IACP Summit Report

DATA, PRIVACY and PUBLIC SAFETY

A LAW ENFORCEMENT PERSPECTIVE ON THE CHALLENGES OF GATHERING ELECTRONIC EVIDENCE

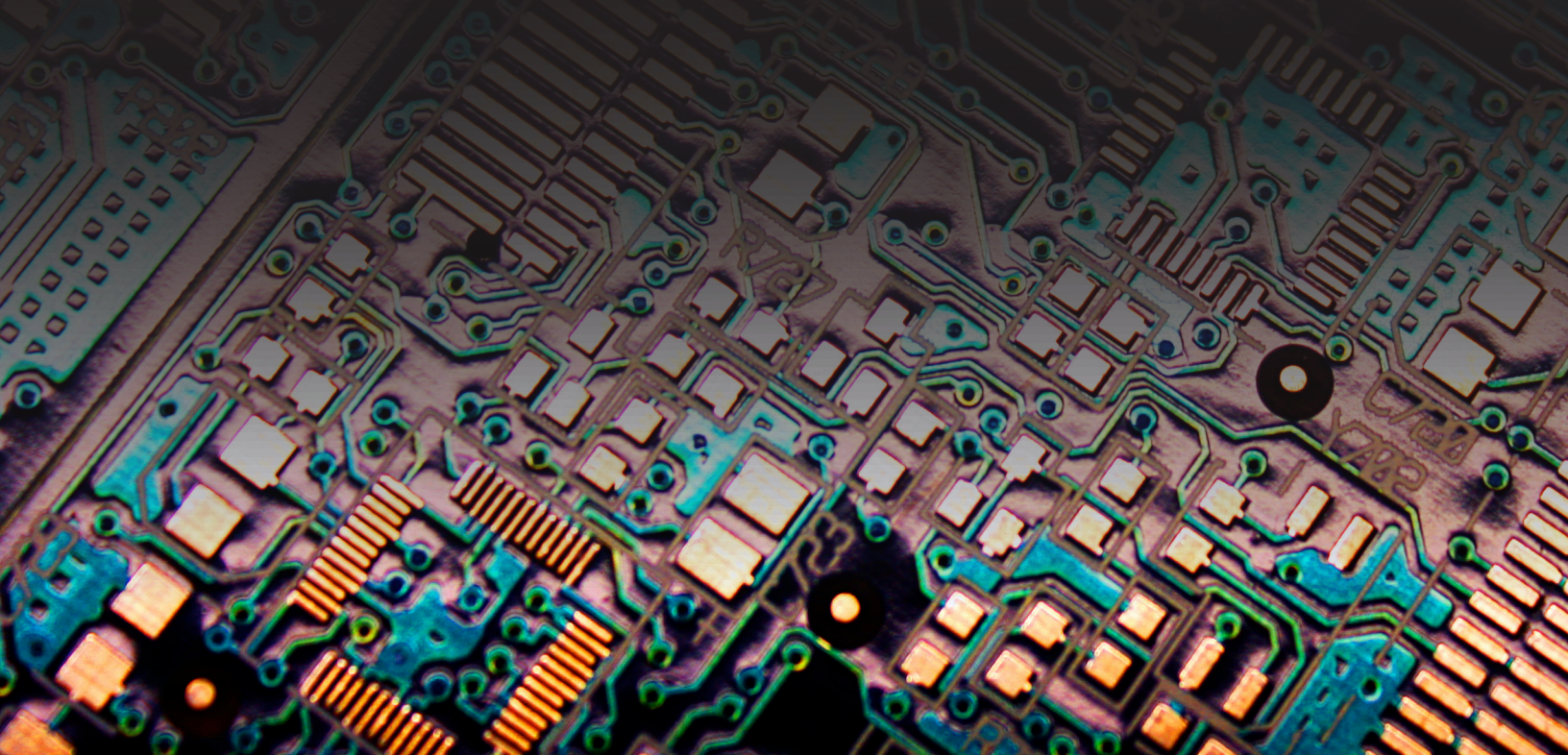

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Ubiquitous access to interconnected mobile devices and other advanced communications systems has transformed how we live, work, and communicate, enabling global communication with the touch of a smartphone screen. This expansion of interconnectedness has also provided a new tool of the criminal trade for criminals and created new challenges for law enforcement investigators. The issue of "Going Dark"—law enforcement's decreasing ability to lawfully access and examine digital evidence at rest and evidence in motion due to technical and non-technical barriers—is increasingly placing public safety at risk.

Historically, the impact that advances in technology had on law enforcement capabilities was moderated by industry's willingness and ability to comply with a law enforcement legal demand for access to evidence on a device or in a network. Historically, the manufacturer of a tablet or smartphone maintained a way to access a device even if the user could not. That access also prevented criminals from hiding data from law enforcement. With the proper legal authority, the police could require a manufacturer or service provider to furnish the key to unlock the device.

Recently, however, new technologies and strategies developed to advance network security are preventing law enforcement and justice agencies from executing lawful court orders to investigate criminal or terrorist incidents or to secure electronic evidence. Clear and sometimes insurmountable barriers to access of electronic evidence have been placed in the way of law enforcement seeking to identify suspects and protect communities from further crime. Those barriers to access include data encryption, outdated legislation, elevated proof requirements, cloud infrastructure, lack of data retention and preservation, and unreliable provider assistance.

Recognizing the growing challenges these issues represent for local, state, federal, and international law enforcement and criminal justice agencies, the International Association of Chiefs of Police (IACP) organized the Law Enforcement Summit on Going Dark in February 2015. The summit assembled a group of subject matter experts, including law enforcement executives and investigators, privacy experts, legal specialists, scholars and other professionals, to explore the nature of the challenges of Going Dark and to examine the technical, operational, legal, and policy issues that must be confronted in addressing these challenges. The summit also explored potential strategies and action steps to craft a balanced approach to privacy and public safety and to ensure lawful access to evidence at rest and in motion.

In this report, participants in the Law Enforcement Summit on Going Dark detail the technological and legal landscape surrounding the issue of Going Dark, they define the barriers to access faced by law

enforcement every day, and they outline the key ideas that their law enforcement peers should know when discussing the issue of Going Dark. Those themes are the following:

1. Continuing law-enforcement's long-standing commitment to individual liberty.
2. Recognizing that network security measures such as encryption are important, appropriate, and justifiable.
3. Adhering to Constitutional protections and time-honored, established legal process that guarantees judicial review and approval of search warrants is also critical.
4. Understanding that technology is evolving, and solutions are being developed that prevent the discovery and collection of information—potential evidence—from digital devices and communications systems even with a court order.
5. Knowing that the harms resulting from the inability of technology companies to comply with court-ordered surveillance warrants are not abstract; they have very real, tangible consequences in many criminal and national security investigations. The threat is real and it is already hindering the ability to keep the public safe.
6. Conveying that we are not seeking to expand the surveillance authority of government, but rather to ensure that evidence collection by lawful court order can be accomplished when authorized and needed.

They also outline seven concise recommended strategies and action steps necessary to move law enforcement and industry toward a balanced approach to 21st Century public safety, data and privacy. Those recommendations include the following:

1. Provide guidance and recommended strategies to address Going Dark.
2. Bring public awareness and transparency to the impact Going Dark has on public safety.
3. Create an electronic data and privacy policy framework.
4. Prepare an analysis of current legislation that relates to evidentiary collection of electronic data.
5. Work with domestic and international partners to continue dialogue about the effects of Going Dark.
6. Hold a national press day to educate the public about the public safety implications of Going Dark.
7. Focus on educating congressional and other policy leaders on Going Dark.

Law enforcement is committed to working collaboratively and in good faith with interested stakeholders to explore solutions to the Going Dark issue. We look forward to identifying approaches that protect privacy, while still allowing lawful access to stored data and electronic communications in order to prevent, investigate and solve crimes.

INTRODUCTION

> *"Law enforcement simply needs to be able to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations of serious crime and terrorism."*
>
> —Chief Richard Beary, IACP President[1]

In recent years, revolutionary changes in modes of electronic communication have transformed the way Americans live and work. Ubiquitous mobile phone and Internet communication through smartphones and other devices has shaped a society that can communicate globally with the touch of a screen. While this expansion of electronic communication continues to extend the reach of American trade and commerce globally and provides expansive opportunities for personal communication, it has also armed those who wish to harm others with new tools.

Law enforcement around the world are keenly aware of the ways in which criminals and terrorists leverage electronic communications technology to their advantage, including using the Internet to organize criminal conspiracies; to establish virtual communities to propagate sex crimes; to facilitate criminal trade of guns and drugs; to organize and promote global networks that commit crimes and terrorist acts on U.S. soil; and even to execute sophisticated attacks that breach critical information systems and infrastructure, steal corporate intellectual property, and access the sensitive personal information of millions of Americans.

More importantly, the expansion of communications technology means that crime scenes—the ones that state and local law enforcement respond to every day—are much more complex than ever before. Crime scenes from homicides, kidnappings, assaults, and incidents of domestic violence—crimes that impact thousands of victims, families, and U.S. communities annually—now more often than not, include digital communications evidence. Digital footprints left at the "scene" (which is no longer a localized crime scene, but a point that can be accessed from anywhere in the world through smartphones or computers) are the modern-day fingerprint that law enforcement uses to protect the public. Law enforcement needs access to this digital information to solve crimes, locate perpetrators, protect victims, and ensure prosecution. Americans expect that law enforcement will keep them safe from criminals or, at the very least, locate and prosecute those who victimize others.

---

[1] Beary, Richard, "Going Dark: Addressing the Challenges of Data, Privacy and Public Safety," President's Message, The Police Chief 82 (April 2015): 6. http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3673&issue_id=42015

At the same time, our nation's security requires secure networks to prevent unauthorized cyber access to critical infrastructure, data, and intellectual property. Insecure systems create holes in cyber security and render electronic assets vulnerable to myriad attacks from individuals or groups who can be located virtually anywhere in the world. These attacks create tangible consequences, including vulnerabilities in financial institutions, major retail chains, social networking sites, and even government agencies.[2] Exploiting these vulnerabilities can in turn enable criminal access to the personal information of millions of people around the world, leaving them open to identity fraud and other forms of victimization. The law enforcement community understands these consequences, and supports and encourages the use of innovative technology to secure networks.

New technologies and strategies developed to advance network security, however, can also prevent law enforcement and justice agencies from executing lawful court orders to investigate criminal or terrorist incidents, or to secure electronic evidence. Due to nearly universal support for efforts to use strong encryption and other technologies to secure cell phones, email, text messages, and other online communications and transactions, recent initiatives by industry to develop and deploy encryption and sophisticated tools to protect the privacy of their customers have created impenetrable barriers to complying with lawful court orders to provide access to digital evidence.

As FBI Director James Comey has noted,

> *"Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we lack the technical ability to do so."*[3]

Not only does law enforcement lack the technical ability to access communications and information pursuant to a lawful court order, but industry is also, *by design,* incapable of accessing or retrieving the information. Industry touts their security features as market differentiators, as noted on Apple's website which states:

---

[2] Major cyber security breaches have occurred at Target [http://krebsonsecurity.com/tag/target-data-breach/], Home Depot [https://corporate.homedepot.com/mediacenter/pages/statement1.aspx], and the Office of Personnel Management (OPM) [https://www.opm.gov/cybersecurity].

[3] James Comey, Director, Federal Bureau of Investigation. *Remarks on Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?* October 16, 2014. Brookings Institute, Washington, DC.

https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

"On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[4]

This inability to access digital communications data not only inhibits access to evidence in federal criminal and terrorism cases, but it is also keeping state and local law enforcement from being able to do their job. The ability of the police to build criminal cases is dependent on discovering facts and evidence that will identify the person(s) responsible for the crime. Technologies and strategies that keep them from accessing digital evidence when legally authorized are putting public safety at risk.

Recognizing the growing challenges these issues represent for local, state, federal, and international law enforcement and criminal justice agencies, the International Association of Chiefs of Police (IACP) organized the *Law Enforcement Summit on Going Dark* in February 2015. The summit assembled a group of subject matter experts, including law enforcement executives and investigators, privacy experts, legal specialists, scholars, and other professionals, to explore the nature of the challenges of Going Dark and to examine the technical, operational, legal, and policy issues that must be confronted in addressing these challenges. The summit was also designed to explore potential strategies and action steps in crafting a balanced approach to privacy and public safety.

