us unless we can decipher it. But

my analysts have had some success importing social media data and leveraging PENLink[84] to make sense of it," said Milwaukee Police Captain David Salazar.

Although the tech companies may be required to surrender the data, there are no laws or standards governing how the data is presented. When the police receive highly coded data, they often must expend considerable resources trying to decipher it.

Companies may notify suspects: Police can also encounter challenges because of tech companies' notification procedures. Many tech companies have policies to notify users when data on their device is subject to seizure by the police, unless prohibited by a gag order from a judge. Notification can tip off criminals and give them time to flee or destroy vital evidence. In some cases, this practice may enable suspects to intimidate witnesses.[85]

Some experts suggested that cooperation from tech companies may depend on the nature of the case being investigated. Companies may be fearful of tarnishing their reputations if they are uncooperative in sensitive cases, particularly those that involve juvenile victims.



Milwaukee Police Capt. David Salazar

> "For sex crimes, especially human trafficking, we have found that tech companies respond to subpoenas very quickly, because they don't want to give the appearance that they're impeding an investigation of the trafficking of a 12-year-old victim. In these cases, data is turned over in three to four days, which is several times faster than data requests for homicide cases."
>
> **— Tulsa Police Deputy Chief Dennis Larsen**



Tulsa Deputy Police Chief Dennis Larsen

Some participants expressed frustration over the inability to obtain data that is the subject of judicially issued subpoenas and search warrants. "In one high-profile case, we presented a company with a valid search warrant and carefully followed the process for data requests outlined in their law enforcement manual," said Superintendent Drew Evans of the Minnesota Bureau of Criminal Apprehension. "The company refused to provide the data based on the public perception of the case."

Some experts believe that the intentions of police departments seeking data are often misunderstood. "We are not seeking a backdoor," said New Jersey State Police Major Frederick Fife. "We're trying to go in the front door like we always have, with a warrant, and have tech companies respect judicial authority in the United States as it pertains to us getting digital evidence."

---

84. PENLink is a company that provides data intercept equipment and software to law enforcement agencies. See https://www.penlink.com/about/

85. "Apple, Facebook, Others Defy Authorities, Increasingly Notify Users of Secret Demands after Snowden Revelations." *The Washington Post,* May 1, 2014. https://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html?utm_term=.6495e8bb0847

Seeking Legislative and Policy Changes

> "Unless Congress acts soon to require compliance with a warrant, I anticipate that the choices being made today by technology companies to rapidly move to ubiquitous hard encryption will cripple investigations of even the most disgusting of crimes—Internet crimes against children."[86]
>
> **— Indiana State Police Captain Charles Cohen**

While contracting with private experts or working directly with tech companies can provide relief in some cases, most experts argue that the best way to address the issue of encryption is through legislation. As a result, public safety officials have begun advocating legislative and policy reforms that would increase their ability to execute lawful court orders.

On April 19, 2016, for example, Indiana State Police Captain Charles Cohen testified before the U.S. House of Representatives to highlight the issue of "going dark." He cited a child exploitation case in which a federal judge ordered the suspect, Randall Fletcher, to disclose his encryption key so investigators could examine several storage devices thought to contain child pornography. The suspect provided a passcode, but it only opened two of the three storage devices in question. Investigators found thousands of images of children forced to engage in sexually explicit conduct. To date, the contents of the third device have not been recovered due to encryption. Cohen testified, "It is always difficult to know what evidence and contraband is not being recovered, the child victims who are not being rescued, and the child sex offenders who are not being arrested as the result of encryption."[87]

Police leaders are being encouraged to discuss publicly the "going dark" problem and provide examples of how it is impacting investigations. Educating lawmakers and the public on the issue may be an important first step to producing a legislative solution.

Educating Judges, Prosecutors, and Jurors About the Benefits—and Limitations—of Technology

Another challenge facing criminal investigators is that judges, prosecutors, and other criminal justice officials do not always fully understand the technology behind digital evidence.

Like all warrants or subpoenas, requests for digital evidence must be approved by a judge, who may or may not have expertise about the technology involved. For example, judges may be reluctant to issue search warrants for digital devices because they contain vast amounts of personal information, some of which may not be connected with the investigation.

Burlington, VT Police Lieutenant Mike Warren explained this dilemma:

>> continued on page 46



Burlington, VT Police Lt. Michael Warren

86. "Deciphering the Debate Over *Encryption: Industry and Law Enforcement Perspectives*." Testimony of Charles Cohen. U.S. House of Representatives. April 19, 2016. P. 7. http://docs.house.gov/meetings/IF/IF02/20160419/104812/HHRG-114-IF02-Wstate-CohenC-20160419.pdf

87. Ibid., p. 6.

Understanding the Harm Caused by the Microsoft Decision

One of the biggest frustrations that investigators face is the inability to get data from smartphones, tablets, and other mobile communications devices, even when they have a valid search warrant for the data. A main source of this frustration is the 2016 appellate court decision in *Microsoft Corporation v. United States*.[88] In this case, the U.S. Court of Appeals for the Second Circuit determined that the government, even with a warrant, cannot require Internet Service Providers (ISPs) based in the United States to relinquish data *that is stored overseas*.

A Harvard Law Review article summarized the nature of the issue, arguing that the problem is that laws are lagging behind the reality of information technology:

> Nearly all Internet users interact with "the cloud" every day, but most never consider what—or where—"the cloud" is. As it turns out, "the cloud" is composed of server farms located all over the world. Companies like Google, Facebook, Apple, Microsoft, and Amazon now host large quantities of data abroad, raising novel jurisdictional questions.
>
> Recently, in *Microsoft Corp. v. United States*, the Second Circuit held that the government cannot compel Internet Service Providers (ISPs) to turn over data stored overseas, even with a warrant. The court did not acknowledge the unique "un-territorial" nature of data, instead proceeding as if it were considering a physical object.
>
> Increasingly, courts must apply old laws to new technology. In doing so, they can either acknowledge the unique features of modern technology, or, like the Second Circuit, they can disregard these differences. Only the first approach allows courts to grapple with the legal issues generated when old law meets new tech. In *Microsoft*, the majority did not engage with the emerging scholarly consensus that the "where" of data is not a straightforward inquiry. It thus did not address the novel issues implicated in this case and failed to reason through its decision fully.[89]

The Microsoft verdict has created major legal challenges for law enforcement officials seeking digital evidence for criminal prosecutions. Participants at the *Critical Issues* meeting discussed the challenges they have faced in light of the Microsoft Decision.

Mutual Legal Assistance Treaty: There is a "workaround" that law enforcement agencies can sometimes use to obtain data stored in foreign countries, called the Mutual Legal Assistance Treaty (MLAT).[90] MLATs are "bilateral agreements that effectively allow prosecutors to enlist the investigatory authority of another nation to secure evidence—physical, documentary, and testimonial—for use in criminal proceedings by requesting mutual legal assistance."[91]

However, the process of soliciting assistance from foreign countries through MLAT can be slow and cumbersome, and it may require legal resources that many law enforcement agencies do not

88. U.S. Court of Appeals for the Second Circuit. *Microsoft Corporation v. United States of America*. July 14, 2016. http://www.scotusblog.com/wp-content/uploads/2017/07/17-2-opinion-below.pdf

89. "Microsoft Corp. v. United States: Second Circuit Holds that the Government Cannot Compel an Internet Service Provider to Produce Information Stored Overseas." *Harvard Law Review,* Dec. 9, 2016. https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/

90. Additional information about the MLAT process is available at "Mutual Legal Assistance Treaties." https://mlat.info/.

91. "Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests." K & L Gates Legal Insight, January 20, 2017. http://m.klgates.com/files/Publication/669681d7-12d7-451e-8240-a33cf67c959f/Presentation/PublicationAttachment/ec5fc22d-3e3c-4607-bcb3-f4e99e3f59b4/GE_Alert_01202017.pdf.

possess. Some departments reported simply discontinuing or scaling back investigations when they learn that critical data is stored overseas.

"The MLAT process can take between six months to a year. A lot of departments don't go down that avenue because they don't have time to jump through the hurdles," said Jeff Lybarger, Director of Training for the National White Collar Crime Center.

Some law enforcement leaders have called for a legislative remedy, because the MLAT process is only occasionally helpful. "A clear, singular legal mandate for provider compliance to legal process is the only viable solution," said Massachusetts Assistant Attorney General Christopher Kelly in testimony before a subpanel of the U.S. Senate Judiciary Committee.[92] "And it should remedy the chaos and confusion caused to the providers in the wake of the Second Circuit's decision. The MLAT process shouldn't be necessary in the first place, and is not a viable solution to this problem."[93]

DOJ is challenging the Microsoft decision: In October 2017, the U.S. Supreme Court granted a petition by the U.S. Justice Department to review the *Microsoft* decision. In its brief, the Justice Department urged the court to reverse the Second Circuit ruling. "Under longstanding principles, the recipient of a subpoena to produce documents in the United States must produce all specified materials within its control, even if the recipient chooses to store those materials abroad," the Justice Department said.[94]

Within the Department of Justice, the Computer Crime and Intellectual Property Section (CCIPS) is challenging the decision on multiple fronts, including litigating against the Second Circuit's stance on a district-by-district basis across the country. Seven federal district courts have disagreed with the *Microsoft* decision. CCIPS also has proposed federal legislation to roll back the Second Circuit's Microsoft decision.

CCIPS Attorney Erica O'Neil encouraged local and state law enforcement leaders to get involved with these issues. "The Computer Crime and Intellectual Property Section would like to know about the challenges state and local law enforcement agencies have faced because of the *Microsoft* decision," she said.



Attorney Erica O'Neil, Computer Crime and Intellectual Property Section, U.S. Dept. of Justice

92. Testimony of Christopher W. Kelly before the U.S. Senate Judiciary Committee, May 10, 2017. https://www.judiciary.senate.gov/imo/media/doc/05-24-17 percent20Kelly percent20Testimony.pdf

93. Ibid, 5.

94. "Brief for the United States," *U.S. v. Microsoft Corp.* August 28, 2017. Page 32. https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf

continued from page 43

"Some judges don't quite understand how the technology works, so they might grant us a warrant but say we cannot search the whole phone. Unfortunately, the technology is designed so that you cannot perform a forensic dump on a phone by only taking a few things. You have to extract all of the data and sort through it."

"CSI Effect" creates unrealistic expectations: Criminal prosecutions can also be hindered by jury members who may have an inadequate or mistaken understanding of the technical facets of digital evidence. "We are experiencing a 'CSI effect,' where juries are expecting digital evidence in many cases," said National District Attorneys Association Executive Director Nelson Bunn. Jurors also may expect digital investigative technologies to work flawlessly every time, because television dramas portray the technologies that way. As a result, jurors may be suspicious of a prosecution if it fails to present extremely high levels of digital evidence.

"I see digital evidence becoming a demand of juries down the road," said Cornelia Sigworth, Associate Deputy Director of the Bureau of Justice Assistance. "Juries know that digital evidence is available, and it is going to be required as part of the cases. I don't think this is something that we can back away from."

In some cases, juries may simply discount digital evidence for unknown reasons. Ames, IA Police Commander Geoff Huff described a homicide trial where the suspect shot her husband while he was sleeping. A week before the murder, the suspect conducted a Google search about "how to kill your husband in his sleep." Although this evidence was introduced in the trial, the jury did not seem to take it into account when determining a verdict, along with some other evidence. "I don't know if the jurors didn't trust the information or what their reluctance was, but the defendant was only convicted of voluntary manslaughter on what looked like a clearly premeditated murder," Huff said.



Nelson Bunn, Executive Director, National District Attorneys Association



Cornelia Sigworth, Associate Deputy Director, Bureau of Justice Assistance

How Criminal Investigations Are Changing: What Agencies Are Doing to Address the Changing Nature of Crime

THE CHANGING NATURE OF CRIME HAS DRAMATICALLY RESHAPED criminal investigations. In the past, detectives responding to a crime scene could focus almost exclusively on securing and collecting physical evidence and interviewing witnesses.

Now, in addition to those activities, investigators must also attempt to secure and access smartphones and other communications devices; review social media accounts of victims, suspects, their friends and relatives, and others; review nearby camera feeds or gunshot detection systems; and check any "Internet of Things" devices, such as Fitbits or video cameras in cars, that may be associated with the victim or suspects.

For example, a person's presence in a room on a certain date may be inferred if the person asked a question of an Amazon Echo device, because the device keeps a record of all inquiries and when they were made. And the specific questions that a person asked an electronic device may provide clues to the person's thoughts or activities.

How well police agencies carry out these investigations of digital evidence increasingly will determine how successful they are in solving crimes.

Police also must develop new expertise in areas such as dark web investigations, social media apps, and other investigative tools. Agencies also need to examine how their investigative functions are organized and staffed, and what training and technical assistance they need to be successful.

Using New Investigative Tools

Just as criminals are adopting new methods, police need to develop new investigative strategies. Attendees at the *Critical Issues* meeting described how police are becoming adept with social media, web-based applications, Internet of Things (IOT) devices, the dark web, and other technologies as key elements of their investigative strategies.

>> continued on page 50

Peter the Great: A Case Study in New Investigative Techniques

How an Overdose Death in Portland, Oregon Led Police to an International Online Drug Trafficker

When there is a fatal drug overdose in Portland, Oregon, the Portland Police Bureau (PPB) immediately initiates a full-scale investigation into the circumstances surrounding the death. If detectives can determine who supplied the drugs and the evidence is strong enough, prosecutors may seek so-called "Len Bias charges" against the supplier.

Named after the University of Maryland basketball star who died of a cocaine overdose in 1986, the Len Bias Act is a federal law that provides for a 20-year minimum prison term for dealers convicted of supplying drugs that result in a person's death. Under the law, when a local police department investigates an overdose death, the U.S. Attorney's Office in that jurisdiction may take the case for federal prosecution if sufficient evidence is present and certain requirements are met. In Portland, the PPB works closely with the U.S. Attorney's Office and federal law enforcement agencies to determine whether a case warrants prosecution under the Len Bias Act.

A recent opioid overdose case in Portland illustrates the important role that technology—in particular, dark web investigations—can play in drug trafficking investigations. At the *Critical Issues* meeting, officials with the Portland Police Bureau, Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI), the U.S. Postal Inspection Service, and the Greenville, SC Police Department detailed a compelling case that they recently investigated, involving an online trafficker who went by the name of "Peter the Great."

Combining Digital and Physical Evidence to Trace the Last Actions of an Overdose Victim

On February 16, 2017, 18-year-old Aisha Zughbieh-Collins was found dead in her Southeast Portland apartment from an overdose of a synthetic opioid called U-47700 (or simply U4). The drug was so new to the Portland area that neither police investigators nor the city's public health officials had ever encountered it before.

Aisha's mother, suspecting that her daughter had purchased the drugs online, provided detectives with Aisha's email address. That was a start, but not enough to launch an online investigation.

At the scene, however, detectives uncovered important physical evidence indicating that the drugs had likely been shipped through the mail. This evidence included a distinctive brand of pregnancy kit (sold only at Dollar Tree stores) that was likely used to hide the drugs during shipment. They also found a mailing envelope inside the apartment. U.S. postal inspectors determined that envelope had a fictitious return address, but that it was purchased at a post office in Greenville, SC. Importantly, they discovered a notepad with an alphanumeric code written on it.

Unsure of what the code meant, Portland police turned to a Portland-based ICE/HSI agent who is regarded as a national expert in "dark web" marketplaces, where synthetic opioids and other drugs are often sold. Special Agent Guy Gino is assigned full-time to Portland's High Intensity Drug Trafficking Area (HIDTA) interdiction team. He is housed in a PPB facility, and therefore can work directly with police investigators at the outset of cases such as this one that involve the dark web.

Investigators learned that the alphanumeric code was Aisha's PGP key. PGP, or Pretty Good Privacy, is an encryption program designed to increase the security of email communications and other online transactions. PGPs are often used by individuals to access hidden marketplaces on the dark web.

One Case Leads to Nearly 10,000 Drug Transactions

Using Aisha's email address and PGP key, investigators determined that just five days before her death, she had purchased the U-4 opioid on a dark web marketplace called AlphaBay, which had emerged as

a leading marketplace for illegal merchandise following the takedown of Silk Road in 2013. The date of that purchase matched up with the timing of the mailing envelope recovered inside Aisha's apartment. The alleged online seller's username was "Peter the Great." Data from AlphaBay indicated he had made nearly 10,000 transactions on the site.

In April, detectives went on the dark web and purchased U4 from Peter the Great. The drugs arrived wrapped in the same pregnancy kits and containing the same type of shipping labels found in Aisha's apartment. Postal inspectors further determined that the shipping labels used on the packaging originated from an online company that accepts only Bitcoin digital currency.

From Portland, to Greenville, to China

Further investigation revealed that the online shipping label purchases were tied to two secure email addresses. Investigators filed a subpoena for any records connected to those email addresses. That led them to Theodore Khleborod, a person of interest living in Greenville. Detectives determined that Khleborod had received numerous international packages from China, where a great deal of U4 is made. Through social media postings, they also found out that Khleborod was in a relationship with a woman named Ana Barrero.

Next, investigators collected sales information showing a spike in pregnancy kit purchases at a particular Dollar Tree store in Greenville. They also retrieved store video showing Barrero purchasing numerous pregnancy kits at that store. Portland officials traveled to Greenville and, with the assistance of Greenville Police and ICE/HIS agents in South Carolina, began surveillance of both Khleborod and Barrero. They witnessed Barrero mailing large numbers of parcels that matched other packages in the investigation, including the one from Aisha's apartment.

In late April, officers arrested Khleborod and Barrero. They faced federal drug distribution charges in both South Carolina and Oregon, with Oregon officials considering additional "Len Bias charges" as well. Investigators believed "Peter the Great" may be connected to more than a dozen other overdose deaths across the country. In November 2017, Khleborod was found dead in a jail cell in Spartanburg County, SC, an apparent suicide.

3 Lessons Learned

From the Peter the Great case, the Portland Police Bureau developed critical lessons for future high-tech overdose investigations. Captain Mark Kruger and Sergeant Chris Kenagy outlined three of those lessons at the *Critical Issues* meeting:

1. Police and prosecutors need to develop a working knowledge of the dark web and the use of crypto-currency (such as Bitcoin). These investigative elements can be present not only in drug cases, but also gun sales, human trafficking, and financial fraud crimes committed by gang members and other criminals to fund their operations.

2. To effectively collect and analyze digital evidence from the dark web, local, state, and federal agencies should have a close working relationship with one another and be willing to share information, resources, and expertise.

3. New, technology-based approaches to criminal investigations are important, but they must be combined with traditional investigative work that is thorough and detailed.

Captain Kruger noted that if every state had at least one multi-jurisdictional team like the Portland HIDTA that investigated overdose deaths, and if each team conducted at least one major takedown per year, then police could potentially save hundreds of lives.

continued from page 47

Social Media Postings Show Connections between Victims and Susects

Social media—Twitter, Facebook, Instagram, and other apps—have become an essential investigative tool for police agencies. Social media can be used to collect evidence, locate suspects, and identify criminal networks.

"Social media can be used to connect all of the people involved in a case," said Ames, Iowa Police Commander Geoff Huff. "Investigators can go to user profiles to see who is friends with whom, and identify other people they should be talking to."



Ames, IA Police Commander Geoff Huff

Investigators are also using social media to identify potential suspects—for example, persons who engaged in hostile exchanges with a victim online. In other cases, police may have video footage or witness descriptions of a suspect who was wearing unusual clothing or jewelry at the time of the crime. "So detectives and analysts look at social media to see if potential suspects have posted pictures or videos wearing outfits that match the clothing descriptions," Philadelphia Police Inspector Jim Smith said.

Some offenders use social media to facilitate crimes, while others actually post incriminating evidence about crimes they have been involved in. "We had a case where the victim was viciously beaten and robbed, and video of the attack was uploaded to Facebook and Instagram," said Fayetteville, NC Police Captain James Nolette.

Social media platforms contain an abundance of readily available digital evidence. And because many people do not use the privacy controls on their social media accounts to limit who can see their postings, much of the information on social media is public. So police do not always have to seek warrants to access the information.

Participants at the *Critical Issues* meeting shared cases in which agency personnel successfully used social media to support their investigations:

- **Washington, DC:** While investigating a fraud case, the Washington, D.C. Metropolitan Police Department discovered that someone had opened three credit card accounts in the victim's name. Through an address listed on one of the credit card statements, police determined that a possible suspect was the manager at the fast food restaurant where the victim worked. While reviewing the suspect's Facebook page, detectives noticed a correlation between various social media posts (pictures of vacations, activities, and other purchases) and charges on the victim's credit card. By connecting the digital posts with charges on the credit card statements, investigators used social media to successfully prosecute the case.

- **Chicago:** The Chicago Police Department has had success using social media to quickly track drown suspects. In one case, police discovered a picture of a police badge on social media with the caption, "Look what I just got my hands on." Using the subject's social media profile, "police were knocking on the suspect's door and arrested him within 10 minutes," recalled Deputy

Chief Steve Caluris. In a separate case, a gang member posted a picture of himself under a street sign with the caption, "Come and get me." An hour later, a rival gang member reposted the image to his own social media account after having shot the man in the picture. Again, social media profile information led police to the shooter.

- **Volusia County, FL:** Detectives from the Volusia County, FL Sheriff's Office investigated a burglary in which a bank bag filled with cash was stolen. Investigators had a description of the suspect based on surveillance footage, but the suspect's identity was initially unknown. However, the suspect had distinctive tattoos, and investigators were able to use them to identify a potential suspect. Detectives then turned to Facebook to locate pictures of her tattoos and compare them to the tattoos depicted in the surveillance footage to get an identification.

Using social media as an investigative tool requires only limited technical knowledge on the part of investigators. So this approach does not have to be limited to computer crime or technical specialists. Almost any detective should be versed in how to access the most common social media platforms and retrieve publically available information.

Mobile Apps Provide Additional Clues

As people use more mobile applications on their smartphones (e.g., navigation, social networking, shopping, banking, etc.), police investigators are increasingly turning to suspects' use of mobile apps to trace their location and activities. These applications are becoming a rich source of investigative information that police agencies should cultivate.