"Going Dark" is a term used by law enforcement agencies to describe their decreasing ability to lawfully access and examine evidence at rest on devices and evidence in motion across communications networks. The rapid growth of new services and technologies means that an increasing amount of evidence that resides on criminals' computers and mobile devices is beyond the reach of law enforcement, evidence that law enforcement needs to investigate illegal activity and prosecute criminals.

Report Organization

This report is an overview of the Going Dark issue as discussed by meeting participants. It lays out the technological and legal foundation of the issue, and then provides a description of the barriers to access electronic communications and data that law enforcement faces every day, as well as a brief overview of the technology industry perspective. The report outlines the key "takeaways" or ideas for the chief executive regarding the issue of Going Dark, as well as suggested action items for the law enforcement community to pursue in response to Going Dark. A list of recommendations is outlined for

[4] Apple, *Government Information Requests*, http://www.apple.com/privacy/government-information-requests/.

moving forward in developing a balanced approach to solving the challenges inherent to balancing 21st Century data, privacy, and public safety.

UNDERSTANDING THE TECHNOLOGY & LEGAL FRAMEWORK OF GOING DARK

Charting the Technological Landscape

As noted above, the global technological landscape continues to evolve at an exponential pace. The processing speed and storage capacity of computers have continued to advance, doubling every 12–18 months, significantly reducing data storage costs. New computing paradigms, such as cloud computing,[5] offer mass storage at commodity pricing. Technology is fundamentally changing the way people communicate, shop, manage finances, organize their time, navigate the world, record memories, and work on a daily basis. However, this type of growth can exceed our ability to immediately comprehend the operational and privacy implications that surface as these technologies are integrated into daily life.

Increasingly, individuals and organizations rely on an expanding array of technologies, including computers, laptops, tablets, smartphones, electronic readers, GPS mapping and tracking devices, personal health monitoring devices (e.g., Fitbit, Jawbone, Apple Watch), digital cameras, flash memory devices, SD cards, USB drives, hard discs, backups, cloud storage (e.g., Dropbox, Google Drive, Box.Net, Amazon Cloud Drive), compact discs (CDs), digital video and Blu-ray discs (DVDs). Moreover, automation is insinuating itself into all manner of *things* with network connections embedded in everyday objects, such as homes, automobiles, televisions, refrigerators, electrical systems, clothing and personally worn healthcare devices, creating what is referred to as the Internet of Things (IoT). People can program their home to turn on lights, open the garage door, and change the interior temperature even before arriving home. They can manage email, texts, and calendars; place and receive telephone calls; get step-by-step directions to an address; and monitor their heart rate and blood glucose all while automatically sending reports to a medical care provider with a digital watch costing less than $400.[6]

Gartner projects that nearly 26 billion devices will be connected through the IoT by 2020.[7] In addition to owning these technology devices, people are using them to create and share a host of digital products, including word processing documents; spreadsheets; presentations (e.g., PowerPoint);

---

[5] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing,* (Gaithersburg, MD: National Institute of Standards and Technology), September 2011, p. 2, at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[6] Apple Watch. http://www.apple.com/watch/. http://www.diabetesforecast.org/2015/may-jun/glucose-monitoring.html?referrer=https://www.google.com/

[7] http://www.gartner.com/newsroom/id/2636073

electronic communications such as email messages, instant messages (IM), chats, and text messages; web-browser history; digital media such as pictures, audio recordings, and video files; and configuration and activity logs. Each of these technologies and products capture, record, create, transmit, and/or generate volumes of data.

Leveraging Data

Data may be *real data*, such as the specific content of an email, text message, or voice call, or *metadata*, which is information about information. Examples of metadata include date, time, and location (GPS coordinates) of where and when the device was used and has been or where transactions were created, such as where a photo was taken, a sale was made, and a call was initiated, as well as information about the technological device that was used.[8]

Industry utilizes this data and metadata—often referred to as *digital breadcrumbs*[9] *in the private sector*—to assist developers and technology companies in gathering detailed information on how people use their equipment and applications. Capturing these digital breadcrumbs also reflects vastly profitable business models that track consumer interests and precisely target marketing strategies and advertising campaigns based on those interests. Recognizing the growing privacy implications surrounding industry's use of digital breadcrumbs created by multiple devices many people carry, and to better understand them, the Federal Trade Commission (FTC) is organizing a workshop on cross-device tracking for marketing and advertising in November 2015 to better understand those implications.

> *"It's not that device-tracking is a new practice, but the number of devices each person uses has significantly increased over time, creating lucrative opportunities for marketers to learn even more about web browsers' habits. Now, it's possible to watch users browse for vacation destinations on their iPads, buy a weekend in the country on their desktop and then drive there using their cell phone's GPS. That kind of detailed consumer picture is worth a lot of money if you're [sic] job is finding out what people are interested in with an eye toward selling them something they'll entertain buying."*[10]

Law enforcement did not ask that service providers create these systems and capabilities, but now that they exist, they have become another place where evidence of crime might be found. Law

---

[8] National Information Standards Organization (NISO), *Understanding Metadata,* (Bethesda, MD: NISO Press, 2004).

[9] http://postalmag.com/blog/new-scanners-leave-digital-breadcrumbs-for-tracking-carriers/. Evan I. Schwartz, "Finding Our Way with Digital Bread Crumbs," *MIT Technology Review,* August 18, 2010, at http://www.technologyreview.com/news/420277/finding-our-way-with-digital-bread-crumbs/

[10] International Association of Privacy Professionals (IAPP), *The Privacy Pitfalls of Cross-Device Tracking,* September 30, 2015, at https://iapp.org/news/a/the-privacy-pitfalls-of-cross-device-tracking/

enforcement's goal has always been to lawfully gather as much of the available evidence as possible in order to ensure that justice is done, and some of these breadcrumbs become evidence. "Evidentiary breadcrumbs" represent important potential leads in criminal investigations, and are sometimes highly relevant to civil and criminal litigation.[11]

Homicide of Brittney Mills
Baton Rouge, Louisiana
April 24, 2015

"Baton Rouge detectives can't get into murder victim Brittney Mills' iPhone, which they hope holds clues to a killing that so far has stumped them.

….

Those who support strong encryption claim it prevents crime, specifically hacking, and protects personal property. Apple and other players in the tech industry say the encryption upgrades made to their software mends the trust they had with international companies that was damaged during the Snowden leaks.

Critics of the upgraded encryption argue that while privacy is important, law enforcement needs legal access to encrypted phones when an investigation requires it. Criminals, like the one who shot Mills, go free when vital clues remain locked away on digital devices, they say.

….

Mills, 29, and eight months pregnant, was fatally shot April 24 at her Ship Drive apartment. Authorities believe Mills opened the door for someone who wanted to use her car and was shot when she refused. Doctors delivered her son, Brenton Mills, who died a week later .

Investigators said the shooter likely was someone Mills knew. They have looked to her cellphone for evidence, but her iPhone uses iOS8 software that blocks anyone without the pass code.

IPhone owners can choose to use Touch ID, which unlocks the phone with the owner's fingerprint, but Mills used only a pass code, Moore said.

Apple allows only a few consecutive pass code guesses before it returns the phone to factory settings — with none of the user's information on it.

Moore said investigators are increasingly encountering problems with [this type of] encryption. On several occasions, police have tried to search for information about drug dealers from the phones of people who fatally overdosed but did not know the access codes, he said.

Sgt. Brian J. Blache, of the East Baton Rouge Sheriff's Office, said as more people use cellphones for everyday tasks, the information stored in them will be increasingly useful.

About 90 percent of the Sheriff's Office cases involves some type of cellphone or computer analysis, Blache said.

If nothing can be extracted from a cellphone, Blache said, the Sheriff's Office will lock it up in evidence with the hope that technology down the line will allow them to open it later."

Source: *http://theadvocate.com/news/13122948-123/phone-codes-issue-for-police*

[11] See, e.g., Kashmir Hill, "Fitbit data just undermined a woman's rape claim," June 29, 2015, at http://fusion.net/story/158292/fitbit-data-just-undermined-a-womans-rape-claim/; Neda Shakoori, *Wearable Technology: A Perfect Fit For Litigation,* August 21, 2014, at http://www.mcmanislaw.com/blog/2014/Wearable-Technology-A-Perfect-Fit-For-Litigation; Kashmir Hill, "Google Glass Will be Incredible for the Courtroom," *Forbes Tech,* March 15, 0213, at http://www.forbes.com/sites/kashmirhill/2013/03/15/google-glass-will-be-incredible-for-the-courtroom/

Data in Criminal Investigations

Law enforcement needs digital evidence to identify and locate suspects and to develop and prosecute criminal cases. That evidence may involve the contents of communications, or it may be event-related data, which refers to everything associated with a particular communication other than the content. This could be the time and date of a phone call, the location of the cell tower that a phone was used at a particular date and time, an IP session address or an IP destination address, or the web address of a site that a user contacts. In the context of a digital file (e.g., photo or video), metadata contains information about when the photo was taken, what device was used, and any other details that are embedded in the file structure within the digital file itself.

When discussing Going Dark, it is important to understand that law enforcement faces overlapping challenges with regard to digital evidence. The first concerns real-time court-ordered interception of "evidence in motion," such as phone calls, email, and live chat sessions. The second challenge concerns court-ordered access to evidence stored on devices, such as email, text messages, photos, and videos—or what is referred to as "evidence at rest." Both real-time communication and stored data are increasingly becoming encrypted; in some instances, by default.

Data in motion. Information that is "in transit," or *data in motion***,** includes real-time information such as phone calls, emails and chat sessions. In the past, law enforcement could access data in motion (when necessary for criminal investigation) with legal process—usually meaning monitoring a landline telephone or pager. As with physical data at rest, the technologies police used to get this information, with the appropriate warrant, was fairly simple, albeit time-consuming. Telephone companies assisted the police in capturing the dialed digits and in intercepting lawfully authorized conversations. Now, with the proliferation of mobile devices, a wide variety of communications services, and encryption, obtaining access to this information is becoming increasingly difficult.

Data at rest. Data stored in files—whether on paper or in electronic form—comprises data at rest. Data at rest includes emails, text messages, photos and videos stored on computers, cell phones, tablets, flash drives and other digital devices.[12] Data of this kind, found in both systems and devices, may contain an estimate of a geographic position that can help to locate a suspect or a victim, place a suspect at the scene of a crime, or imply a probable location associated with an entity having an estimated geographic position. Law enforcement has historically been able to access data at rest when needed with the assistance of service providers who are able to provide "exceptional access" to the device with a court order.

---

[12] Beary, Richard, "Going Dark: Addressing the Challenges of Data, Privacy and Public Safety," President's Message, The Police Chief 82 (April 2015): 6.
http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3673&issue_id=42015

Location information. Location information is data, either at rest or in motion, that pertains to the location of a particular communications device. It contains an estimate of a geographic position or implies a probable location associated with an entity.

Data containing location information is especially valuable electronic evidence, value that comes from three types of information that can be derived from each location record: (1) the place a device was when something happened, (2) the time it was there, and (3) association of that device with a particular actor. The location component can be precise, like A-GPS[13] data from a cell phone, or general, like the city or market area that a particular residential telephone number belongs to. Often it comes from mobile devices, but it can also come from installed trackers and other sources.

When and if location information is available by lawfully authorized access, an investigator may be afforded the opportunity to collect electronic information that can locate the victim of a crime, the perpetrator of a crime, tangible entities associated with a crime, a missing person, and/or a person requiring medical assistance. It can also include or exclude a person or tangible entity from an investigation and support or refute an alibi or alternate theory of the crime.

Data Retention and Preservation. In many criminal investigations, including murders, robberies, rapes, and organized crime, a suspect is only identified weeks or months after the crime has been committed. If the communications evidence related to that person has disappeared from a service provider's servers, the evidence is lost. If data is routinely retained for some period of time, law enforcement can identify historic linkages between stored communications data and offenses. These linkages begin to create a picture of how the crime occurred and who was involved so that law enforcement can apprehend and prosecute the suspect in an effort to protect others from becoming victims of the same offenders. For these reasons, retention and preservation of data by service providers is of concern to law enforcement.

Existing Legal Framework

To understand how and why law enforcement is legally and constitutionally able to access criminal communications data in specific cases, it is important to understand the law and the extensive checks, balances, and safeguards that frame it.