Following are two examples cited at PERF's *Critical Issues* meeting of how investigators used mobile app information to identify suspects:

- The Milwaukee Police Department investigated a case in which a woman was kidnapped and raped by two individuals in a truck. While in the vehicle, the victim noticed the driver was using Google Maps on his cellphone for navigation, and she provided that information to investigators. Police then executed a search warrant to do a "cell tower dump" in a specific area of a freeway, based on the victim's statement. Google was able to tell investigators which users were using the app at that time and which cell towers the rapists' phone was pinging. "The data from Google was crucial evidence needed to prosecute the case," said Captain David Salazar. "By mapping the data, we were able to connect the offenders to another related attempted kidnapping and rape."

- Investigators in Essex County, NJ used information from Fandango, an app used to purchase movie tickets, to help identify a suspect in a murder case. When investigators reviewed the victim's smartphone, they discovered two critical pieces of information: the victim had recently used Fandango to purchase movie tickets, and the suspect was listed as a recent contact. Detectives then pulled surveillance video from the theater, which showed the victim

and the suspect there together. During questioning, the suspect denied being at the theater, so the Essex County Prosecutor's Office is using that information to impugn the suspect's credibility. Prosecutors have also charged the suspect with two other murders and one aggravated assault.

"Internet of Things" Devices Can Store Important Data

The term "Internet of Things" (IOT) refers to the network of digital objects that transmit data using embedded sensors. Examples of IOT devices include Fitbits, Amazon Echos, house security systems that use the Internet, "connected cars" equipped with Internet access, and smart appliances.[95] As IOT devices become integrated with everyday life, police should be looking to extract data from them to support their investigations.

Here are two recent examples of how IOT data was used during criminal investigations:



Seattle Police Sgt. Shane Anderson

- The Seattle Police Department used data from a Fitbit during an investigation of an attempted sexual assault. While on a run, the victim stopped at a park to use the restroom, where she was attacked by the suspect. The victim was able to fight the suspect off with the help of a witness. Police used data from the Fitbit to map out the victim's movements for the jury. "The information bolstered the prosecution by showing the victim's movements from arrival to the restroom, the struggle that ensued, and her departure from the area," said Sergeant Shane Anderson.

- The Middletown, OH Police Department used data from an electronic heart monitor to investigate the possibility that a man had set his house on fire for the purpose of insurance fraud. The man had told a 911 call-taker that when he noticed the fire, he packed some suitcases and threw them out a bedroom window after breaking the glass with his walking stick. Given that the man has an artificial heart linked to an external pump, investigators were suspicious that he could have exerted himself as he described. Police executed a search warrant for the records from the suspect's electronic heart monitor. Data from the device, including the suspect's heart rate and cardiac rhythms, reportedly contradicted his account, and he was indicted on charges of aggravated arson and insurance fraud.[96]

While accessing IOT data has proven useful in these and other investigations, it should be noted that defense attorneys and others have raised constitutional issues and privacy concerns. This will likely be a growing area for drafting of law enforcement policies, and for court rulings.

---

95. "Internet of Things devices, applications, & examples." *Business Insider,* Dec. 19, 2016. http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8.

96. "Middletown man's electronic heart monitor leads to his arrest." *WLWT-5,* Jan. 27, 2017. http://www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942.

Other Innovations

With many digital devices in use today, police are finding other innovative ways to use technology to support investigations. Following are three examples presented at the *Critical Issues* meeting:

- **Bluetooth in cars:** The Northern California Regional Intelligence Center was able to help investigators solve a murder by placing the suspect at the scene of the crime, after extracting Bluetooth-enabled data from a vehicle. When cell phones are connected to vehicles via Bluetooth, data from the phone—including call logs—may be stored in the vehicle. "So if you connect your smartphone to a car via Bluetooth, we may be able to extract the information through the car, even if your phone is inaccessible or locked," explained Deputy Director Daniel Mahoney.

- **Tracking Wi-Fi connections:** Some digital devices automatically attempt to connect to nearby Wi-Fi signals. While investigating a shooting, the Fayetteville, NC Police Department knew that a suspect's vehicle was stopped at a certain intersection around the time of the crime. "We tracked the movement of the vehicle driving down the street as devices within the car automatically connected to the free Wi-Fi from stores," said Captain James Nolette. Investigators were able to identify the suspect by seeing who had connected to the Wi-Fi of a particular store near the intersection during the same time that the suspect's car was in the area.

- **K-9s can detect digital media:** The New Jersey State Police is using digital media K-9 dogs to locate digital evidence. "There are chemicals used in digital media, thumb drives, discs, etc., and a dog can recognize those trace chemicals," Colonel Joseph Fuentes explained. "We had a case where we found a thumb drive and other media behind a wall. Dogs can be trained to sense that."

Rethinking the Organization and Operations of Investigative Units

TO KEEP PACE WITH CHANGES IN CRIME, ESPECIALLY COMPUTER-enabled crime, some police agencies are rethinking their organizational and operational structures. This includes creating or strengthening computer crime units, and also working to build up digital investigation skills that all personnel can benefit from throughout the department.

Police leaders at the *Critical Issues* meeting discussed some of the approaches they are taking:

- **Restructuring investigations:** The Fairfax County, Virginia Police Department is restructuring its Criminal Investigations function to better address the challenges of new crime types and the needs of technology-driven criminal investigations. The department is building three investigative units: 1) Major Crimes, 2) Organized Crime, Narcotics, and Intelligence, and 3) Cyber and Crime Scene. The department is also putting its computer forensics unit under the new Cyber and Crime Scene Bureau. The goal is to integrate traditional and digital investigative techniques.

> I was a homicide detective for 10 years, and the way homicide cases are done now is completely different. Back in the day, a homicide investigation was all about doing an interview, going to the victim's job, talking to the family, etc. You would get firsthand information from people, and that's how you would put a timeline together.
>
> Nowadays, victims typically have one to three smart devices, and witnesses and suspects do too. So if I want to trace a victim's movements, I have to download cell records, obtain subpoenas to review text messages, look at phone logs and social media accounts, and review all other forms of digital evidence. In the past, I would collect one or two binders of information. Now I now end up with 125 gigabytes of digital evidence from just three people.
>
> The upside to that is that we typically have a pool of witnesses for our detectives to speak to within three hours. Today we can easily establish a suspect's habits, which used to take us three months of observation. Now we have so much digital evidence that in a matter

of two days, my analysts can establish a picture of where the victim was, at what time, and who they were texting. You can get a lot of information, but you need the layers of expertise and technical support in order to build the case.

You need a minimum of three support people behind each homicide detective, to cipher data and unmask the people behind the technologies of the internet. The analyst can be embedded at the hip of a detective and tell them exactly what they need to collect, or where to get a statement on the record that can demonstrate inconsistencies.

— Major Richard Perez, Fairfax County (VA) Police Department

- **Spreading expertise around:** The Paterson (NJ) Police Department is working to ensure that its detective squads have a range of skills and expertise. Within each squad of four to five detectives, the department aims to pair detectives who are familiar with social media platforms and recovering digital evidence with seasoned detectives who have extensive experience with interrogations, physical evidence collection, and other traditional investigative skills. "As a smaller agency, that helps us cover all bases for our investigations, because those two types of detectives complement each other well," said Captain Richard Reyes.

- **Making best use of digital forensics examiners:** The Montgomery County, MD Police Department revamped its digital forensics capabilities and decentralized its forensic examiners. In addition to the five full-time digital forensic examiners housed in the Electronic Crimes Unit, the department trained five additional detectives from other units of the department to serve as part-time examiners. When a digital forensic examination can be improved through expertise in a particular type of crime (e.g., auto theft or child exploitation), the part-time examiners can step in and serve as subject matter experts, providing guidance on the most relevant evidence that investigators should focus on. The specialized examiners can assist the full-time examiners from the outset of an investigation by helping to triage investigative priorities and write search warrants that focus on the most important pieces of evidence. The new staffing alignment has spread additional expertise throughout the department, without incurring the major expenses of hiring new personnel.

  "This program allows the department to have a ready group of reinforcements should the need arise, and they serve as ambassadors of knowledge to assist other investigative units," said Sgt. Michael Yu of Montgomery County's Electronic Crimes Unit. "The department has not had to increase overall agency staffing, as our only costs are associated with training, which we try to alleviate through as much free training as possible through courses offered by the National White Collar Crime Center or the National Computer Forensics Institute."

- **Strategic investigative capabilities:** Former DC Metropolitan Police Chief Cathy Lanier noted that during her tenure as chief, the department began to emphasize strategic investigative capabilities. For example, the department

moved away from its traditional "vice squads," which had focused largely on "buy and bust" and "jump out" operations. The department invested more heavily in real-time crime analysis and digital evidence capabilities.

- **Merging Organized Crime and Detective Bureaus:** To increase its overall investigative capabilities, the New York City Police Department decided to fold its longstanding Organized Crime Control Bureau into the Detective Bureau. The move was designed to increased coordination and speed up investigations. "We found that we had really great detectives working homicides and working narcotics," Chief of Detectives Robert Boyce said. "If we channeled them into one unit to attack the gang problem, we could get a quick investigation. Now, typically in six to eight months, we're able to take down the gangs that we are targeting."

New Approaches to Staffing

New types of computer-enabled crime and new approaches to criminal investigations are putting pressure on police agencies to recruit, hire, and train people who can operate effectively in this new environment. Simply reallocating existing personnel, even with additional training, may not be sufficient for meeting the requirements of today's criminal investigations.

Many police agencies are now looking to hire civilian personnel who have the specialized skill sets needed to support today's digitally driven investigations. Participants at the PERF conference said that it is important for these personnel to have a range of technical and analytical skills that complement the skills of experienced detectives. They must also be able to operate effectively in a fast-paced, high-stress environment.

The St. Paul, MN Police Department recently conducted a study to determine its staffing needs. One of the key findings was the need to allocate staff to manage digital evidence and to assist with administrative work in support of the department's detectives. "We need adequate personnel to assist with subpoenas, search warrants, digital evidence and technology needs, so our investigators can focus on their core responsibilities," said Chief Todd Axtell. "We are hoping to find 10 to 15 investigators through identified staff reallocation who can help us with this need."



St. Paul, MN Police Chief Todd Axtell

Police executives looking to hire specialized civilian staff to support criminal investigations face two hurdles: how to justify spending resources on hiring non-sworn personnel, and how to ensure that the positions continue to be funded.

"Trying to convince the politicians and the public that you need these civilian employees to do effective criminal investigations is a tough sell," said former Chief Cathy Lanier. Other chiefs echoed this concern. "When I try to back-fill positions that support police officers, particularly in a world that has increased suspicions about police surveillance and privacy, it is hard to get anywhere," said Metropolitan Nashville Police Chief Steve Anderson. In addition, when state and local municipalities implement budget cuts, civilian positions are often the first to be targeted for layoffs, hiring freezes, or other cost-saving

>> continued on page 58

How Washington, D.C. Police Are Using Civilian Specialists To Accelerate and Improve Criminal Investigations

Washington, D.C.'s Metropolitan Police Department has invested in specialized civilian positions to support its criminal investigators. With the proliferation of video security cameras, body-worn cameras (the department is outfitting all of its officers with BWCs), citizen cell phone video, and other digital data sources, the department wanted to focus on how to quickly access and process these new data sources, while reducing the burden on detectives for combing through that evidence.

Under former Chief Cathy Lanier,[97] the department created several civilian Criminal Research Specialist (CRS) positions. These research specialists are different from traditional crime analysts, who typically focus on collecting and analyzing statistical data, often in support of a Compstat-like process. Rather, a Criminal Research Specialist's primary responsibility is to gather and analyze digital evidence in criminal cases—and to do so quickly.

A CRS focuses on collecting potential evidence from a variety of sources, including security cameras, gunshot detection systems, computer-aided dispatch data, GPS tracking devices, and others. The specialists then integrate the data from different systems into a customized dashboard that can be accessed in MPD's command center.

Collecting evidence more quickly: Former Chief Lanier said the MPD found the Criminal Research Specialists to be especially valuable in cases such as non-fatal shootings and homicides, where the prompt collection and sharing of evidence are crucial. For example, when the city's gunshot detection system picks up the sound of gunfire, the activation appears on the dashboard, and any security cameras operated by MPD can be turned in the direction of the gunfire so that the research specialists can observe the scene. The Criminal Research Specialists also have the option of pulling up the scene on a map, to tap into traffic enforcement cameras in the area, in the event that suspects use a car to flee the scene.

Relevant information can be pushed out to patrol officers and detectives at the scene, or while they are traveling to the scene. In some cases, detectives arrive on the scene equipped with a folder of preliminary information developed by the CRS. This approach saves detectives time and can help ensure that investigations move quickly.

Chief Lanier said the division of labor between detectives and the CRS specialists is an effective way to ensure that all angles of an investigation are covered. "I think the answer to dealing with the changing nature of criminal investigations is to rely more on civilians," she said. "It is too much to expect one person to be a top-notch specialist on the technological aspects in addition to traditional investigative techniques."

97. Lanier currently is Senior Vice President of Security for the National Football League.

continued from page 56

measures. So even when police executives can hire non-sworn technical positions, it may be hard to hold onto those positions.

Reducing Staff Turnover

Retention of personnel—among specialized civilian staff as well as sworn investigators—is another challenge facing police agencies as they strive to ensure that they have the right people in place for today's complex investigations. Given the amount of time, funding, and other resources it takes for a police employee to undergo training and become effective in the digital aspects of criminal investigations, police executives need to consider innovative strategies for minimizing staff turnover in these specialized areas.

Participants at the PERF meeting noted that often, civilians who develop advanced technical skills at a police agency may, after a short time, be tempted to leave for jobs in the private sector, where pay and opportunities for advancement may be greater. "When you invest funding and effort to train people from the ground up—particularly younger civilians—they became attractive candidates for other agencies and companies," said Chief of Detectives Quovella Spruill of the Essex County, NJ Prosecutor's Office. For police agencies, developing career paths, competitive pay, and meaningful work for civilian employees is key to minimizing turnover.



Chief of Detectives Quovella Spruill, Essex County, NJ Prosecutor's Office

Retention can be a challenge among sworn personnel as well. In most agencies, individuals who develop expertise within specialized technical units have to transition out of those units when they get promoted. With the increased reliance on highly trained personnel to handle digital evidence, police agencies must think creatively about how to retain a strong technical capacity at every level of their organizations. One method would be to allow sworn personnel with unique technical skills to remain within their specialized units even after they are promoted.

Chief Daniel Slaughter of the Clearwater, FL Police Department said, "We need to be recruiting for different skill sets and educational experiences than a typical boots-on-the-ground guy. We need to develop the future leaders of our department into this specialty."

Privatization of Support Services Is an Option

Another consideration for police agencies looking to streamline their criminal investigations is to privatize some support services. The use of private digital forensics labs is one approach that could help agencies deal with the growing flood of digital evidence.

Given the time and expense it takes for police agencies to develop the capacity to perform forensic examinations in-house, some agencies have considered contracting out these services. This approach could help agencies take advantage of the latest in technology and training, and could possibly reduce personnel costs.

"Right now, I am fortunate enough to have three trained forensic computer staff members, but they are the probably the most expensive single unit that I have in my police department. Does it make sense for us to continue to have our three trained sworn staff and surrounding agencies to have theirs? Or should we potentially hire a private enterprise on a contractual basis that has the ability to maintain a cadre of technical specialists and keep current on technology?"

— Chief Jay Farr, Arlington, VA Police Department



Arlington, VA Police Chief Jay Farr

New Approaches to Training

"As a small department, we find it's really important for the patrolman who's just out of the academy to know some of these tactics on how to do these cyber investigations, because we are faced with all of these complex crimes, like any other jurisdiction."

— Deputy Chief Robert Fincher, Martinsville, VA Police Department



Martinsville, VA Deputy Police Chief Robert Fincher

Training is another critical component that police agencies must address as they improve their investigative capabilities and tackle new types of crime. Participants at the *Critical Issues* meeting identified three types of training that are especially important in this new environment:

- Training for detectives on digital facets of investigations,
- Specialized technical training for digital forensic examiners, and
- Training for patrol officers on how to handle and secure digital evidence at crime scenes.

Providing technology-related training can be difficult and expensive, especially for small to medium-sized agencies. "We are a small agency, so even with free training, the costs of travel and time away from the office are often too expensive for us," said Martinsville, VA Police Deputy Chief Robert Fincher.

It also can be difficult for agencies to provide their digital evidence specialists with the training they need to keep up with new and emerging technologies, while at the same time keeping staffing levels sufficient for investigations. "There's a balance that has to be struck between training and working, because the training has to be continuous. You're not trained once and good to go forever," said Sean Goodison, Deputy Director of the Center for Applied Research and Management at PERF.



Metropolitan Nashville Police Chief Steve Anderson

"With all the training involved, our people are probably out two months of the year. And the reason is that the technology is constantly changing, so the training is constantly changing."

— Chief Steve Anderson, Metropolitan Nashville Police Department

Free or Low-Cost Training Programs for State and Local Police Agencies

There are several options for free or reduced-cost training that state and local police agencies can pursue. The United States Secret Service runs the National Computer Forensics Institute (NCFI) in Hoover, Alabama.[98] The NCFI provides training on digital forensics and high-tech investigations for state and local police officers at no charge.

Other subsidized training opportunities for state and local agencies include online and in-person instruction from the National White Collar Crime Center; SEARCH (The National Consortium for Justice Information and Statistics); and the National Cyber Crime Conference.

The Law Enforcement Cyber Center, managed by the U.S. Bureau of Justice Assistance, has compiled a web page of searchable training opportunities for executives, officers, and prosecutors.[99]

Participants at the PERF conference agreed that federal and state agencies should expand the training and other resources they offer to local agencies on investigating computer-related crime.

Training the Entire Department

> "We need to look at the amount of digital evidence, and ask if our first responders understand its priority and how to triage, given the volume."
>
> **— Chief Steve Anderson, Metropolitan Nashville Police Department**

Participants at the *Critical Issues* meeting discussed the need to train forensic examiners and detectives, and also patrol officers, who typically are the first to come into contact with digital evidence at a crime scene. A number of officials said that rather than develop technical training in silos, police agencies should provide all personnel, including patrol officers, with a baseline of training on how to recognize and handle digital evidence. The National Institute of Justice has identified training for first responding officers on how to handle digital evidence as one of the priority needs for state and local justice agencies.[100]

Ensuring that all officers can distinguish useful and non-useful digital evidence: For example, the Montgomery County, MD Police Department has started training officers in its academy on how to recognize digital evidence. Through its "Shift ID" school, the department trains new recruits in how to recognize devices that may contain digital evidence, so that they do not miss important evidence that can help build a case. The training also serves

98. National Computer Forensics Institute. https://www.ncfi.usss.gov/ncfi/

99. Law Enforcement Cyber Center. "Training." http://www.iacpcybercenter.org/topics/training-2/

100. Sean E. Goodison, Robert C. Davis, and Brian A. Jackson, Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, RAND Corporation (2015). https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf.

another purpose: to help officers weed out devices that probably don't need to be analyzed. This can serve to reduce the backlog of digital evidence that agencies need to process. "For example, if detectives are at a crime scene, they might seize an old laptop with an inch of dust on it," said Sgt. Michael Yu of the department's Electronic Crimes Unit. "In most cases, there would be no need for it, because any information on it would probably be years old."

> "It's important to conduct training for the entry-level officer in the initial training academy. They are the frontline first responders, who come into the most contact with citizens and initial 911 calls. Because digital technology is so pervasive in all our lives, everyone needs to have a strong foundation and baseline knowledge of where evidence might reside, and what might be important in an investigation. They don't need to know the technical aspects of how to retrieve that digital evidence; they just need to know what might exist, how to preserve it, collect it, and understand the nexus to their case. We could not fathom an officer in the late 20th century not understanding the importance of fingerprints or DNA, so we must acknowledge the importance of digital evidence in the 21st century."
>
> **— Sergeant Michael Yu, Montgomery County, MD Police Department**



Sergeant Michael Yu, Montgomery County, MD Police Department

On-the-Job Training

> "You need to put experienced investigators on these interviews, because many of the technically savvy perpetrators like to talk. Many of these criminals like to brag about how smart they are, and you can get them to walk you through the technical pieces of their crimes."
>
> **— Special Agent Guy Gino, Immigration and Customs Enforcement/ Homeland Security Investigations**



Special Agent Guy Gino, ICE-Homeland Security Investigations

Participants at the *Critical Issues* meeting stressed the importance of learning on the job as well as in training sessions. In some cases, investigators learn about technology from criminals themselves.

For example, interviews conducted with suspects can yield important clues about the latest tools, techniques, and tradecrafts that facilitate computer-related crimes. As part of some plea agreements, suspects can be compelled to provide detailed information to investigators about how they committed their crimes.

Investigators also underscored the importance of getting onto various technology platforms and learning how to use them through hands-on experimentation. Detectives who work on dark web investigations have been able to strengthen their cases and discover other perpetrators through account takeovers, in which they assume the identity of a dark web hidden services provider to learn more about their operations.

Cybersecurity and Officer Safety Concerns

Police agencies should not rush into complex technical investigations—like dark web or social media investigations—without understanding the potential cybersecurity hazards and the risks to officer safety. Awareness and training on how to approach and conduct these types of complicated inquiries are critically important to the success of the investigations and the safety of the officers conducting them.

"If someone just wants to jump onto the dark web without any training, we have to be careful not to authorize that without fully considering all the dangers to which we may be subjecting them," said Captain James Nolette of the Fayetteville, NC Police Department. For example, investigators should work with technical experts to learn how to protect their digital footprints[101] and secure their networks prior to launching dark web and other complex online investigations. Learning those platforms through trial and error can be counterproductive and dangerous, if officers' identities are not protected online.

Deconfliction is critically important: Dark web and social media investigations also present challenges involving deconfliction. When multiple agencies, or multiple units within an agency, are investigating a case, investigations run the risk of becoming intertwined, especially when different agencies or units don't know that other law enforcement entities are operating in the same sphere or targeting the same subjects. The risk of inadvertent "blue-on-blue" encounters is particularly high on the dark web, where user anonymity is highly protected.

"Within a department, you may have a gang unit, a narcotics unit, and detectives from other units all on social media," said Chicago Police Deputy Chief Steve Caluris. "The chance for blue-on-blue is just so magnified, and there isn't really a good structure in place to solve that." Experts at the meeting noted that agencies such as the FBI's National Domestic Communications Assistance Center (NDCAC) can provide technical assistance to agencies to develop digital officer safety training programs and protocols.[102]

The Importance of Collaboration with Local, State, and Federal Partners

To build their capacity to investigate computer-enabled crime and manage more complex online investigations, police agencies are increasingly developing partnerships with other local, state, and federal agencies. From regional cooperatives to federal task forces, police are combining resources and expertise to expand their ability to manage these often complex cases.