[13] Assisted Global Positioning System, a technology used by modern cell phones to determine a relatively precise location for the cellular handset (the phone). This is one way a network can identify the location of a mobile phone user who dials 911.

The Constitution

The Fourth Amendment to the United States Constitution grants citizens broad protection against the exercise of government power, couched in remarkably simple language:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*—U.S. Constitution Amendment IV

This language was included in the Bill of Rights as a rejection of the practice of using "general warrants" during British rule of the colonies. These writs were issued by a government official rather than a neutral magistrate, and they did not expire, allowing Crown tax enforcers to search whether or not they had an individualized reason to believe evidence was located within. The colonists possessed no right to stop these searches, and there was no appeal.[14] Out of the resulting frustration, the Fourth Amendment was born.

The framers of the Constitution understood that banning all government searches was equally impractical, rendering enforcement of criminal law impossible. The rule of law required a balance between protection and enforcement, privacy and security, liberty and safety. As a result, they sought to prevent only "*unreasonable* searches and seizures." The amendment itself contemplates authorization of a search based upon a warrant presented to and signed by a neutral magistrate or judge. Additionally, case law has developed over the years allowing for warrantless searches in certain cases, such as emergencies.[15] Where the law allowed a proper search, law enforcement was allowed to go further unimpeded in its pursuit of evidence.

Today, when law enforcement investigators seek access to electronic information *stored* (data at rest) on a device, such as a smartphone, or data in transit (data in motion), they are bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

A number of other legal standards are in place to more concisely define how and under what circumstances law enforcement can and should have access to digital communications and data.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III or the Wiretap Act)

In many cases, federal and state law impose additional statutory controls on electronic surveillance above and beyond the dictates of the Fourth Amendment. Generally speaking, in order for

---

[14] See Boyd v. United States, 116 U.S. 616, 624-25 (1886).

[15] See e.g. Brigham City v. Stuart, 547 U.S. 398, 403 (U.S. 2006); Illinois v. McArthur, 531 U.S. 326, 330-31 (2001).

law enforcement to conduct *real-time* electronic surveillance of the content of a suspect's communications (i.e., collect *content evidence in motion*), it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as Title III or the Wiretap Act) or an equivalent state statute. These laws authorize law enforcement to obtain a court order to conduct surveillance of wire, oral, or electronic communications when investigating certain enumerated felonies.[16]

Regardless of which statute governs it, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a federal district court judge must find:

- that there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;
- that alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and
- that there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

Wiretap laws often also require the approval of a supervising prosecutorial authority, authorize interception in carefully controlled increments, and require minimization of interception of non-evidentiary communications.

The Communications Assistance for Law Enforcement Act (CALEA)

Amidst major changes in the telecommunications industry in the 1990s, the government faced the issue of determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. Similar to the changing technology of today, law enforcement was increasingly unable to conduct intercepts of mobile voice communications. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994.

CALEA requires telecommunications companies (or "carriers") to develop and deploy intercept solutions to ensure that government organizations can intercept electronic communications when

[16] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 deals with wire line and oral conversation content but not electronic communications. Title I of The Electronic Communications Privacy Act (ECPA) deals with the contents of an electronic communication. For example, "The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications." See: https://it.ojp.gov/privacyliberty/authorities/statutes/1285

authorized by law. Specifically, CALEA requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as pen register information or dialing, signaling, and routing information). The Act does not, however, require the carrier to decrypt communications encrypted by the customer or by a particular application or device manufacturer.

Law enforcement, therefore, was able to provide a court order to a telecommunication carrier, the carrier would access, isolate, and route (real-time) all the intercepted calls associated with the subject of the investigation to the respective law enforcement agency. The agency would then monitor the conversations and conduct investigative activities based upon the intercepted information.

When CALEA was enacted in 1994, and the Internet was in its early years, Congress exempted "information services" from any CALEA obligation. In 2006, the Federal Communications Commission (FCC) issued a report and order expanding CALEA's coverage to include some of the newer communications services. However, CALEA was never updated to address information services, and most of the advanced communication services and technologies available today (Facetime, Skype, iMessage, Twitter, etc.) have no requirement to develop and maintain existing lawful intercept capability.[17]

Currently, no statutes, regulations, or further amendments to CALEA exist that mandate providers of information services or manufacturers of communication devices to develop or maintain any lawful intercept capability. As a result, many current communication service providers and device manufacturers today (those currently outside of CALEA, where compliance is not required) do not develop lawful intercept capabilities or retain meaningful communications content or records. They are unresponsive even when presented with a court order.

Electronic Communications Privacy Act of 1986 (ECPA)[18]

The Electronic Communications Privacy Act of 1986, commonly known as "ECPA," supplemented the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone

[17] FCC rule-making brought two emergent communications technologies under CALEA: (1) Facilities-based providers of any type of broadband Internet access service are subject to CALEA, including but not limited to wireline, cable modem, satellite, wireless, fixed wireless, and broadband access via power line. The legal argument focused on the "substantial replacement provision." (2) The FCC further concluded that CALEA applies to providers of "interconnected VoIP services." As defined in the VoIP E911Order, interconnected VoIP services include those VoIP services that (a) enable real-time, two-way voice communications; (b) require a broadband connection from the user's location; (c) require IP-compatible customer premises equipment; and (d) permit users to receive calls from and terminate calls to the Public Switched Telephone Network (PSTN).

[18] The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred to together as the Electronic Communications Privacy Act (ECPA) of 1986. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including the USA PATRIOT ACT, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

The hierarchical structure of the ECPA was designed to enable law enforcement agents to proceed with lawful requests for disclosures at the initial stages of an investigation, where little is known and nothing can be assumed, to a point probable cause can be established for more intrusive legal processes such as orders and search warrants. During the inception and earliest stages of an investigation, law enforcement investigations are bound to a criminal investigative timeline that inevitably proceeds apace. This uninvited mandate to move forward rapidly imposes a form of de-facto minimization on law enforcement officers. Therefore, from the very beginning of an inquiry, the information and evidence gathering strategies and tactics of investigators are intentionally designed to allow non-pertinent information to be identified, culled, and discarded swiftly.

Moving beyond the ECPA statute, law enforcement is lawfully able to collect other information that reveal an individual's location from third-party providers other than wireless phone carriers and smartphone platform vendors. For example, valuable and probative location information can be lawfully obtained from either license plate readers or transactional records, such as tollbooth, public transport, and credit card records. Additionally, this type of location information is collected and used by commercial entities for marketing and other revenue-generating activities.

Evidence and Legal Processes

Law enforcement access to electronic and digital evidence is strictly governed by the Constitution, statutory law, and cases decided by the courts, as described in the preceding section. Some of the current debate over regulation of law enforcement conduct centers on what level of proof investigators must have before they can access different kinds of information. This section describes the levels of proof and legal demands that investigators must satisfy in order to gain lawful access to search for evidence.

The first two levels of proof include reasonable suspicion and probable cause.

- *Reasonable suspicion* is a specific and objective basis for suspecting someone of criminal activity. Reasonable suspicion is understood to be more than a hunch, but less than probable cause.
- *Probable cause* is defined as facts and circumstances, along with reasonable inferences drawn from them, that would lead a reasonable person in the officer's position to believe that the fact at issue is probably true.

Both are lower standards of proof than the "preponderance of the evidence" standard (that it is more likely than not that a particular point is true) that governs the outcome in civil trials. All three fall below the requirement of proof beyond a reasonable doubt that must sustain a valid conviction in a criminal trial.

Modern investigators are confronted with a variety of legal demands throughout an investigation, each with its own level of proof and corresponding type of required response information.

- *Administrative subpoenas* are a low level of legal demand based on a law enforcement determination that records sought are relevant to an ongoing criminal investigation. The limits on this authority vary among federal and state agencies, but the common characteristic is that the authorization of a judge is not required.
- *Pen register orders* are a low level of legal demand based on a law enforcement statement of jurisdiction and relevance, and a judge's authorization. A pen register order, or a pen/trap order,[19] allows the collection of data evidence (but not content evidence) in motion.
- *Judicial subpoenas/court orders/2703(d) orders* are different types of an intermediate level of legal demand; a judge has to find reasonable suspicion to believe that the records sought are relevant to an ongoing criminal investigation. This level of demand is sometimes explained as a "nexus" or a showing of "specific and articulable facts" to the issuing court that the records are relevant; something less than probable cause.
- *Search warrants* are legal demands based on a showing of probable cause to a judge. A search warrant can be used to authorize a range of activities from the production of content evidence at rest in the possession of a service provider to the real-time determination of a cell phone's location.
- *Wiretap orders, T-III orders,[20] or intercept orders* are a higher-level court order issued by a judge after law enforcement demonstrates probable cause and meets certain extra requirements outlined in the wiretap statute. This allows for the collection of content evidence in motion; essentially, people talking or otherwise communicating in real-time. Sometimes called "probable cause plus," since it requires, probable cause plus the satisfaction of special conditions. The actual standard of proof is exactly the same as that required for a search warrant or other probable cause–based order.

[19] The term "pen register" properly refers to an obsolete piece of surveillance equipment that allowed registration and collection of outgoing calls from a particular phone. The companion device was called a "trap and trace," and it facilitated collection of the numbers that called in to a particular phone. The terms are now commonly used to refer to the practice of collecting event-related data on a particular communications stream.

[20] The use of the term "T-III" or "T3" to describe a communications intercept order is a reference to Title III of the federal Omnibus Crime Control and Safe Streets Act of 1968, which addresses electronic surveillance.

- *Emergency/Exigent Circumstances* trigger legal provisions that allow a service provider to disclose certain records without the immediate submission of legal process in response to a law enforcement demonstration that there is an immediate threat of death or serious physical injury. Note that the determination of what constitutes an emergency is currently left up to the service provider, not the law enforcement officer who needs the records. This can leave officers without emergency recourse in circumstances where the facts are concerning, but not immediately critical, such as a gradually elevating level of concern for a missing person. There are currently exceptions built into existing law that allows law enforcement to request electronic evidence in the possession of a third party without a formal legal demand when human life or safety hangs in the balance. These are referred to as emergency or exigent requests; the second term is derived from the "exigent circumstances" exception to the search warrant requirement.

It is helpful to have a basic understanding of the following legal concepts when talking about the standards for law enforcement access to digital evidence at rest and evidence in motion.

- *The third-party doctrine* holds that if an individual gives property over to a third party, they are manifesting a reduced expectation of privacy in that information. Thus, law enforcement would generally be required to obtain a search warrant to gather records in a person's home, but a subpoena might suffice for documents left with their bank or accountant.
- *The origin of the records* is also significant to some courts. Some would draw a distinction between records created in the normal course of business and records created solely based on a law enforcement legal demand. This theory would offer the business records a lower level of protection; this is really the third-party doctrine from a different perspective.
- *The "mosaic theory" of the Fourth Amendment* holds that a series of actions by law enforcement that don't amount to a search by themselves can rise to the level of a search (thereby requiring a search warrant) when they are collected together or looked at as a whole.

Collectively, these statutes and the cases interpreting them reflect a concerted congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several, sometimes competing, yet equally legitimate social interests: privacy, public safety, national security, and effective justice.

BARRIERS TO LAW ENFORCEMENT ACCESS TO ELECTRONIC EVIDENCE

Law enforcement's mission is to keep the public safe, to ensure national security and to protect communities by preventing and investigating criminal conduct, identifying the people who are

responsible for committing crime, and ensuring that they are successfully prosecuted so as not to re-offend. To accomplish that, investigators need access to evidence of criminal activity wherever it is located, whether it is in physical, testimonial, biological, circumstantial, or digital form.

A significant percentage of communications content evidence and related data evidence have shifted *from* face-to-face, telephonic, cellular, or text-message transport *to* Internet-based communications and remote storage. This evidence is becoming inaccessible to law enforcement because of barriers to access or obstacles that law enforcement faces in collecting digital and communications evidence. Barriers to access can be technological, such as encryption, lack of data retention, and technological complexity or they can be non-technological, such poor response times to legal demands or heightened legal burdens. With these changes, law enforcement's ability to protect the public is diminishing. Even armed with proper judicial authorization, law enforcement is increasingly not able to detect, locate, identify, isolate, intercept, or access many criminal communications or critical evidence—it is Going Dark.

Barriers to Access

This section outlines barriers to access of electronic evidence as discussed during the summit.

1. Outdated Legislation Regarding Access to Evidence in Motion.

Today, the ability of law enforcement to conduct lawful intercepts on advanced communications services is a critical tool of public safety. As was outlined above, many of the existing statues governing access to evidence at rest and evidence in motion have been outpaced by technology and need to be updated in a way that addresses privacy *and* public safety concerns.

2. Data Encryption and Evidence at Rest.

Further complicating the landscape is the deployment of encryption technology by communication service providers (e.g., Snapchat and WhatsApp) and device manufacturers (e.g., Apple and Google). Currently, there exists no prohibition in the United States restricting the use of any encryption algorithm or key length (e.g., 256 bit) to secure one's communications or stored information. In fact, given the cyber threats that exits today, individuals are encouraged to use strong encryption technology to protect their personal and financial information.

Recently, technology companies (Apple and Google, specifically) have begun to develop devices with "full-disk" encryption. This means that through software re-engineering, their operating systems do not allow anyone but the user (or those who have the user's password) to access the device or data on the device—not even the technology company itself. According to the Apple website,

> *"On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed*

under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[21]

To understand the significance of this development, consider that Apple and Google operating systems run on 94 percent of smartphones in the U.S.[22]

For law enforcement and crime victims, the ability to encrypt communications and stored information by criminals for the purpose of concealing criminal activity has proven to be a significant challenge. As an example, the inability to access communications and stored information on the phone of an individual who has kidnapped and is exploiting a child may severely restrict law enforcement from being able to effectively locate and extricate the victim and to apprehend the offender.

According to a New York Times Op-Ed piece written by the Manhattan District Attorney, "between October [2014] and June [2015], 74 iPhones running the iOS8 operating system could not be accessed by investigators for the Manhattan district attorney's office – despite judicial warrants to search the devices. The investigations that were disrupted include the attempted murder of three individuals, the repeated sexual abuse of a child, a continuing sex trafficking ring and numerous assaults and robberies."[23]

When law enforcement lawfully seizes a mobile device pursuant to a search warrant, there exists an increasing likelihood that the device and all the information stored on the device depicting criminal activity will be encrypted and therefore inaccessible to law enforcement. Given individuals' rights under the Fifth Amendment to the U.S. Constitution, defendants cannot be compelled to incriminate themselves (i.e., provide the password to law enforcement to unlock the device). As a result, law enforcement is often unable to gather critical evidence necessary to protect public safety.

3. Inability to Access Location Evidence: Elevating the Proof Requirement.

Under the Electronic Communications Privacy Act (ECPA), law enforcement has accessed stored historical location information by demonstrating to a court that reasonable suspicion supported by articulable facts relevant and material to a criminal investigation exists and merits an order to disclose the information sought. This standard of access is reasonable to apply during the initial stages of an

---

[21] Apple Privacy, Government Information Requests Page. Accessed on August 25, 2015 from http://www.apple.com/privacy/government-information-requests.

[22] comScore. "comScore Reports January 2015 U.S. Smartphone Subscriber Market Share." March 4, 2015. Downloaded on September 1, 2015 from https://www.comscore.com/Insights/Market-Rankings/comScore-Reports-January-2015-US-Smartphone-Subscriber-Market-Share.

[23] Vance Jr., Cyrus R. Francois Molins, Adrian Leppard, and Javier Zaragoza. "When Phone Encryption Blocks Justice." *The New York Times*, Opinion Pages. August 11, 2015.

investigation where few facts are known with certainty and the building blocks of probable cause are to be collected. Applying lower standards of proof to building blocks of probable cause like location evidence allows agents to pursue early investigative leads and "build up" to the use of more intrusive tools to obtain more sensitive information protected by higher access standards, such as the contents of communications.

Law enforcement does not wish to gather more location information than is required to meet the immediate needs of an investigation. Thus, applications bearing reasonable suspicion supported by articulable facts and relevant to a criminal investigation are intentionally limited in scope to the time and place of a crime or event and particular to the least number of possible suspects.

Recently proposed legislation, however, would require law enforcement agents to demonstrate a heightened standard for access in order to obtain location information. Under these proposals, an agent might access historical location information at rest or prospective location information in motion only if an order has been issued based on a showing of probable cause, a higher standard than has been required in the past.

Elevating the proof requirement for different types of evidence poses problems in the investigative process. Law enforcement can meet a probable cause standard of proof only by discovering, collecting, and logically assembling relevant facts, statements, and observations. Advocates seek to extend the level of protection offered to a person's home to more and more of the electronic evidence that they create. Any time the level of proof is elevated, it becomes more difficult and time-consuming to build a case, placing the safety of the public at increased risk.

4. Cloud Infrastructure.

"Cloud storage" refers to a service offered by companies that allows a user to store electronic information on equipment that is owned by the service provider and located outside of the user's residence or office. The question then becomes whether information stored on a cloud service should be afforded the same level of legal protection that applies to a residence or some lower standard.

Cloud storage also poses problems independent of the type of legal demand that can be used to obtain it. Consider investigators with a state Medicaid Fraud Control Unit who are executing a search warrant on the premises of a medical billing operation that they believe has defrauded the system of hundreds of thousands of dollars that are meant to guarantee the health and well-being of vulnerable citizens. If that business uses an array of cloud services to store its electronic records, then the evidence that the investigators need may well be on machines belonging to a series of different companies, physically located far from the search location.

5. Lack of Data Retention and Preservation.

Government access to stored communications records and tech-based records are governed by the Electronic Communications Privacy Act (ECPA),[24] specifically Title II of that statute, the Stored Communications Act. The law clearly defines when and under what authorities or circumstances "electronic communication services" and "remote computing services" may voluntarily disclose or be compelled to disclose stored wire and electronic communications, as well as transactional records. While the act addresses the compelled preservation of stored records, it is silent concerning the retention of communications data. However, the act does authorize the tactic of compulsory data preservation.

Because no statutory standard exists for record retention times,[25] the amount of time service providers choose to retain historical information about account holders is inconsistent and varies widely across the industry. These retention schedules are unregulated and changeable. One provider may elect to retain account information, transactional information, and message content for as long as their own operational policies and legal position deem necessary, while some service providers (such as a provider of non-contract prepaid services) claim not to retain any historical information at all. When the government uses lawful authorities to compel the production of retained records, results vary by company and are uneven at best.

The lack of a predictable industry-wide retention regime can thwart law enforcement efforts to protect the public. When service providers are not required to retain data, evidence becomes unavailable—even when government has a need and a lawful requirement. If records simply do not exist, legal requirements for access and decryption matter little. While law enforcement does not support storing data for longer than is useful, government's need for it to ensure public safety and the administration of justice should be considered as criteria for service providers' retention schedules.

6. Unreliable Provider Assistance:

Increased volume and complexity of the communications environment requires that law enforcement relies even more heavily on service providers to assist in providing lawfully authorized access to electronic communication and stored data. Historically, communications providers have readily provided that assistance to the criminal justice community.

In fact, legislation mandates technical assistance provision by service providers in legally authorized cases. The Wiretap Act, 18 U.S. Code Chapter 119, 2510–2522 ("Title III") includes provisions mandating such requisite technical assistance so that government is able to carry out activities

[24] More information on this legislation can be found in the "legal framework" section of this chapter.

[25] The amount of time a service provider must keep records it generates in the normal course of business.

authorized by the court. For example, Title III specifies that a service provider, landlord, or other person shall furnish [the government] with all technical assistance necessary to accomplish the interception.[26]

Additionally, as previously explained, CALEA was intended to provide regulatory and service provider assistance to law enforcement accessing switch-based telephone and mobile telephone communications. This assistance preserved the ability of telecommunication carriers and manufactures of telecommunication equipment to ensure the ability to perform lawful intercepts on their networks. Continued assistance in 2005 addressed diminished access and increased complexity through the FCC's CALEA Broadband Coverage Order. CALEA coverage was extended to two basic Internet-based services: facilities-based broadband Internet access and two-way interconnected VoIP (Voice Over Internet Protocol).

However, these laws have proved insufficient in keeping up with ever-increasingly complex technology, including Internet-based technology. While the expansion of CALEA in 2005 proved to be extremely helpful, it simply does not go far enough to cover the exponentially increasing use of Internet-based communications services such as email, social networking, Internet messaging, or peer-to-peer services. This has caused a gaping hole in law enforcement' ability to execute court orders related to Internet-based communications.

Even in situations where access to electronic communications is covered by law, and legal requirements are met by law enforcement, service providers are increasing reluctant and/or unable to comply in a timely, complete, and effective manner. Non-technical barriers frequently encountered by law enforcement during criminal investigations include, erratic intake of orders and subpoenas; delayed response or unpredictable timelines for response; inaccurate responses; incomprehensible or imprecise responses; and/or prohibitively expensive responses. Particularly in situations where subpoenas or other legal orders are issued and expediency is required to identify and stop further damage or victimization, these issues severely debilitate law enforcement efforts.

The digital age has and will continue to assist people in their everyday lives. However, the inability of law enforcement to legally access communications data through the legal processes explained above is a legitimate public safety concern. If not addressed via a policy, legislative and/or technology solution, criminals may be able to store information on their mobile devices or use Internet services that will be completely inaccessible to police, even when they are legally authorized to access the information contained on those devices or provided by that service.

[26] "Procedure for Interception of Wire, Oral, or Electronic Communications" https://www.law.cornell.edu/uscode/text/18/2518

WRONGFUL CONVICTIONS—SEARCHING FOR THE TRUTH

The gut-wrenching realities of wrongful convictions bare testament to law enforcement's need to access evidence that is both accurate and *unalterable.* Evidence that would substantially increase the accuracy of investigations is being lost as law enforcement loses its ability to gather data in an increasingly data-driven world.

The IACP National Summit on Wrongful Convictions was held in August 2013 and led to a report that listed recommendations that subject matter experts from the law enforcement, forensic science, academia, and the legal profession felt could greatly impact law enforcement's ability to arrest the right person and avoid wrongful convictions. At this summit, a working group focused on the capacity of technology and forensic science to enhance the quality of law enforcement criminal investigations and arrest decisions. Included among the recommendations in the report, *The Evolution of the Justice Culture: Preventing Wrongful Arrests, Prosecutions, and Convictions*, was Recommendation #26 that stated, "Law enforcement agencies should develop an ongoing plan to identify, assess, and invest in emerging technology that can enhance investigative quality and accuracy."

Data offers "witnesses without an agenda." Utilizing 21st Century technology would enable law enforcement to follow "the digital footprint" that would allow for accuracy and efficiency. Supreme Court Justice Samuel Alito stated that "no one imagined the scope" of the information-rich environment. It is this information that offers solid proof that can support confessions, location, and exonerations.

Understanding the Industry Perspective

As mentioned previously, in the past, service providers have assisted law enforcement with court orders by providing access to data at rest through what they call "exceptional access" to encrypted messaging applications. This means that, for data at rest, technology companies have been able to comply with court orders to access encrypted data on smartphones or other communications devices by decrypting the information in response to legal process. Recently, however, technology companies are implementing full-disk encryption of their operating systems in an effort, they claim, to better secure users' data on their devices. Full-disk encryption does not allow anyone but the user (or those who have the user's password) to access the device or data on the device—not even the technology company itself. So, there is no one, except the user, who has the "key" to provide access to data on the device.

For their part, the technology industry insists that allowing law enforcement to maintain their capabilities of exceptional access to stored data compromises privacy, costs excessive amounts of money, and renders America's communications and data vulnerable to intrusion.[27] In a recent report published by MIT on the subject, security experts cite three major arguments for discontinuing exceptional access to law enforcement. First, they state that providing this access to communications moves away from the industry best practice of working to make the Internet more secure. Second, they claim that it substantially increases the complexity of the system, creating more vulnerability. Third, the writers claim

[27] Abelson, Harold, et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." Massachusetts Institute of Technology. MIT-CSAIL-TR-2015-026. July 6, 2015. www.csail.mit.edu

exceptional access creates concentrated targets that could attract those looking to attack the system.[28]

These arguments give insight into the reasoning behind the need to develop technologies that protect against potential vulnerabilities in electronic communications and stored data. They do not, however, provide an understanding of the spirit of industry's reluctance and inability to assist law enforcement in its quest to access data that will help keep the public safe. The divergent perspectives and priorities make it clear that any solution to the issue of Going Dark will require the uninhibited, good-faith participation of both law enforcement and industry.