---

101. See *Understanding Digital Footprints: Steps to Protect Personal Information.* Criminal Intelligence Coordinating Council, Global Advisory Committee, 2016. https://www.it.ojp.gov/GIST/1191/File/Understanding percent20Digital percent20Footprints-09-2016.pdf.

102. See "A hub for technical knowledge management." National Domestic Communications Assistance Center. https://ndcac.fbi.gov/.

Regional Cooperation to Pool Resources

Police executives at the *Critical Issues* meeting spoke about the need to pool resources at a regional level. By joining together, state and local agencies can provide staffing and other assistance to each other, and handle sophisticated challenges associated with digital evidence.

In the Los Angeles area, for example, the Beverly Hills Police Department created a *West Side High-Tech Task Force* that includes the Clover City Police Department, Santa Monica Police Department, and the UCLA Police Department. The Task Force is locally run and locally funded, but also includes federal partners such as the U.S. Secret Service. The Task Force specializes on cases that involve large amounts of money and complex applications of digital evidence.

Beverly Hills Police Captain Mark Miner described how pooling resources in this specialized area can serve as an important force multiplier for all of the partners. "Our department was able to purchase an off-network secure server with an immense storage capacity, as well as other types of state-of-the art technology and the latest software," he said. "But we knew that we would need multiple people to respond to these issues. The other departments help us when we're in need of additional assistance, and we can assist our partner agencies."



Beverly Hills, CA Police Lt. Mark Miner

Other jurisdictions are pursuing different approaches to regional cooperation. In some areas, large or mid-sized agencies with the most experienced digital forensic examiners handle complicated examinations for smaller agencies, in exchange for assistance with basic examinations. In the greater San Diego region, the Automated Regional Justice Information System (ARJIS) has allowed more than 80 agencies in the area to collectively share the licenses for expensive software. This has allowed all partners to obtain sophisticated technology that supports information-sharing, crime analysis, facial recognition, and other high-tech solutions.[103]

Participation on Federal Task Forces

As local agencies conduct complex criminal investigations, the federal government can assist in two important ways. First, federal task forces can be an essential first step toward building local agencies' capacity to investigate internet-enabled crime. Second, prosecuting cases in federal courts is often desirable, or even essential, for many types of digital investigations that cross city, state, or international borders.

For example, the "Peter the Great" investigation (see page 48) by the Portland High Intensity Drug Trafficking Area (HIDTA) relied on collaboration among federal, state, and local partners working side by side. What began as a local investigation of an overdose death, which would not have come to the attention of federal authorities, became a complex dark web case that reached across the country and around the world. Involving the task force had two primary benefits: it provided local authorities with federal expertise and resources,

103. Automated Regional Justice Information System. http://www.arjis.org.

and it allowed the criminal case to be brought in federal court, where charges are often more appropriate and penalties can be higher upon conviction.

"From the outset of many of our cases, we have federal experts who can advise us on best practices for the dark web and use of crypto-currencies," said Sgt. Chris Kenagy of the Portland Police Bureau. In Portland, communication and coordination among agencies are relatively straightforward, because federal agents from Immigration and Customs Enforcement/Homeland Security Investigations are stationed in Portland Police Bureau offices, and all parties know one another.



Sgt. Chris Kenagy, Portland, OR Police Bureau

Similarly, the New York City Police Department assigns investigators from its Grand Larceny Division to the FBI New York Cyber Crimes Task Force. The FBI agents provide NYPD investigators with extensive technical expertise, while NYPD investigators give the FBI insight into the operations of local criminal organizations on the ground. "This partnership can give us a picture of the true extent to which violent and computer-enabled financial crimes are tied," said NYPD Deputy Chief Joseph Dowling. "It also allows us to address crime affecting our community that would not trigger the federal threshold for these types of crimes."

Regional Computer Forensic Labs

Cooperation across the federal, state, and local levels can also help address another critically important concern: the extensive backlogs that some agencies are facing with the processing of digital evidence. Because there is a shortage of personnel and technical tools, state and local agencies are increasingly turning toward Regional Computer Forensic Labs (RCFLs) or fusion centers in their areas to assist with digital forensic examinations.

"Based on the overwhelming need in our region and our mandate to support criminal investigations, we created a digital evidence analysis capacity," said Deputy Director Daniel Mahoney of the Northern California Regional Intelligence Center. "State and local agencies with limited resources can give us their digital forensics for analysis and we also provide them with certified experts to testify in court," Mahoney added. The NCRIC has helped state and local agencies with video analytics, digital evidence extraction from vehicles, audio/video enhancement, and other capabilities. This approach can be tested and applied in other jurisdictions.

Although federal task forces can be effective in addressing complex crimes with digital components, experts at the *Critical Issues* meeting noted that these task forces cannot investigate every case. State and local agencies must also build their own internal capacity to investigate crimes that do not meet federal thresholds for investigation, or crimes that stand outside the jurisdiction of individual task forces. It is critically important that state and local police agencies secure funding and develop the training and capacity to tackle computer-enabled crimes on their own.

Technologies that Could Shape the Future of Criminal Investigations

> "The digital world is going to require digital solutions."
>
> **— Warren Loomis, President and CEO, Versaterm, Inc.**

Just as technology is fundamentally changing crime in the United States, technological innovations also have the potential to change the nature of criminal investigations. Participants at the *Critical Issues* meeting discussed three technologies that will likely shape criminal investigations well into the future: machine learning/artificial intelligence; video analytics; and real-time crime analysis.



Warren Loomis, President and CEO, Versaterm, Inc.

Machine Learning/Artificial Intelligence Will Speed Investigations

> "In the future, we're anticipating artificial intelligence systems that are capable of thinking like an actual detective: learning about the average criminal profile, the average characteristics of particular types of crime, and narrowing down leads from thousands and thousands of records, documents, and data, with minimal perimeters to help you identify what you should look for."
>
> **— Cathy Lanier, former Chief of the Metropolitan Washington, DC Police Department**



Cathy Lanier, Senior Vice President of Security, National Football League and former Chief of Police, Metropolitan Police Dept. of Washington, DC

With the volume of data involved in many police investigations today, the potential for saving time through machine learning and artificial intelligence (AI) is considered essential for public safety agencies. Artificial intelligence refers to the simulation of human intelligence by machines or computers; machine learning is the ability for a machine to "learn" from the universe of previous experiences involving the same basic set of variables.

The potential for applying artificial intelligence and machine learning to criminal investigations is vast. Artificial intelligence may be used in the future to quickly generate incident or crime reports from dictation, body-worn camera footage, and other discrete pieces of information; to comb through vast amounts of public records to help identify potential criminal suspects; or to support predictive analytics.[104] For example, Motorola Solutions is currently developing "intelligent cameras" that can comb through a variety of camera feeds looking for objects or persons of interest, including missing persons, exploited children, or criminal suspects.[105]

---

104. Walter L. Perry, Brian McInnis, Carter C. Price, Susan C. Smith, & John S. Hollywood. "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations." RAND Corp., 2013. https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf

105. "AI at the Edge: Motorola Solutions and Neurala to Work Together on Intelligence for Cameras." News media release, July 17, 2017. https://newsroom.motorolasolutions.com/news/ai-at-edge-motorola-solutions-and-neurala-to-work-together-on-intelligence-for-cameras.htm.

As the amount and variety of data involved in criminal investigations continue to grow, AI and machine learning are likely to take on added importance. "It is all going to come down to artificial intelligence, because no analyst can sift through the sheer volume of what investigators have access to and need," said Chief Lanier. "Artificial intelligence will become 100 times more effective than a person in sifting through and narrowing down data to what is important."

Video Analytics Technology Is Essential for Managing Huge Volume of Recordings

Another challenge facing police agencies is the volume of video they are collecting. As police departments increase their deployment of body-worn cameras and gain access to an ever-widening net of public and private security cameras, the amount of video data that departments will have at their disposal has the potential to overwhelm investigators.

Video analytics technology can help police agencies address this challenge by sifting through massive amounts of video to identify the pieces that are important to investigators. Video analytic software relies on algorithms to detect patterns and recognize particular behaviors, physical characteristics, or motion. Sgt. Michael Yu of the Montgomery County, MD Police Department noted that computer software can easily analyze many hours of video footage to identify the minutes in which motion is occurring. So if police are trying to find footage of a burglar entering a building, for example, "you can drive down the number of man hours required in an investigation to a fraction of the previous time," he said.

While many types of technology currently exist, law enforcement agencies are still learning how to harness the capabilities. And as the technology continues to advance, agencies will need to develop policies, procedures, and expertise to take full advantage of video analytics. If implemented carefully and thoughtfully, video analytics software has the potential to drastically change how investigators and crime analysts look at crimes and how they manage crucial video evidence.

Real-Time Crime Analysis Speeds Police Response

Participants at the *Critical Issues* meeting also noted that real-time crime and data analysis will play an even larger role in criminal investigations in the future. "Real-time analysis is essential in solving homicides and other crimes, so moving forward, our investigative units are going to have to work better with real-time crime centers," said Chief Inspector Cynthia Dorsey of the Philadelphia Police Department.

For example, the Chicago Police Department has created Strategic Decision Support Centers (SDSC), which fuse "geographic-specific, real-time data, such as crime information, video surveillance, and gunshot detection, into a

single platform for analysis."[106] The department has placed SDSCs in several of Chicago's high-crime police districts to collect and analyze data in real time, and then dynamically deploy resources to address crime problems as they arise. The SDSCs play a role in investigating crimes as they occur and preventing future crimes of the same type in that community.

Chicago Police Deputy Chief Steve Caluris offered an example of how real-time crime analysis has improved police operations. "Earlier today, my team got an alert that a gang member posted, 'Just rode past the police, 40 in my hand. Come and get me,'" Deputy Chief Caluris said. Within 15 minutes, crime analysts were able to ascertain information about the individual's identity, as well as license plate and vehicle registration information. Armed with that information, patrol officers in the district were able to stop the suspect and confiscate his gun. "If we can operate in real time like that, we're going to hit home runs," Caluris said. "We don't have the luxury of taking a lot of time to respond to threats, especially those on social media."

106. "Police Department Announces Expansion of Predictive Technology in Chatham and Auburn Gresham." City of Chicago, Office of the Mayor, news media release, July 25, 2017. https://www.cityofchicago.org/city/en/depts/mayor/press_room/press_releases/2017/july/PolicePredictiveTech.html

CONCLUSION

Catching Up with the Changes in How Crimes Are Committed: 9 Urgent Recommendations

THE CRIME STORY IN THE UNITED STATES TODAY IS A SCHIZOPHRENIC ONE. On one hand, violent crime and property crime rates, as measured by the FBI's Uniform Crime Reporting system (UCR), remain near record lows. Altogether, the UCR gathered 1,248,185 reports of violent crimes in 2016, plus 7,919,035 property crimes. Adjusted for population, these totals are roughly half of what they were in the early 1990s.[107]

This is a tremendous achievement by law enforcement agencies and their communities, to be sure.