KEY TAKEAWAYS FOR THE CHIEF EXECUTIVE

> *"The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress….The core question is this: Once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime*."[29]—Director James Comey

Discussions at the Law Enforcement Going Dark Summit provided a number of key themes that all law enforcement executives should understand when discussing the issue of access to electronic evidence.

1. Recognizing and respecting the privacy rights of citizens is paramount.

During the Summit, participants discussed the challenges of Going Dark, and the delicate balance that must be struck between protecting the communities they serve and safeguarding individual privacy rights. American citizens have a reasonable expectation of privacy, including a right to communicate without unauthorized surveillance. This is a foundational piece of American democracy that is particularly vital in light of technology that continuously extends our ability to communicate. Law enforcement understands and respects this privacy, its legal merits, and constitutional foundation.

---

[28] Abelson, Harold, et al. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." Massachusetts Institute of Technology. MIT-CSAIL-TR-2015-026. July 6, 2015. www.csail.mit.edu

[29] James Comey, Director, Federal Bureau of Investigation. Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee. July 8, 2015. Washington, DC.

2. Network security measures such as encryption are important, appropriate, and justifiable.

Today, electronic communication is ubiquitous and a profoundly important part of our lives both as individuals and as a nation. With the saturation of mobile communications and data into every part of how we live and work comes new threats. Breaches of network security can result in threats to public safety and criminal access to private information, often resulting in fraud. Protection of electronic communications data (i.e., through encryption) is a required part of enabling safe and effective communication. Law enforcement supports and encourages "the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote overall safety."[30]

3. Adhering to Constitutional protections and time-honored, established legal processes to ensure judicial review and approval of search warrants is also critical.

Equally important to public safety are constitutional protections against unreasonable searches and seizures that government agents (e.g., police investigators) must abide by in every criminal investigation. Investigators seeking access to evidence in electronic form are bound by the mandates of the Fourth Amendment, which authorizes law enforcement to compel production of evidence in a variety of ways, based upon the degree of intrusion into a protected area. This range of choices, with a warrant based upon demonstration of probable cause to a neutral magistrate at the top, allows law enforcement to build a case by obtaining evidentiary records in layers. Law enforcement should have access to the building blocks of evidence that it needs whenever it meets the appropriate legal standard on this scale.

4. Technology is evolving, and solutions are being developed that prevent the discovery and collection of information—potential evidence—from digital devices and communications systems even with a court order.

Recently, new encryption technology that is prolific on smartphones used by the majority of Americans gives users sole control over access to the data (both data at rest and data in motion) on their smartphone. Law enforcement, even with the assistance of service providers, cannot gain access to this data with a court order. Technology companies have effectively designed their way out of assisting law enforcement by designing operating systems that do not allow them (or any third party, for that matter) access to a user's data.

[30] James Comey, Director, Federal Bureau of Investigation. Joint Statement with Deputy Attorney General Sally Quillian Yates Before the Senate Judiciary Committee. July 8, 2015. Washington, DC.

The rule of law requires a balance between protection and enforcement, privacy and security, liberty and safety. The challenge is the continual balance of privacy and public safety in the context of technological innovation.

5. *The harms resulting from the inability of technology companies to comply with court-ordered surveillance warrants are not abstract; they have very real, tangible consequences in many criminal and national security investigations. The threat is real, and it is already hindering the ability to keep the public safe.*

The more society relies on mobile technology to communicate and store information, the more likely it is that evidence resides on these devices. The consequences of terrorists' and criminals' use of electronic communications to execute criminal activity are real. Every day critical evidence necessary to solve crimes resides on smartphones, on computers, and in online communications.

However, even as the need for law enforcement to access electronic communications information increases, their ability to do so decreases. While criminals develop new and innovative ways to exploit electronic communications for their benefit, law enforcement encounters new barriers (some technical, some non-technical) to access the information they need to protect the public from those criminals. Sometimes, they are stopped entirely. It is far too easy for an unsophisticated person to put their communications beyond the reach of any lawfully authorized investigation.

Failure to address these challenges will result in fewer investigative leads, longer investigative timelines, diminished safety for Americans and a less effective justice system for victims of crime.

6. *We are not seeking to expand the surveillance authority of government, but rather to ensure that evidence authorized by lawful court order is accessible when needed.*

To be clear, the law enforcement community is not asking for new surveillance authorities above and beyond what is currently provided by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the electronic communications of all citizens. Law enforcement simply needs to be able to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations or serious crimes and terrorism.[31]

---

[31] Twelve Criminal Justice Associations. *Letter to The Honorable Kevin Yoder, U.S. Representative, Third District, Kansas Re: HR 699 – Updating the Electronic Communications Privacy Act (ECPA) and Reducing the Effects of Non-Technical Barriers on Lawful Access of Electronic Evidence.* July 6, 2015.

Homicide of Ray C. Owens
Evanston, IL
June 8, 2015

In June, Ray C. Owens, a father of six, was shot and killed in his car on a Monday afternoon in Evanston, IL, a suburb 10 miles north of Chicago. The Evanston police believe that the victim, Ray C. Owens, had also been robbed. There were no witnesses to his killing and no surveillance footage.

With a killer on the loose and few leads at their disposal, investigators in Cook County, which includes Evanston, were encouraged when they found two smartphones alongside the body of the deceased: an iPhone 6 running on Apple's iOS 8 operating system, and a Samsung Galaxy S6 Edge running on Google's Android operating system. Both devices belonged to Owens—not the killer. Both were passcode protected.

An Illinois state judge issued a warrant ordering Apple and Google to unlock the phones and share with authorities any data therein that could potentially solve the murder. When investigators served search warrants on Apple and Google to unlock the phones, the companies were unable to because both were using operating systems that were fully encrypted and had been password protected by the user. Apple and Google responded to the warrant—in essence that they could not—because they did not know the user's passcode, and therefore were incapable of accessing the devise.

According to Commander Joseph Dugan of the Evanston Police Department, investigators were able to obtain records of the calls to and from the phones, but those records did not prove useful. By contrast, interviews with people who knew Owens suggested that he communicated mainly through text messages—the kind that travel as encrypted data—and had made plans to meet someone shortly before he was shot.

To date, the homicide remains unsolved. The killer remains at large.

Source:
http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0

In a letter to U.S. Representative Kevin Yoder dated July 6, 2015, twelve of the nation's leading criminal justice associations, including the IACP, National Sheriffs' Association, and the National District Attorneys Association said, "While we support efforts to guarantee the privacy rights of all citizens, it is imperative that we ensure that law enforcement, with appropriate judicial supervision and approval, maintain its ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes."[32]

MOVING FORWARD: RECOMMENDED STRATEGIES AND ACTION STEPS

As law enforcement and criminal justice executives, it is critical that we take leadership roles in ensuring that law enforcement continues to have access to the evidence we need to protect the public. The issues associated with Going Dark are complex ones, and there is no one-size-fits-all strategy that will ensure progress. Rather, we must seek approaches that are developed and implemented

[32] Ibid.

collaboratively, addressing the legitimate, but competing concerns of all stakeholders, while acting with clarity on what is best for the nation.

Below is a list of recommended strategies and action steps for moving toward balanced solutions to the issue of Going Dark.

1. *Based on work accomplished at the summit, provide guidance and recommended strategies to address the issues that most hinder the ability of law enforcement to provide public safety as a result of barriers to access, such as encryption, to electronic evidence. This guidance should ensure consistency of messaging on these issues, and should include, but not be limited to issues such as the legal standard to access electronic information, regulation of industry retention standards, requirements for industry to react to lawful court orders in a timely manner, processes for industry to accept, request and order information and cost factors in producing legally required information.*
2. *Develop and implement a tracking process to bring public awareness and transparency to the impact Going Dark has on public safety. This tracking process should clearly identify cases that have resulted in harm to the public because of the inability of law enforcement to collect needed information from encrypted systems.*
3. *Create an electronic data and privacy policy framework for law enforcement, based on best policy and practices. This framework should offer guidance on such areas as policy development, training, and current case law pertaining to electronic data and privacy.*
4. *Prepare an analysis of current legislation that relates to evidentiary collection of electronic data. The analysis should include a comprehensive review of the Communications Assistance for Law Enforcement Act (CALEA), FCC rules and Electronic Communications Privacy Act (ECPA), and should include recommendations for legislative change that balances protecting the public and protecting the public's right to privacy.*
5. *Work with domestic and international partners to continue dialogue about the effects of Going Dark, and the need for solutions that are not only U.S.-based, but also an international solution. The IACP has the ability to supply the format and framework to engage the international community.*
6. *Coordinate a nationwide press day that will educate the public about the challenges of Going Dark, and being unable to obtain needed evidence in an encrypted world. Press will include specific examples of compromised public safety as the result of lack of access to electronic information.*
7. *Organize and host a briefing for congressional leaders, state legislative associations, national governors and others on the ways in which public safety is compromised as a result of Going Dark.*

CONCLUSION

Networks must be secure, but the law cannot allow safe havens for criminals.

While technology may change, our commitment to protecting the safety of communities and our constitutional traditions does not. The law enforcement mission to protect and defend Americans' lives, liberty, privacy, and quiet enjoyment of their property requires relentless pursuit of those who would deprive us of these rights.

In our ever-evolving world, long-term technical and legal solutions must be employed. Law enforcement is committed to working collaboratively and in good faith with interested stakeholders to explore solutions to the Going Dark issue. We look forward to identifying approaches that protect privacy while still allowing lawful access to stored data and electronic communications.

END NOTES

The International Association of Chiefs of Police (IACP)

The International Association of Chiefs of Police (IACP) is the world's largest association of law enforcement executives. Founded in 1893, the IACP has more than 23,000 members in more than 100 countries around the world. The IACP's mission is to advance professional police services; promote enhanced administrative, technical, and operational police practices; and foster cooperation and the exchange of information and experience among police leaders and police organizations of recognized professional and technical standing throughout the world. Additionally, the IACP champions recruitment and training of qualified persons in the police profession and encourages all police personnel worldwide to achieve and maintain the highest standards of ethics, integrity, community interaction, and professional conduct. To this end, the IACP prioritizes addressing, in an honest and open way, those issues that potentially cause harm to the profession of policing and to the ability to keep communities safe.

IACP Law Enforcement Summit on Going Dark: Balancing Public Safety, Data, and Privacy

Recognizing the growing challenges that the issues related to data, privacy, and public safety place on international, federal, state, and local law enforcement and criminal justice agencies, the IACP organized *the Law Enforcement Summit on Going Dark* in February 2015. The summit assembled a group of subject matter experts to explore the nature of the challenges faced; discuss technical, operational, legal, and policy changes to address these challenges; and develop recommended solutions and strategies to move toward crafting a balanced approach to privacy and public safety. Sixty affiliates from across the world, including law enforcement executives and investigators, privacy experts, legal specialists, scholars, and other professionals were invited to to share their knowledge and views on this complex issue.

Director James Comey of the Federal Bureau of Investigation opened the summit by presenting on the impact of Going Dark on federal law enforcement's ability to protect the homeland and solve crime. Participants were then broken down into three groups: Outreach and Messaging; the Law, Legislation, and Policy; and Technology. Facilitators for each group were tasked with promoting discussion among participants to come up with the most important challenges as well as a course of action in which to overcome those challenges. The three breakout groups reconvened to present their findings to the entire group.

GLOSSARY

Administrative subpoenas are a low level of legal demand based on a law enforcement determination that the records sought are relevant to an ongoing criminal investigation. The limits on this authority vary among different federal and state agencies, but the common characteristic is that the authorization of a judge is not needed.

Cloud storage refers to a service offered by companies that allows a user to store digital information on equipment that is owned by the service provider and located outside of the user's residence or office. The question then becomes whether information stored on a cloud service should be afforded the same level of legal protection that applies to a residence or some lower standard.

Communications evidence is a subset of electronic or digital evidence and is the product of people using technology to communicate (a conversation over a cell phone or an exchange of emails), or law enforcement using technology to collect communications (using a special microphone to intercept a conversation between two people standing in the same room, for example). Communications evidence, and in particular the legal standards that govern law enforcement access to it, can be better understood if it is thought of in terms of two sets of alternatives: the type of information (*content vs. data*) and the place where it is found (*at rest vs. in motion*).[33]

Content or **Content Evidence** is the substance of a communication, the part that conveys what you want the other person or people to know. It could be a written message, a telephone conversation, or an email.

Content in motion is content that, at the point of collection, is actively being exchanged by target systems, like e-mails or voice calls that are intercepted in real time, as they occur.

Data or data evidence (may also be called event-related data, or non-content Evidence— understood to be short for "communications event-related data") is everything associated with a particular communication other than the content. This could be the time and date of a phone call, the location of the cell tower that a phone used at a particular time, or the web address of a site that a user contacts.

Electronic Communications Privacy Act of 1986 (ECPA):

*Background***.** The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

General Provisions. The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.

[33] This is sometimes simplified to "data at rest" and "data in motion." When these terms are used in this way, they generally refer to communications content that is either in storage (at rest) or moving across a network (in motion).

Specific Provisions. The ECPA has three titles:

Title I of the ECPA, which is often referred to as the Wiretap Act, prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence. 18 U.S.C. § 2515.

> Exceptions. Title I provides exceptions for operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." 18 U.S.C. § 2511. It provides procedures for Federal, State, and other government officers to obtain judicial authorization for intercepting such communications, and regulates the use and disclosure of information obtained through authorized wiretapping. 18 U.S.C. § 2516-18. A judge may issue a warrant authorizing interception of communications for up to 30 days upon a showing of probable cause that the interception will reveal evidence that an individual is committing, has committed, or is about to commit a "particular offense" listed in § 2516. 18 U.S.C. § 2518.

Title II of the ECPA, which is called the Stored Communications Act (SCA), protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses. 18 U.S.C. §§ 2701-12.

Title III of the ECPA, which addresses pen register and trap and trace devices, requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace. The authorization order can be issued on the basis of certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the applicant's agency.

Electronic evidence in the broadest sense is any information stored on or created by technology. In the national debate that this document addresses, the main focus is evidence that is either proof of criminal activity (pictures, recordings, location information) or communications regarding criminal activity. Electronic evidence is generally found in two places: on devices, and in the possession of service providers. Evidence stored "in the cloud" is stored on devices that are maintained by a service provider rather than on premises controlled by an individual. Service providers are also one access point for a particular "communications stream," that is, the ongoing exchange of information from one party to a conversation to another.

Emergency/Exigent Circumstances trigger legal provisions that allow a service provider to disclose certain records without legal process in response to a law enforcement demonstration that there is an immediate threat of death or serious physical injury. Note that the determination of what constitutes an emergency is currently left up to the service provider, not the law enforcement officer who needs the records. This can leave officers without emergency recourse in circumstances where the facts are concerning, but not immediately critical, such as a gradually elevating level of concern for a missing person. There are currently exceptions built into existing law that allows law enforcement to request

electronic or digital evidence in the possession of a third party without a formal legal demand when human life or safety hangs in the balance. These are referred to as emergency or exigent requests; the second term is derived from the "exigent circumstances" exception to the search warrant requirement.

Evidence at rest is evidence (either content or non-content evidence) that is stored in some fashion, such as saved emails, text messages, or records of which phones a particular number called. It could be either content or data. "Event-related data evidence at rest" is also sometimes called "historical data" to distinguish it from communications evidence that is being collected in real time, as it happens.

Evidence in motion is evidence that is moving across a network in real time. It could be content or event-related data or both. "Event-related data in motion" is non-content transactional records that are being actively exchanged by target systems at the point of collection, like the time, date, and length of phone calls.

Full-Disk Encryption (FDE), also known as *whole disk encryption*, is the process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication to the FDE product. This means that operating systems do not allow anyone but the user (or those who have the user's password) to access the device or data on the device—not even the technology company itself.

Going Dark is a term used by law enforcement agencies to describe its decreasing ability to lawfully seize and examine stored data and to monitor criminal communications in the electronic age.

Judicial subpoenas/court orders/2703(d) orders are different types of intermediate level of legal demand; a judge has to find reasonable suspicion to believe that the records sought are relevant to an ongoing criminal investigation. This level of demand is sometimes explained as a "nexus" or a showing of "specific and articulable facts" to the issuing court that the records are relevant; something less than probable cause.

Location evidence is evidence that pertains to the location of a particular communications device, and by extension, the person using it. Location evidence is generally understood to be event-related data (as opposed to communications content), and it can be collected by law enforcement either at rest or in motion. Since it is not content (a status that some advocates would dispute), it is afforded less protection than content, but courts often offer location evidence a higher level of protection than other types of event-related data. These courts usually cite a sense that individuals have an unusually high privacy interest in location information and thus require more proof of criminality from law enforcement before allowing access.

Metadata is literally "data about data," and in the law enforcement context usually means the same thing as "data evidence" or "event-related data." In the context of an electronic or digital file like a picture or video, metadata contains information about when the picture was taken, what device was used, and any other details like that embedded in the file structure with the electronic file itself.

The "mosaic theory" of the Fourth Amendment holds that a series of actions by law enforcement that don't amount to a search by themselves can rise to the level of a search (thereby requiring a search warrant) when they are collected together or looked at as a whole.

Non-technological barriers to access are barriers to access to electronic or digital communications and data that include poor response times to legal demands or heightened legal burdens.

Pen register orders are a low level of legal demand based on a law enforcement statement of jurisdiction and relevance, and a judge's authorization. A pen register order, sometimes called a pen/trap order,[34] allows the collection of data evidence (but not content evidence) in motion.

Rule 41 is the rule in the Federal Rules of Criminal Procedure that governs the issuance of search warrants, including rules for obtaining and executing them.

Search warrants are legal demands based on a showing of probable cause to a judge. A search warrant can be used to authorize a range of activities from the production of content evidence at rest in the possession of a service provider to the real-time determination of a cell phone's location.

Technological barriers to access are barriers to access to electronic or digital communications and data that include encryption, lack of data retention, or technological complexity.

Third-party doctrine holds that if an individual gives property over to a third party, they are manifesting a reduced expectation of privacy in that information. Thus, law enforcement would generally be required to obtain a search warrant to gather records in a person's home, but a subpoena might suffice for documents left with their bank or accountant.

Wiretap orders, T-III orders,[35] or **intercept orders** are a higher-level Court Order issued by a judge after law enforcement demonstrates probable cause and meets certain extra requirements outlined in the wiretap statute. This allows for the collection of content evidence in motion; essentially, people talking or otherwise communicating in real time. Sometimes called "probable cause plus," since it requires, probable cause plus the satisfaction of special conditions. The actual standard of proof is exactly the same as that required for a search warrant or other probable-cause-based order.

[34] The term "pen register" properly refers to an obsolete piece of surveillance equipment that allowed registration and collection of outgoing calls from a particular phone. The companion device was called a "trap and trace," and it facilitated collection of the numbers that called in to a particular phone. The terms are now commonly used to refer to the practice of collecting event-related data on a particular communications stream.

[35] The use of the term "T-III" or "T3" to describe a communications intercept order is a reference to Title III of the federal Omnibus Crime Control and Safe Streets Act of 1968, which addresses electronic surveillance.

ADDITIONAL GOING DARK REFERENCE MATERIALS

1. "U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata" http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html

2. "Monitor Your Glucose With the Apple Watch" http://www.diabetesforecast.org/2015/may-jun/glucose-monitoring.html?referrer=https://www.google.com

3. "Finding Our Way with Digital Bread Crumbs" http://www.technologyreview.com/news/420277/finding-our-way-with-digital-bread-crumbs

4. Google search for what is the internet of things https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=what%20is%20the%20internet%20of%20things

5. Gartner search for Internet of things http://www.gartner.com/search/site/freecontent/simple?typeaheadTermType=&typeaheadTermId=&keywords=Internet+of+things

6. "The Hacker's New Toy: Smart Cars" https://www.7safe.com/research-and-insight/cyber-business-insight/detail/our-blog/2015/08/28/the-hacker-s-new-toy-smart-cars

7. "Cyber Business Insight" https://www.7safe.com/research-and-insight/cyber-business-insight

8. How Apple is trying to protect your privacy as its products get more personal https://www.washingtonpost.com/news/the-switch/wp/2015/09/29/apple-is-selling-targeted-ads-but-its-new-privacy-policies-show-why-its-thinking-different-about-tracking

9. Petition to the Obama administration to reject laws or mandates that would give law enforcement a way to unlock encryption https://www.savecrypto.org

10. "Going Dark: The Internet Behind the Internet" http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet

11. "Judge Rules Phone Passcodes Are Protected Information" http://www.wsj.com/article_email/judge-rules-phone-passcodes-are-protected-information-1443138209-lMyQjAxMTE1NDI3NTAyNjU5Wj

12. "The Privacy Pitfalls of Cross-Device Tracking" https://iapp.org/news/a/the-privacy-pitfalls-of-cross-device-tracking

13. "The Internet of Things" http://www.theinternetofthings.eu

14. "Better Internet for Kids" http://www.saferinternet.org/online-issues/parents-and-carers/mobile-phones

15. "Federal Appeals Court Set to Hear Microsoft 'Cloud' Case" http://bigstory.ap.org/article/c46af160cd9f460790bf81cf772ef1fd/federal-appeals-court-set-hear-microsoft-cloud-case

16. *Riley v. California*, 573 U.S. ___ (2014) http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

17. "Search Warrants for Digital Devices" http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3527&issue_id=102014

18. "Law Enforcement Grapples with iPhone's Enhanced Encryption" http://phys.org/news/2014-10-law-grapples-iphone-encryption.html

19. http://www.futureofprivacy.org/wp-content/uploads/SwireCrypto070715.pdf

20. "Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology" http://www.justice.gov/opa/file/767321/download

21. "Wiretap Report 2014" http://www.uscourts.gov/statistics-reports/wiretap-report-2014

22. "As FBI Fearmongers About 'Going Dark' because of Encryption, Actual Wiretaps Almost Never Run into Encryption" https://www.techdirt.com/articles/20150701/23344231523/as-fbi-fearmongers-about-going-dark-because-encryption-actual-wiretaps-almost-never-run-into-encryption.shtml

The International Association of Chiefs of Police

GOING DARK

Addressing the Challenge of Digital Encryption

February 10-11, 2015
44 Canal Center Plaza
Alexandria, VA

Hassan Aden
Director of Research and Programs
International Association of Chiefs of Police

Jacques Battiste
Supervisory Special Agent
Federal Bureau of Investigation

Ben Bawden
Principal and Founder
BrooksBawden LLC

Richard Beary
President
International Association of Chiefs of Police

Gwen Boniface
Deputy Executive Director
International Association of Chiefs of Police

Gregory Brazzle
Computer Science Engineer
U.S. Secret Service

Al Cannon
Sheriff
Charleston County Sheriff's Office

James Comey
Director
Federal Bureau of Investigation

John Conroy, Supervisor
Electronic & Technical Surveillance Unit
Montgomery County Poilice Department

Ryan Daugirda
Project Coordinator
International Association of Chiefs of Police

Anthony DiClemente
Deputy Assistant Director (retired)
Federal Bureau of Investigation

Matthew Fine
Supervisory Special Agent
Federal Bureau of Investigation

John Firman
Director of Strategic Partnerships
International Association of Chiefs of Police

Jenny Gargano
Development Coordinator
International Association of Chiefs of Police

Joseph Ghattas
Visiting Fellow
International Association of Chiefs of Police

Michael Gleysteen
Assistant Director
Bureau of Alcohol, Tobacco, & Firearms

Sarah Guy
Manager, Legislative and Media Affairs
International Association of Chiefs of Police

Louis Grever
Executive Assistant Director (retired)
Federal Bureau of Investigation

George Guzman
Unit Chief
United States Department of Homeland Security

Russell Hamill
Assistant Chief
Montgomery County Police Department

Randy Hansen
Detective
San Bernardino County Sheriff's Department

Steele Hays
Marketing Director
Wynyard Group

Amy Hess
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation

Jay Hoffman
San Bernardino County District Attorney's Office

Richard Hohl
Trooper
Pennsylvania State Police

Lindsay Hovis
Intelligence Analyst Supervisor
Pennsylvania State Police

Steven Jansen
Vice President
Association of Prosecuting Attorneys

Dave Johnson QPM
Director
National Technical Assistance Centre, London, England

Mark Keel
Chief
South Carolina Law Enforcement Division

Tom Kulpinski
Detective, Electronic Surveillance Unit
New Jersey State Police

Steve Lowenstein
Chief Inspector/ Attorney
United States Marshals Service

Josiah Landers
Director, Investigative Technology Center
Rockland County Regional Investigative Resource Center