However, in recent years, we've been hearing about a new "iceberg of crime," which is mostly below the surface, hidden from public view: crimes facilitated by computers, the internet, social media, and other new technologies. Identity theft. Ransomware and other online extortion attacks. Looting of bank accounts. Fraudulent credit card charges. Confidence games via email. Sexual exploitation conducted online. Investment schemes. Phony lotteries and sweepstakes targeting people on their computers. Phishing and similar schemes in which criminals impersonate legitimate banks or other financial institutions.

The "Peter the Great" case described in this report (see page 48) demonstrates how a new breed of criminals can commit their crimes anonymously, hidden in the "dark web" corners of the internet, causing havoc and death to victims thousands of miles away. A woman in Portland, OR died of an opioid overdose. Police in Portland, working with federal agents, found that the woman received the drug *by mail* from a dark web dealer who called himself "Peter the Great," who lived in Greenville, SC. They also found that the dealer had made nearly 10,000 transactions online, and that he was obtaining the drugs by mail from China. Investigators believe that the dealer may have been connected to at least a dozen other overdose deaths.

107. "2016 Crime In the United States." FBI. https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/tables/table-1

The Peter the Great case is one small piece of the United States' opioids epidemic, which resulted in the deaths of nearly 50,000 people in 2016.[108] And it is an entirely new type of drug trafficking, in which buyers and sellers never even see each other.

Unfortunately, the data we have on these new types of crime are crude. The FBI's Internet Crime Complaint Center estimates that only 15 percent of these crimes are reported. But the FBI estimates that these crimes number *in the millions per year.*

So the UCR tells us that we had 1.2 million violent crimes in 2016, plus 7.9 million property crimes. *But we also know that we have millions of additional crimes that are not being counted, and all indications are that these crimes are exploding in number.* The national UCR figures that indicate very low historical crime rates are not conveying the whole truth, because there are millions of crimes that are completely under the radar.

And so the traditional ways in which we measure crime, and investigate crime, are radically changing. But the policing field is not prepared for these changes. The 18,000 law enforcement agencies across the country, most of which are quite small, simply do not have the expertise and resources to undertake the major changes that are needed—in personnel, in training, and in the ways entire police departments are organized.

- We need a national commitment to undertaking changes.
- We need to hire police officers and analysts with new skills, and give them the continuous training they will need to keep up with constantly changing crime patterns. Detectives in particular will need to adjust how they do their jobs.
- We need better systems for gathering data about these new types of crime.
- We need a new national approach to who "owns" these crimes. These crimes usually involve multiple jurisdictions, because the victims and the perpetrators are often located far away from each other, and the crimes often involve financial institutions located somewhere else. The first step in solving a crime is deciding which police agency is responsible for solving it.
- We need to find a way of getting local law enforcement agencies up to speed, because the FBI and other federal agencies can investigate only a small fraction of these crimes.

Most importantly, we need a sense of urgency about this issue. The people committing these new types of crime, or committing old types of crime in new ways, realize that their risk of being caught is minuscule. Law enforcement agencies at all levels—federal, state, and local—must step up and take on new responsibilities for identifying these crimes and investigating them.

---

108. See "Drug overdose deaths skyrocketed in 2016 — and traditional opioid painkillers weren't the cause." *Vox,* Sept. 5, 2017. https://www.vox.com/policy-and-politics/2017/9/5/16255040/opioid-epidemic-overdose-death-2016

Following are nine recommendations that are based on the insights and perspectives of the nearly 200 law enforcement officials and subject matters experts who participated in PERF's conference in August 2017. These recommendations are not exhaustive, nor are they permanent. This list should be considered a mere starting point for placing law enforcement agencies in a better position to investigate, solve, and prevent crimes now and in the future.

9 Steps That Law Enforcement Agencies Should Take to Catch Up

1	**Evolve, quickly:** As crime continues to change, law enforcement agencies must change as well.

That means rethinking organizational models that reflect traditional "silos" such as organized crime, gangs, and narcotics. Instead, agencies should look at ways to integrate computer-focused criminal investigations, digital forensic science, and leading-edge technologies such as artificial intelligence and real-time crime analysis throughout their organizations. For example, units that investigate gangs should have financial crimes experts who are adept at finding the sources of gang funding, which are increasingly connected with cyber-crimes.

2	**Personnel:** Law enforcement agencies need to attract and retain personnel with the skills needed to operate effectively in this new environment.

Jim Collins, author of the business bestseller *Good To Great,* emphasizes the importance for organizations of hiring people who have the skills and attributes that are needed to perform their jobs—or as Collins expressed it, "getting the right people on the bus." For law enforcement agencies trying to keep up with changing patterns of crime and new investigative strategies, that means finding officers, detectives, and analysts who have the skill sets and capacity to understand and operate effectively in this new environment. In many cases, that will involve recruiting—and then working to retain—employees with specialized skills in technology, information retrieval, and data analytics.

3	**Continuous training:** Agencies need to continuously train and retrain their employees on issues related to computer-enabled crime.

Because almost every type of crime today can have a digital footprint, it is especially important that agencies train all of their personnel—patrol officers, crime scene technicians, and detectives—in how to recognize, handle, process, and manage digital evidence. And because criminals' strategies and tactics are constantly changing, law enforcement training must be a continuous process as well. Agencies should take advantage of the training offered by federal and

state agencies, as well as other organizations such as the National White Collar Crime Center.

4	**The "dark web":** As crimes like drug trafficking move from street corners to the internet, police agencies need to develop a working knowledge of the dark web, the use of crypto-currencies such as Bitcoin, and other online enablers of crime.

And as agencies begin to undertake dark web investigations, they need to thoroughly train their personnel in how to operate safely in the dark web, protecting their identities and avoiding potentially dangerous "blue-on-blue" encounters with other law enforcement agencies conducting similar investigations.

5	**Partnerships:** To strengthen their investigations of computer-enabled crime, local law enforcement agencies should form partnerships with federal, state, and other local agencies.

Partnerships with agencies such as the FBI, the U.S. Secret Service, and Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI) are especially important in dark web investigations and those involving data encryption. Local police agencies should form close working relationships with the U.S. Postal Inspection Service, because many criminal enterprises that operate on the dark web use the U.S. mail to transport illegal drugs, firearms, and stolen goods. USPIS has trained inspectors who can help local agencies conduct investigations that involve the mail.

6	**Small and mid-size agencies:** Regional efforts to combat computer-enabled crime should include small and mid-sized agencies.

Smaller jurisdictions are being disproportionately impacted by problems such as opioid addiction, which is increasingly connected with the dark web. Yet many of the police departments and sheriffs' offices in these communities lack the resources to initiate their own dark web investigations. These agencies should look to form compacts with larger departments and state agencies that can pool the resources and expertise needed to investigate a range of computer-enabled crimes. For example, in the San Diego region, more than 80 agencies are sharing licenses for expensive software that facilitates information-sharing, crime analysis, facial recognition, and other high-tech solutions. State and local agencies also are creating Regional Computer Forensic Labs and regional fusion centers to assist with digital forensic examinations.

7	**Legal and privacy issues:** Investigations in which law enforcement agencies seek information from technology companies can raise legal, privacy, and technical issues.

For example, technology companies often are unwilling, or in some cases claim to be unable, to unlock criminal suspects' smartphones, computers, or other

devices. Unfortunately, this situation will only get worse until law enforcement agencies can find a new working relationship with the private sector. At the moment, there are more problems than solutions for law enforcement agencies on this issue. In very important cases, such as the San Bernardino mass shooting incident in 2015, law enforcement agencies have paid private technical experts to unlock smartphones or other devices, but this can be very expensive and outside the reach of most departments. Participants at PERF's meeting reported mixed success in obtaining digital evidence from technology companies. For example, the Milwaukee Police Department has been able to use private-sector software to decipher highly coded data. Because some successes have been reported, law enforcement agencies should explore available options, including contracting with technical experts, engaging with the tech industry, and working with organizations like SEARCH, the National Consortium for Justice Information and Statistics. Police also can take leadership roles in seeking federal and state legislation that supports criminal investigations.

8	**Police must educate others:** Law enforcement leaders should educate the public and, when necessary, other criminal justice officials about the digital aspects of crime and criminal investigations.

Judges, prosecutors, and juries don't always seem to understand the basic elements of digital evidence, and how and why it is important to so many of today's criminal investigations. This problem can be acute among members of the public whose understanding of digital evidence is influenced by the entertainment media and the so-called "CSI effect," in which extremely advanced law enforcement technology is portrayed as working consistently, quickly, and flawlessly to identify suspects and make cases. Law enforcement leaders should work with subject matters experts and practitioners to educate the public and justice system personnel about computer-enabled crime, and about the advantages as well as the limitations of digital technology and evidence in their criminal investigations.

9	**Integration of new and old investigative techniques:** To be successful, law enforcement agencies need to integrate new technology-driven approaches to criminal investigations with traditional investigative techniques.

Very few crimes can be solved solely through technology-led investigations and digital evidence. Even the most complex of dark web investigations will likely require some measure of traditional investigative work. Police and sheriffs' departments need to develop investigative strategies that take advantage of, and coordinate, both types of approaches.

About the Police Executive Research Forum

THE POLICE EXECUTIVE RESEARCH FORUM (PERF) IS AN INDEPENDENT research organization that focuses on critical issues in policing. Since its founding in 1976, PERF has identified best practices on fundamental issues such as reducing police use of force; developing community policing and problem-oriented policing; using technologies to deliver police services to the community; and developing and assessing crime reduction strategies.

PERF strives to advance professionalism in policing and to improve the delivery of police services through the exercise of strong national leadership; public debate of police and criminal justice issues; and research and policy development.

The nature of PERF's work can be seen in the titles of a sample of PERF's reports over the last decade. Most PERF reports are available without charge online at http://www.policeforum.org/free-online-documents.

To learn more about PERF, visit www.policeforum.org.

- *The Revolution in Emergency Communications (2017)*
- *The Unprecedented Opioid Epidemic: As Overdoses Become a Leading Cause of Death, Police, Sheriffs, and Health Agencies Must Step Up Their Response (2017)*
- *The "Crime Gun Intelligence Center" Model: Case Studies of the Denver, Milwaukee, and Chicago Approaches to Investigating Gun Crime (2017)*
- *Hiring for the 21st Century Law Enforcement Officer: Challenges, Opportunities, and Strategies for Success (2017)*
- *ICAT: Integrating Communications, Assessment, and Tactics (2016)*
- *Guiding Principles on Use of Force (2016)*
- *Identifying and Preventing Gender Bias in Law Enforcement Response to Sexual Assault and Domestic Violence (2016)*
- *Advice from Police Chiefs and Community Leaders on Building Trust: "Ask for Help, Work Together, and Show Respect" (2016)*
- *Re-Engineering Training on Police Use of Force (2015)*
- *Gun Violence: Regional Problems, Partnerships, and Solutions (2015)*
- *Constitutional Policing as a Cornerstone of Community Policing (2015)*

- *Defining Moments for Police Chiefs (2015)*
- *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned (2014)*
- *Local Police Perspectives on State Immigration Policies (2014)*
- *New Challenges for Police: A Heroin Epidemic and Changing Attitudes Toward Marijuana (2014)*
- *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime (2014)*
- *The Police Response to Active Shooter Incidents (2014)*
- *Future Trends in Policing (2014)*
- *Legitimacy and Procedural Justice: A New Element of Police Leadership (2014)*
- *Compstat: Its Origins, Evolution, and Future in Law Enforcement Agencies (2013)*
- *Civil Rights Investigations of Local Police: Lessons Learned (2013)*
- *A National Survey of Eyewitness Identification Procedures in Law Enforcement Agencies (2013)*
- *An Integrated Approach to De-Escalation and Minimizing Use of Force (2012)*
- *Improving the Police Response to Sexual Assault (2012)*
- *2011 Electronic Control Weapon Guidelines (2011)*
- *Managing Major Events: Best Practices from the Field (2011)*
- *It's More Complex than You Think: A Chief's Guide to DNA (2010)*
- *Promoting Effective Homicide Investigations (2007)*
- *"Good to Great" Policing: Application of Business Management Principles in the Public Sector (2007)*
- *Managing a Multi-Jurisdiction Case: Identifying Lessons Learned from the Sniper Investigation (2004)*

In addition to conducting research and publishing reports on our findings, PERF conducts management studies of individual law enforcement agencies; educates hundreds of police officials each year in the Senior Management Institute for Police, a three-week executive development program; and provides executive search services to governments that wish to conduct national searches for their next police chief.

All of PERF's work benefits from PERF's status as a membership organization of police officials, who share information and open their agencies to research and study. PERF members also include academics, federal government leaders, and others with an interest in policing and criminal justice.

All PERF members must have a four-year college degree and must subscribe to a set of founding principles, emphasizing the importance of research and public debate in policing, adherence to the Constitution and the highest standards of ethics and integrity, and accountability to the communities that police agencies serve.

PERF is governed by a member-elected President and Board of Directors and a Board-appointed Executive Director.

About Motorola Solutions and the Motorola Solutions Foundation

MOTOROLA SOLUTIONS CREATES INNOVATIVE, MISSION-CRITICAL COMMUNICATION solutions and services that help public safety and commercial customers build safer cities and thriving communities.

Our solutions, including devices, infrastructure, software and services, help people be their best in the moments that matter. We serve public safety and commercial customers in industries including law enforcement, fire, emergency medical services, utilities, mining, manufacturing and education. Customers in more than 100 countries around the world depend on our radio networks and devices, as well as our managed and support services. We are also continuing our rich history of innovation by creating "smart public safety solutions," which are technology-driven software, systems and applications that provide critical intelligence to public safety users, improving safety and efficiency.

The Motorola Solutions Foundation is the charitable and philanthropic arm of Motorola Solutions. With employees located around the globe, Motorola Solutions seeks to benefit the communities where it operates. We achieve this by making strategic grants, forging strong community partnerships, and fostering innovation. The Motorola Solutions Foundation focuses its funding on public safety, disaster relief, employee programs and education, especially science, technology, engineering and math programming.

Motorola Solutions is a company of engineers and scientists, with employees who are eager to encourage the next generation of inventors. Hundreds of employees volunteer as robotics club mentors, science fair judges and math tutors. Our "Innovators" employee volunteer program pairs a Motorola Solutions employee with each of the nonprofits receiving Innovation Generation grants, providing ongoing support for grantees beyond simply funding their projects.

For more information on Motorola Solutions Corporate and Foundation giving, visit www.motorolasolutions.com/giving.

For more information on Motorola Solutions, visit www.motorolasolutions.com.

APPENDIX A:

Participants at the Critical Issues Meeting: The Changing Nature of Crime and Criminal Investigations

August 9, 2017, Washington, D.C.

Participants are listed alphabetically by the name of their department or agency. Participants' titles and affiliations are those at the time of the August 9, 2017 meeting.

Jody Weis
ACCENTURE

Assistant Chief Robert Huntsman
ALBUQUERQUE POLICE DEPARTMENT

Lieutenant David Saladin
ALBUQUERQUE POLICE DEPARTMENT

Detective Annette Saladin
ALBUQUERQUE POLICE DEPARTMENT

Commander Geoff Huff
AMES, IA POLICE DEPARTMENT

Detective Nicholas Ingram
AMTRAK POLICE DEPARTMENT

Captain Herbert Hasenpusch
ANNE ARUNDEL COUNTY, MD POLICE DEPARTMENT

Detective John Bamford
ARLINGTON COUNTY, VA POLICE DEPARTMENT

Chief Jay Farr
ARLINGTON COUNTY, VA POLICE DEPARTMENT

Deputy Chief Charles Penn
ARLINGTON COUNTY, VA POLICE DEPARTMENT

Chief Kyle Heagney
ATTLEBORO, MA POLICE DEPARTMENT

Colonel Alexander Jones
BALTIMORE COUNTY, MD POLICE DEAPARTMENT

Captain John McGann
BALTIMORE COUNTY, MD POLICE DEAPARTMENT

Lieutenant Michael Hill
BEVERLY HILLS, CA POLICE DEPARTMENT

Captain Mark Miner
BEVERLY HILLS, CA POLICE DEPARTMENT

Steven Edwards
BUREAU OF JUSTICE ASSISTANCE

Associate Deputy Director Cornelia Sigworth
BUREAU OF JUSTICE ASSISTANCE

Lieutenant Mike Warren
BURLINGTON, VT POLICE DEPARTMENT

Mark Nicholas
CAMDEN COUNTY, NJ POLICE DEPARTMENT

Chief Scott Thomson
CAMDEN COUNTY, NJ POLICE DEPARTMENT

Captain Richard Verticelli
CAMDEN COUNTY, NJ POLICE DEPARTMENT

Deputy Chief Joseph Wysocki
CAMDEN COUNTY, NJ POLICE DEPARTMENT

Captain Gregory Whitaker (ret.)
CHARLESTON, SC POLICE DEPARTMENT

Chief John Fitzgerald
CHEVY CHASE VILLAGE, MD POLICE DEPARTMENT

Deputy Chief Steven Caluris
CHICAGO POLICE DEPARTMENT

Detective Patricia Dalton
CHICAGO POLICE DEPARTMENT

Frank Fernandez, Assistant City Manager, Director of Public Safety
CITY OF CORAL GABLES, FL

Chief Daniel Slaughter
CLEARWATER, FL POLICE DEPARTMENT

Lieutenant Jessie Medina
CORAL GABLES, FL POLICE DEPARTMENT

Assistant Chief Jason Rodriguez
DALLAS INDEPENDENT SCHOOL DISTRICT POLICE DEPARTMENT

Captain Jennifer Krosschell
DAYTONA BEACH, FL POLICE DEPARTMENT

Sergeant Sylvan Altieri
DC METROPOLITAN POLICE DEPARTMENT

Assistant Chief Michael Anzallo
DC METROPOLITAN POLICE DEPARTMENT

Lieutenant Troy Jessup
DC METROPOLITAN POLICE DEPARTMENT

Major Cornelius Yarbro
DEKALB COUNTY, GA POLICE DEPARTMENT

Executive Director Christian Kervick
DELAWARE CRIMINAL JUSTICE COUNCIL

Deputy Director Scott McLaren
DELAWARE CRIMINAL JUSTICE COUNCIL

Chief of Staff H. Tracy Williams III
DEPARTMENT OF THE ARMY, OFFICE OF THE PROVOST MARSHAL GENERAL

Acting Site Director Michael Ferguson, Sr.
DHS, FLETC

Assistant Director George Kovatch
DHS, FLETC

Deputy Director Thomas Brandon
DOJ, ATF

Assistant Director
Michael Gleysteen
DOJ, ATF

Assistant Director
James McDermond
DOJ, ATF

Assistant Director
Christopher Shaefer
DOJ, ATF

Program Manager John Wells
DOJ, ATF

Deputy Assistant Administrator
Frederick Smith
DOJ, DEA

Section Chief Thomas Walden
DOJ, DEA

Brett Chapman
DOJ, NIJ

Advisor Joe Heaps
DOJ, NIJ

Chief Rod Knecht
EDMONTON, AB POLICE SERVICE

Chief Quovella Spruill
ESSEX COUNTY, NJ PROSECUTOR'S OFFICE

2nd Lieutenant Brian Gaydos
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Lieutenant James Krause
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Major Richard Perez
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Major Christian Quinn
FAIRFAX COUNTY, VA POLICE DEPARTMENT

Captain Craig Buckley
FAIRFAX, VA POLICE DEPARTMENT

Chief Carl Pardiny
FAIRFAX, VA POLICE DEPARTMENT

Captain James Nolette
FAYETTEVILLE, NC POLICE DEPARTMENT

Rachael Songalewski
FAYETTEVILLE, NC POLICE DEPARTMENT

Supervisory Special Agent
Raymond Adams
FEDERAL BUREAU OF INVESTIGATION

Gregory Massa
Acting Section Chief/Assistant
Special Agent in Charge
FEDERAL BUREAU OF INVESTIGATION

Assistant Section Chief
Albert Murray
FEDERAL BUREAU OF INVESTIGATION

Kerry Sleeper
Assistant Director, Office of
Partner Engagement
FEDERAL BUREAU OF INVESTIGATION

Stacy Stevens
FEDERAL BUREAU OF INVESTIGATION

Erin Black, Student Intern
FEDERAL BUREAU OF INVESTIGATION,
DIGITAL EVIDENCE FIELD OPERATIONS UNIT

SSA Susan Ellis
FEDERAL BUREAU OF INVESTIGATION,
DIGITAL EVIDENCE FIELD OPERATIONS UNIT

Megan Lewis, Student Intern
FEDERAL BUREAU OF INVESTIGATION,
DIGITAL EVIDENCE FIELD OPERATIONS UNIT

SSA Unit Chief Karen Nester
FEDERAL BUREAU OF INVESTIGATION,
DIGITAL EVIDENCE FIELD OPERATIONS UNIT

Unit Chief Donna Gregory
FEDERAL BUREAU OF INVESTIGATION, IC3

Captain Anthony Ferrara
GAINESVILLE, FL POLICE DEPARTMENT

President Rick Neal
GOVERNMENT STRATEGIES ADVISORY GROUP

Captain Howie Thompson
GREENVILLE, SC POLICE DEPARTMENT

Chief Terry Sult
HAMPTON, VA POLICE DIVISION

Section Chief Matt Wright
ICE/HOMELAND SECURITY INVESTIGATIONS

Special Agent Paul Criswell
ICE/HOMELAND SECURITY INVESTIGATIONS

Special Agent Guy Gino
ICE/HOMELAND SECURITY INVESTIGATIONS

Senior Researcher
Donna Lindquist
IIR

Director of Training Josh Bronson
INTERNATIONAL ASSOCIATION OF CAMPUS
LAW ENFORCEMENT ADMINISTRATORS

Project Coordinator Joseph Marcus
INTERNATIONAL ASSOCIATION OF
CHIEFS OF POLICE

Chief Michael Yankowski
LANSING, MI POLICE DEPARTMENT

President Ronald Hosko
LAW ENFORCEMENT LEGAL DEFENSE FUND

Lauri Stevens
LAwS COMMUNICATIONS

Captain III Charles Hearn
LOS ANGELES POLICE DEPARTMENT

Deputy Chief Robert Fincher
MARTINSVILLE, VA POLICE DEPARTMENT

Deputy Director Mary Ward
MARYLAND DEPARTMENT OF PUBLIC SAFETY
AND CORRECTIONAL SERVICES