Richard Littlehale
Assistant Special Agent in Charge
Criminal Investigation Division
Tennessee Bureau of Investigation

Mel Maier
Chief, Emergency Management Operations
Oakland County Sheriff's Office

David Matthews
Administrator
Wisconsin Division of Criminal Investigation

Robert McConnell
Executive Director
Association of State Criminal Investigative Agencies

Mike McDaniel
Director
High Intensity Drug Traffic Area, Houston

Harlin McEwen
Chairman
Communications & Technology Committee
International Association of Chiefs of Police

Kevin Metcalfe
Technical Liason Director
National Technical Assistance Centre - London, England

Peter Modafferi
Chief of Detectives
Rockland County District Attorney's Office

Michael Moore
President
National District Attorneys Association

Patrick Mulcahy
Senior Investigator
Suffolk County District Attorney's Office

Kelly Oliver
Section Chief
United States Department of Homeland Security

Marybeth Paglino
Interim Director/ Unit Chief
National Domestic Communications Assistance Center, FBI

John Primiano
Special Investigator
Suffolk County District Attorney's Office

Sandra Putnam
Inspector, Investigative Division
Georgia Bureau of Investigation

Maura Quinn
Deputy Chief Counsel
International and Intelligence Law, U.S. Department of Justice, DEA

David J. Roberts
Senior Program Manager
International Association of Chiefs of Police

John Rosiak
Principal, Prevention Partnerships
Rosiak Associates LLC

Thomas Ruocco
Assistant Director
Criminal Investigations
Texas Department of Public Safety

Sherry Sabol
Section Chief
Federal Bureau of Investigation

Kurt Schmid
Director
High Intensity Drug Traffic Area, Chicago

Kerry Sleeper
Assistant Director, Office of Partner Engagement
Federal Bureau of Investigation

Barry Smith
Client Executive
Unisys

James Spero
Special Agent in Charge
United States Department of Homeland Security

Kevin Sullivan
Lieutenant
Montgomery County Police Department

Vincent Talucci
Executive Director/ Chief Executive Officer
International Association of Chiefs of Police

Michael Taylor
Corporal
Pennsylvania State Police

Richard Voss
Initiative Manager, Going Dark
Operational Technology Division
Federal Bureau of Investigation

Ken Walker
Chief of Police
West University Place Police Department

Spring Williams
Unit Chief, STSO
Office of Investigative Technology
Drug Enforcement Administration

Itamar Yeger
Counsel
Rockland County District Attorney's Office

APPENDICES

APPENDIX A

IACP TECHNOLOGY POLICY FRAMEWORK[1]
January 2014

Introduction

New and emerging technologies increasingly play a crucial role in the daily work of police, equipping officers with enforcement and investigative tools that have the potential of making them safer, better informed, and more effective and efficient. Developing and enforcing comprehensive agency policies regarding deployment and use is a critical step in realizing the value that technologies promise, and is essential in assuring the public that their privacy and civil liberties are recognized and protected.

Technological advances have made it possible to monitor and record nearly every interaction between police and the public through the use of in-car and body-worn video, access to an expanding network of public and private video surveillance systems, and the increasing use of smartphones with digital recording capabilities by citizens and officers alike. Police can track suspects with the use of GPS tracking technologies and officers themselves can be tracked with automated vehicle location (AVL) systems. Automated license plate recognition (ALPR) systems can scan the license plates of vehicles within sight of officers in the field and quickly alert them if the vehicle has been reported stolen or is wanted. Identity can be remotely verified or established with biometric precision using mobile fingerprint scanners and facial recognition software. Crimes can be mapped as they are reported, gunshot detection technology can alert law enforcement almost instantaneously when a firearm is discharged, and surveillance cameras can be programmed to focus in on the gunshot location and stream live video to both dispatchers and responding officers. With these advancements come new opportunities to enhance public and officer safety. They also present new challenges for law enforcement executives.

The challenges include identifying which technologies can be incorporated by the agency to achieve the greatest public safety benefits, and defining metrics that will enable the agency to monitor and assess the value and performance of the technologies. Just because a technology *can* be implemented, does not mean that it *should* be. There are also challenges in integrating these technologies across different platforms, building resilient infrastructure and comprehensive security, providing technical support, and maintaining and upgrading applications and hardware. All of this can be confusing and technically demanding, underscoring the need for effective planning, strategic deployment, and performance management.

Addressing these challenges is paramount because of the broader issues that the use of this expanding array of technologies by law enforcement presents. A principal tenet of policing is the trust citizens grant police to take actions on their behalf. If that trust is violated and public approval lost, police are not able to effectively perform their duties to keep communities safe.

The Policy Mandate

Creating and enforcing agency policies that govern the deployment and use of technology, protecting the civil rights and civil liberties of individuals, as well as the privacy protections afforded to the data collected, stored, and used, is essential to ensure effective and sustainable implementation, and to maintain community trust. Policies function to reinforce training and to establish an operational baseline to guide officers and other personnel in proper procedures regarding its use. Moreover, policies help to ensure uniformity in practice across the agency and to enforce accountability. Policies should reflect the mission and values of the agency and be tightly aligned with applicable local, state, and federal laws, regulations, and judicial rulings.

Policies also function to establish transparency of operations, enabling agencies to allay public fears and misperceptions by providing a framework that ensures responsible use, accountability, and legal and constitutional compliance. The use of automated license plate recognition (ALPR) technologies, unmanned aerial systems, and body-worn video by law enforcement, for example, has generated substantial public discussion, increasing scrutiny, and legislative action in recent years.[2] Privacy advocates, elected officials, and members of the public have raised important questions about how and under what circumstances these technologies are deployed, for what purposes, and how the data gathered by these technologies are retained, used, and shared. Having and enforcing a strong policy framework enables law enforcement executives to demonstrate responsible planning, implementation, and management.

Agencies should adopt and enforce a technology policy framework that addresses technology objectives, deployment, privacy protections, records management, data quality, systems security, data retention and purging, access and use of stored data, information sharing, accountability, training, and sanctions for non-compliance. Agencies should implement safeguards to ensure that technologies will not be deployed in a manner that could violate civil rights (race, religion, national origin, ethnicity, etc.) or civil liberties (speech, assembly, religious exercise, etc.). The policy framework is but one of several critical components in the larger technology planning effort that agencies should undertake to ensure proper and effective use of automation.

Universal Principles

Given the privacy concerns and sensitivity of personally identifiable information and other data often captured and used by law enforcement agencies,[3] and recognizing evolving perceptions of what constitutes a reasonable expectation of privacy,[4] the

technology policy framework should be anchored in principles universally recognized as essential in a democratic society.

The following universal principles should be viewed as a guide in the development of effective policies for *technologies that can, or have the potential to monitor, capture, store, transmit and/or share data, including audio, video, visual images, or other personally identifiable information which may include the time, date, and geographic location where the data were captured*.[5]

1. *Specification of Use*—Agencies should define the purpose, objectives, and requirements for implementing specific technologies, and identify the types of data captured, stored, generated, or otherwise produced.
2. *Policies and Procedures*—Agencies should articulate in writing, educate personnel regarding, and enforce agency policies and procedures governing adoption, deployment, use, and access to the technology and the data it provides. These policies and procedures should be reviewed and updated on a regular basis, and whenever the technology or its use, or use of the data it provides significantly changes.
3. *Privacy and Data Quality*—The agency should assess the privacy risks and recognize the privacy interests of all persons, articulate privacy protections in agency policies, and regularly review and evaluate technology deployment, access, use, data sharing, and privacy policies to ensure data quality (i.e., accurate, timely, and complete information) and compliance with local, state, and federal laws, constitutional mandates, policies, and practice.
4. *Data Minimization and Limitation*—The agency should recognize that only those technologies, and only those data, that are strictly needed to accomplish the specific objectives approved by the agency will be deployed, and only for so long as it demonstrates continuing value and alignment with applicable constitutional, legislative, regulatory, judicial, and policy mandates.
5. *Performance Evaluation*—Agencies should regularly monitor and evaluate the performance and value of technologies to determine whether continued deployment and use is warranted on operational, tactical, and technical grounds.
6. *Transparency and Notice*—Agencies should employ open and public communication and decision-making regarding the adoption, deployment, use, and access to technology, the data it provides, and the policies governing its use. When and where appropriate, the decision-making process should also involve governing/oversight bodies, particularly in the procurement process. Agencies should provide notice, when applicable, regarding the deployment and use of technologies, as well as make their privacy policies available to the public. There are practical and legal exceptions to this principle for technologies that are

lawfully deployed in undercover investigations and legitimate, approved covert operations.[6]

7. *Security*—Agencies should develop and implement technical, operational, and policy tools and resources to establish and ensure appropriate security of the technology (including networks and infrastructure) and the data it provides to safeguard against risks of loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. This principle includes meeting state and federal security mandates (e.g., the FBI's CJIS Security Policy[7]), and having procedures in place to respond if a data breach, loss, compromise, or unauthorized disclosure occurs, including whether, how, and when affected persons will be notified, and remedial and corrective actions to be taken.[8]
8. *Data Retention, Access and Use*—Agencies should have a policy that clearly articulates that data collection, retention, access, and use practices are aligned with their strategic and tactical objectives, and that data are retained in conformance with local, state, and/or federal statute/law or retention policies, and only as long as it has a demonstrable, practical value.
9. *Auditing and Accountability*—Agencies and their sworn and civilian employees, contractors, subcontractors, and volunteers should be held accountable for complying with agency, state, and federal policies surrounding the deployment and use of the technology and the data it provides. All access to data derived and/or generated from the use of relevant technologies should be subject to specific authorization and strictly and regularly audited to ensure policy compliance and data integrity. Sanctions for non-compliance should be defined and enforced.

Developing Policies and Operating Procedures

The universal principles provide structural guidance for the development of specific agency policies and operating procedures that comport with established constitutional, legal, and ethical mandates and standards. Agency policies and procedures specify the operational components of each individual technology implementation, deployment, and management, and should typically include and address the following factors:[9]

1. Purpose
    a. A general discussion of the purpose of a specific agency policy to include the agency's position on protecting privacy.
2. Policy
    a. A discussion of the overarching agency policy regarding the deployment and use of a specific technology, its application to members of the agency, and reference to relevant laws, policies, and/or regulations that authorize the agency to implement a technology, or that relate to the use and deployment of a technology.
3. Definitions

a. A description of the technology, its components, and functions.
b. Definitions and acronyms associated with the technology.

4. Management
    a. Strategic Alignment: Describe how the technology aligns and furthers the agency's strategic and tactical deployment objectives.
    b. Objectives and Performance: Identify objectives for the deployment and conditions for use of a technology, and a general strategy for assessing performance and compliance with the agency's policy.
    c. Ownership: Clearly specify that the hardware and software associated with the technology is the property of the agency, regardless whether it has been purchased, leased, or acquired as a service, and that all deployments of a technology are for official use only (FOUO). All data captured, stored, generated, or otherwise produced by a technology are the property of the agency, regardless where the data are housed or stored. All access, use, sharing, and dissemination of the data must comply with the policies established and enforced by the agency.
    d. Classification of Data: Clearly specify the data classification and its level of sensitivity (e.g., top secret, secret, confidential, restricted, unclassified, private, public, etc.), whether the data captured, stored, generated, or otherwise produced by a technology are considered public information, and whether it is subject to applicable public records act requests and under what circumstances.
    e. Privacy Impact: Develop or adopt and use a formal privacy impact assessment (PIA)[10] or similar agency privacy assessment on technology and the data it captures, stores, generates, or otherwise produces.