Captain David Gill
MESQUITE, TX POLICE DEPARTMENT

Sergeant James Gunter
METHUEN, MA POLICE DEPARTMENT

Captain Kristopher McCarthy
METHUEN, MA POLICE DEPARTMENT

Lieutenant Michael Pappalardo
METHUEN, MA POLICE DEPARTMENT

Chief Joseph Solomon
METHUEN, MA POLICE DEPARTMENT

Chief Steve Anderson
METROPOLITAN NASHVILLE
POLICE DEPARTMENT

Lieutenant Mitch Fuhrer
METROPOLITAN NASHVILLE
POLICE DEPARTMENT

Captain Jason Reinbold
METROPOLITAN NASHVILLE
POLICE DEPARTMENT

Lieutenant Joseph Kluh
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY POLICE DEPARTMENT

Deputy Chief Timothy Tyler
METROPOLITAN WASHINGTON AIRPORTS AUTHORITY POLICE DEPARTMENT

Deputy Chief Richard Clements
MIAMI BEACH, FL POLICE DEPARTMENT

Captain David Salazar
MILWAUKEE, WI POLICE DEPARTMENT

Inspector Thomas Stigler
MILWAUKEE, WI POLICE DEPARTMENT

Lieutenant Jeff Rugel
MINNEAPOLIS, MN POLICE DEPARTMENT

Superintendent Drew Evans
MINNESOTA BUREAU OF CRIMINAL APPREHENSION

Lieutenant Marc Erme
MONTGOMERY COUNTY, MD POLICE DEPARTMENT

Captain C. Thomas Jordan
MONTGOMERY COUNTY, MD POLICE DEPARTMENT

Captain Michael Ward
MONTGOMERY COUNTY, MD POLICE DEPARTMENT

Sergeant Michael Yu
MONTGOMERY COUNTY, MD POLICE DEPARTMENT

Tracy Kimbo
MOTOROLA SOLUTIONS

Daniel Cork
NATIONAL ACADEMY OF SCIENCES, ENGINEERING, AND MEDICINE PANEL ON MODERNIZING THE NATION'S CRIME STATISTICS

Executive Director Nelson Bunn
NATIONAL DISTRICT ATTORNEYS ASSOCIATION

Cathy Lanier
Senior Vice President/ Chief Security Officer
NATIONAL FOOTBALL LEAGUE

Policy Analyst Michael Garcia
NATIONAL GOVERNORS ASSOCIATION

Chelsea Hansen
NATIONAL LAW ENFORCEMENT MUSEUM

Jeff Lybarger
Director of Training
NATIONAL WHITE COLLAR CRIME CENTER

Tyler Wotring
NATIONAL WHITE COLLAR CRIME CENTER

Colonel Joseph Fuentes
NEW JERSEY STATE POLICE

Deputy Chief Michael Baldassano
NEW YORK CITY POLICE DEPARTMENT

Lieutenant Gregory Besson
NEW YORK CITY POLICE DEPARTMENT

Chief of Detectives Robert Boyce
NEW YORK CITY POLICE DEPARTMENT

Deputy Chief Joseph Dowling
NEW YORK CITY POLICE DEPARTMENT

Christopher Flanagan
NEW YORK CITY POLICE DEPARTMENT

Detective James O'Sullivan
NEW YORK CITY POLICE DEPARTMENT

Captain Francis Hileman
NEWPORT NEWS, VA POLICE DEPARTMENT

Major Frederick Fife
NJ ROIC

Deputy Director Daniel Mahoney
NORTHERN CALIFORNIA REGIONAL INTELLIGENCE CENTER

Director Joel Cohen
NSC

Major Dominick Pape
PALM BEACH GARDENS, FL POLICE DEPARTMENT

Assistant Chief Clinton Shannon
PALM BEACH GARDENS, FL POLICE DEPARTMENT

Captain Richard Reyes
PATERSON, NJ POLICE DEPARTMENT

Commander Douglas Steele
PEORIA, AZ POLICE DEPARTMENT

Lieutenant Jonathan Josey II
PHILADELPHIA POLICE DEPARTMENT

Chief Inspector Cynthia Dorsey
PHILADELPHIA, PA POLICE DEPARTMENT

Deputy Commissioner
Nola Joyce (ret.)
PHILADELPHIA, PA POLICE DEPARTMENT

Captain Roland Lee Jr.
PHILADELPHIA, PA POLICE DEPARTMENT

Lieutenant Robert Otto
PHILADELPHIA, PA POLICE DEPARTMENT

Inspector James Smith
PHILADELPHIA, PA POLICE DEPARTMENT

Senior Program Manager
Eddie Reyes
POLICE FOUNDATION

David Waltemeyer
Senior Law Enforcement Project Manager
POLICE FOUNDATION

Captain Mark Kruger
PORTLAND, OR POLICE BUREAU

Sergeant Chris Kenagy
PORTLAND POLICE BUREAU - HIDTA INTERDICTION TASKFORCE

Sheriff Melvin High
PRINCE GEORGE'S COUNTY, MD

Inspector General Carlos Acosta
PRINCE GEORGE'S COUNTY, MD POLICE DEPARTMENT

Major Kevin Hughart
PRINCE WILLIAM COUNTY, VA POLICE DEPARTMENT

Executive Director
Kristine Hamann
PROSECUTORS' CENTER FOR EXCELLENCE

Trevor Hewick
PROTOCOL SECURITY AGENCY

Chief Edgar Rodriguez
QUINNIPIAC UNIVERSITY

Dulani Woods
RAND CORPORATION

Lieutenant Robert Marland
RICHMOND,VA POLICE DEPARTMENT

Chief Howard Hall
ROANOKE COUNTY, VA POLICE DEPARTMENT

Lieutenant Richard Weger
SAN JOSE, CA POLICE DEPARTMENT

Sergeant Shane Anderson
SEATTLE, WA POLICE DEPARTMENT

Chief Todd Axtell
ST. PAUL, MN POLICE DEPARTMENT

Deputy Chief Paul Iovino
ST. PAUL, MN POLICE DEPARTMENT

Assistant Chief
Thomas Wuennemann
STAMFORD, CT POLICE DEPARTMENT

Data Scientist Eric Foster-Moore
THE LAB @ DC, EXECUTIVE OFFICE
OF THE MAYOR

Director of Public Safety
Laura Waxman
THE U.S. CONFERENCE OF MAYORS

Director Elizabeth Robert
THE WALT DISNEY COMPANY

President Tim Murphy
TRSS, LLC

Major Julie Harris
TULSA, OK POLICE DEPARTMENT

Deputy Chief Dennis Larsen
TULSA, OK POLICE DEPARTMENT

Deputy Director Steven Griffin
U.S. CUSTOMS AND BORDER PROTECTION

Chief CBP Officer
Stephen McConachie
U.S. CUSTOMS AND BORDER PROTECTION

Michael McCormick
U.S. CUSTOMS AND BORDER PROTECTION

Justin Matthes
Deputy Assistant Secretary
for Law Enforcement Policy
U.S. DEPARTMENT OF HOMELAND SECURITY

Analyst Lennea Mueller
U.S. DEPARTMENT OF HOMELAND SECURITY

Joshua Ederheimer
Senior Law Enforcement Advisor
U.S. DEPARTMENT OF JUSTICE

Senior Policy Advisor David Lewis
U.S. DEPARTMENT OF JUSTICE

Erica O'Neil
U.S. DEPARTMENT OF JUSTICE - CCSIPS

Investigator Yasrian Carvey
U.S. DEPARTMENT OF TREASURY -
INTERNAL REVENUE SERVICE

SIA Robert Blevins
U.S. POSTAL INSPECTION SERVICE

Postal Inspector C.
Brandon Callahan
U.S. POSTAL INSPECTION SERVICE

Postal Inspector Darryl Ford
U.S. POSTAL INSPECTION SERVICE

Paul Ashton
UK NATIONAL CRIME AGENCY

Chief Kim Dine (ret.)
UNITED STATES CAPITOL POLICE

Special Agent in Charge
Michael D'Ambrosio
CRIMINAL INVESTIGATIVE DIVISION,
U.S. SECRET SERVICE

Roseanna Ander
UNIVERSITY OF CHICAGO

James VanderMeer
UNIVERSITY OF CHICAGO

Professor Charles Wellford
UNIVERSITY OF MARYLAND

Matt Edmondson
USBP

Government Affairs Associate
Gabriel Shoglow
VERA INSTITUTE OF JUSTICE

Government Affairs Director
Hayne Yoon
VERA INSTITUTE OF JUSTICE

Deputy CSO Daniel Maloney
VERIZON

President/CEO Warren Loomis
VERSATERM CORPORATION

Sheriff Michael Chitwood
VOLUSIA COUNTY, FL

Captain Paul Kammerer
VOLUSIA COUNTY, FL SHERIFF'S OFFICE

Chief Robert Tracy
WILMINGTON, DE POLICE DEPARTMENT

CRITICAL ISSUES IN POLICING SERIES

Challenge to Change:
The 21st Century Policing Project

Exploring the Challenges
of Police Use of Force

Police Management of
Mass Demonstrations

A Gathering Storm—
Violent Crime in America

Violent Crime in America:
24 Months of Alarming Trends

Patrol-Level Response to a
Suicide Bomb Threat:
Guidelines for Consideration

Strategies for Resolving Conflict and
Minimizing Use of Force

Police Planning for an Influenza
Pandemic: Case Studies and
Recommendations from the Field

Violent Crime in America:
"A Tale of Two Cities"

Police Chiefs and Sheriffs
Speak Out on Local Immigration
Enforcement

Violent Crime in America:
What We Know About
Hot Spots Enforcement

Violent Crime and
the Economic Crisis:
Police Chiefs Face a
New Challenge – PART I

Violent Crime and
the Economic Crisis:
Police Chiefs Face a
New Challenge – PART II

Gang Violence: The Police Role in
Developing Community-Wide
Solutions

Guns and Crime: Breaking
New Ground By Focusing
on the Local Impact

Is the Economic Downturn
Fundamentally Changing
How We Police?

Managing Major Events:
Best Practices from the Field

Labor-Management Relations in
Policing: Looking to the Future
and Finding Common Ground

How Are Innovations
in Technology
Transforming Policing?

Improving the Police Response
to Sexual Assault

An Integrated Approach to
De-Escalation and
Minimizing Use of Force

Policing and the Economic
Downturn: Striving for Efficiency
Is the New Normal

Civil Rights Investigations of
Local Police: Lessons Learned

The Police Response to
Active Shooter Incidents

The Role of Local Law Enforcement
Agencies in Preventing and
Investigating Cybercrime

New Challenges for Police:
A Heroin Epidemic and
Changing Attitudes Toward Marijuana

Defining Moments
for Police Chiefs

Re-Engineering Training
on Police Use of Force

Advice from Police Chiefs and
Community Leaders on Building
Trust: "Ask for Help, Work Together,
and Show Respect"

Guiding Principles on Use of Force

ICAT: Integrating Communications,
Assessment, and Tactics

The Revolution in
Emergency Communications



Police Executive Research Forum
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036
202-466-7820
www.PoliceForum.org

We provide progress in policing.

**We are grateful to the
Motorola Solutions Foundation
for its support of the
Critical Issues in Policing Series**