5. Operations
    a. Installation, Maintenance, and Support: Require regular maintenance, support, upgrades, calibration, and refreshes of a technology to ensure that it functions properly.
    b. Deployment: Identify who is authorized to officially approve the deployment and use of a technology, and the conditions necessary for deployment and use, if applicable.
    c. Training: Require training, and perhaps certification or other documented proficiency, if applicable, of all personnel who will be managing, maintaining, and/or using a technology. Training should also cover privacy protections on the use of the technology, and the impact and sanctions for potential violations.
    d. Operational Use: Identify specific operational factors that must be addressed in deployment and use of a technology. (For example, for ALPR, the officer should i) verify that the system has correctly "read" the license plate characters; ii) verify the state of issue of the license plate; iii) verify that the "hot list" record that triggered the alert is still active in the state or NCIC stolen vehicle or other file, and confirm the

hit with the entering agency; and iv) recognize that the driver of the vehicle may not be the registered owner).

e. Recordkeeping: Require recordkeeping practices that document all deployments of the technology, including who authorized the deployment; how, when, and where the technology was deployed; results of deployments; and any exceptions. Recordkeeping will support efforts to properly manage technology implementation, ensure compliance with agency policies, enable transparency of operations, enable appropriate auditing review, and help document business benefits realization.

6. Data Collection, Access, Use, and Retention
    a. Collection: Define what data will be collected, how data will be collected, the frequency of collection, how and where data will be stored, and under what authority and conditions the data may be purged, destroyed, or deleted in compliance with applicable local, state, and/or federal recordkeeping statutes and policies, court orders, etc. Identify the destruction/deletion methods to be used.
    b. Access and Use: Define what constitutes authorized use of data captured, stored, generated, or otherwise produced by a technology. Define who is authorized to approve access and use of the data, for what purposes and under what circumstances.
    c. Information Sharing: Specify whether data captured, stored, generated, or otherwise produced by a technology can be shared with other agencies, under what circumstances, how authorization is provided, how information that is shared is tracked/logged, how use is monitored, and how policy provisions (including privacy) will be managed and enforced. Any agency contributing and/or accessing shared information should be a signatory of a data sharing Memorandum of Understanding (MOU). Dissemination of any shared information should be governed by compliance with applicable state and federal laws, standards, agency privacy policies, and procedures as agreed in the MOU.
    d. Security: Define information systems security requirements of the technology and access to the data to ensure the integrity of the systems and confidentiality of the data. The security policy should address all state and federal mandated security policies, and clearly address procedures to be followed in the event of a loss, compromise, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure of data, including how and when affected persons will be notified, and remedial and corrective actions to be taken.
    e. Data Retention and Use: Establish data retention schedules in accordance with state or federal law or policy, access privileges, purge,

and deletion criteria for all data captured, stored, generated, or otherwise produced by a technology. Agencies should consider differentiating between data that are part of an ongoing or continuing investigation and information that is gathered and retained without specific suspicion or direct investigative focus. Agencies may wish to limit the retention of general surveillance data. Empirical research assessing the performance of a technology may assist in determining an appropriate retention schedule.

7. Oversight, Evaluation, Auditing, and Enforcement
    a. Oversight: Establish a reporting mechanism and a protocol to regularly monitor the use and deployment of a technology to ensure strategic alignment and assessment of policy compliance.
    b. Evaluation: Regularly assess the overall performance of a technology so that it can i) identify whether a technology is performing effectively, ii) identify operational factors that may impact performance effectiveness and/or efficiency, iii) identify data quality issues, iv) assess the business value and calculate return on investment of a technology, and v) ensure proper technology refresh planning.
    c. Auditing: Audit all access to data captured, stored, generated, or otherwise produced by a technology to ensure that only authorized users are accessing the data for legitimate and authorized purposes, and establish regular audit schedules.
    d. Enforcement: Establish procedures for enforcement if users are suspected of being or have been found to be in noncompliance with agency policies.

Conclusion

Realizing the value that technology promises law enforcement can only be achieved through proper planning, implementation, training, deployment, use, and management of the technology and the information it provides. Like all resources and tools available to law enforcement, the use of new technologies must be carefully considered and managed. Agencies must clearly articulate their strategic goals for the technology, and this should be aligned with the broader strategic plans of the agency and safety needs of the public. Thorough and ongoing training is required to ensure that the technology performs effectively, and that users are well versed in the operational policies and procedures defined and enforced by the agency. Policies must be developed and strictly enforced to ensure the quality of the data, the security of the system, compliance with applicable laws and regulations, and the privacy of information gathered. Building robust auditing requirements into agency policies will help enforce proper use of the system, and reassure the public that their privacy interests are recognized and protected. The development of these policies is a proven way for executives to ensure they are taking full advantage of technology to assist in providing the best criminal justice services, while protecting the privacy, civil rights, and civil liberties of citizens.

[1] This Technology Policy Framework was developed by an ad-hoc committee of law enforcement executives and subject matter experts representing IACP Divisions, Committees, Sections, the IACP National Law Enforcement Policy Center, and other organizations and groups, including the Criminal Intelligence Coordinating Council, Major Cities Chiefs Association, National Sheriffs' Association, Major County Sheriffs' Association, Association of State Criminal Investigative Agencies, the Institute for Intergovernmental Research (IIR), the Integrated Justice Information Systems (IJIS) Institute, and federal partners.

[2] The American Civil Liberties Union (ACLU) recently released two reports addressing law enforcement technologies—ALPR and body-worn video. Both reports discuss the value of the technology to law enforcement operations and investigations, and both call for policies addressing deployment, operations, data retention, access, and sharing. Catherine Crump, *You are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements,* (New York: ACLU, July 2013), at https://www.aclu.org/technology-and-liberty/you-are-being-tracked-how-license-plate-readers-are-being-used-record, and Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, a Win for All,* (New York: ACLU, October 2013), at https://www.aclu.org/technology-and-liberty/police-body-mounted-cameras-right-policies-place-win-all. *Also see,* Massachusetts Senate Bill S.1648, *An Act to Regulate the Use of Automatic License Plate Reader Systems,* Cynthia S. Creem, Sponsor, at https://malegislature.gov/Bills/188/Senate/S1648; Cynthia Stone Creem and Jonathan Hecht, "Check it, then chuck it," *The Boston Globe,* December 20, 2013, at http://www.bostonglobe.com/opinion/2013/12/20/podium-license/R1tKQerV0YAPLW6VCKodGK/story.html; Shawn Musgrave, "Boston Police halt license scanning program," *The Boston Globe,* December 14, 2013, at http://www.bostonglobe.com/metro/2013/12/14/boston-police-suspend-use-high-tech-licence-plate-readers-amid-privacy-concerns/B2hy9UIzC7KzebnGyQ0JNM/story.html; Ashley Luthern and Kevin Crowe, "Proposed Wisconsin bill would set rules for license-plate readers," *Milwaukee Journal Sentinel*, December 3, 2013, at http://www.jsonline.com/news/milwaukee/proposed-wisconsin-bill-would-set-rules-for-license-plate-readers-b99155494z1-234324371.html; Dash Coleman, "Tybee Island abandons license plate scanner plans," *Savannah Morning News,* December 3, 2013, at http://savannahnow.com/news/2013-12-02/tybee-island-abandons-license-plate-scanner-plans#.UqCAy8RDuN0; Kristian Foden-Vencil, "Portland police are collecting thousands of license plate numbers every day," *Portland Tribune*, December 3, 2013, at http://portlandtribune.com/pt/9-news/203130-portland-police-are-collecting-thousands-of-license-plate-numbers-every-day; Alicia Petska, "City Council split over how to handle license plate reader concerns," *The News & Advance,* (Lynchburg, VA), November 12, 2013, at http://www.newsadvance.com/news/local/article_5327dc78-4c18-11e3-bc28-001a4bcf6878.html; Jonathan Oosting, "Proposal would regulate license plate readers in Michigan, limit data stored by police agencies," *MLive,* (Lansing, MI), September 9, 2013, at http://www.mlive.com/politics/index.ssf/2013/09/proposal_would_regulate_licens.html; Katrina Lamansky, "Iowa City moves to ban traffic cameras, drones, and license plate recognition," *WQAD*, June 5, 2013, at http://wqad.com/2013/06/05/iowa-city-moves-to-ban-traffic-cameras-drones-and-license-plate-recognition/; Richard M. Thompson, II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses,* (Washington, DC: Congressional Research Service, April 3, 2013), at http://www.fas.org/sgp/crs/natsec/R42701.pdf; Somini Sengupta, "Rise of Drones in U.S. Drives

Efforts to Limit Police Use," *New York Times,* February 15, 2013, at http://www.nytimes.com/2013/02/16/technology/rise-of-drones-in-us-spurs-efforts-to-limit-uses.html?pagewanted=all; Stephanie K. Pell and Christopher Soghoian, "Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact," *Berkeley Technology Law Journal,* Vol. 27, No. 1, pp. 117-196, (2012), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644; and Stephen Rushin, "The Legislative Response to Mass Police Surveillance," 79 *Brooklyn Law Review* 1*,* (2013), at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2344805. All accessed December 30, 2013.

[3] Personally identifiable information (PII) has been defined as "…any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." Government Accountability Office (GAO), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, (Washington, D.C.: GAO, May 2008), p. 1, at http://www.gao.gov/new.items/d08536.pdf. McCallister, *et. al.,* define "linked" information as "information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual." Erika McCallister, Tim Grance, and Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology,* (Gaithersburg, MD: NIST, April 2010), p. 2-1, at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. McCallister, *et. al.,* go on to describe *linked* and *linkable* information: "For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable." *Id.* Both accessed December 30, 2013.

[4] Justice Harlan first articulated a "constitutionally protected reasonable expectation of privacy" in *Katz v. United States*, 389 U.S. 347 (1967), at 361. Justice Harlan's two-fold test is "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* Many of the technologies being deployed by law enforcement capture information that is publicly exposed, such as digital photographs and video of people and vehicles, or vehicle license plates in public venues (i.e., on public streets, roadways, highways, and public parking lots), and there is little expectation of privacy. "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *United States v. Knotts*, 460 U.S. 276 (1983), at 281. Law enforcement is free to observe and even record information regarding a person's or a vehicle's movements in public venues. The U.S. Supreme Court, however, has ruled that the electronic compilation of otherwise publicly available but

difficult to obtain records alters the privacy interest implicated by disclosure of that compilation. *U.S. Department of Justice v. Reporters Committee for Freedom of the Press,* 489 U.S. 749 (1989). Automation overwhelms what the Court referred to as the *practical obscurity* associated with manually collecting and concatenating the individual public records associated with a particular person into a comprehensive, longitudinal criminal history record. "…[T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.,* at p. 764. This has subsequently been referred to as the "mosaic theory" of the Fourth Amendment. *United States v. Maynard,* 615 F.3d 544 (D.C. Cir.) (2010). *See also,* Orin Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review*, Vol. 111, p. 311, (2012), at http://www.michiganlawreview.org/assets/pdfs/111/3/Kerr.pdf. Accessed December 30, 2013.

[5] These universal principles largely align with the Fair Information Practices (FIPs) first articulated in 1973 by the Department of Health, Education & Welfare (HEW). HEW, *Records, Computers and the Rights of Citizens*, July 1973, at http://epic.org/privacy/hew1973report/default.html. *See,* Robert Gellman, *Fair Information Practices: A Basic History,* Version 2.02, November 11, 2013, at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. Comparable principles have been articulated by various governmental agencies, including the U.S. Department of Homeland Security, (Hugo Teufel, III, *Privacy Policy Guidance Memorandum, Number: 2008-01,* (Washington, DC: DHS, December 29, 2008), pp. 3-4, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf); the Home Office in the United Kingdom (Home Office, *Surveillance Camera Code of Practice,* (London, UK; The Stationery Office, June 2013), pp 10-11, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf); and the Information and Privacy Commissioner of Ontario, Canada (Ann Cavoukian, *Guidelines for the Use of Video Surveillance Cameras in Public Places,* (Ontario, Canada: Information and Privacy Commissioner of Ontario, September 2007), pp. 5-6, at: http://www.ipc.on.ca/images/Resources/up-3video_e_sep07.pdf, and Ann Cavoukian, *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigative Report (Privacy Investigation Report MC07-68)*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, March 3, 2008), p 3, at: http://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf). *Also see*, National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment,* (The National Academies Press: Washington, D.C., 2008), at http://nap.edu/catalog.php?record_id=12452. All accessed December 30, 2013.

[6] Law enforcement is not, for example, expected to notify the subjects of lawfully authorized wiretaps that their conversations are being monitored and/or recorded. These deployments, however, are typically subject to prior judicial review and authorization. *See, e.g., Katz v. United States,* 389 U.S. 347 (1967); *Berger v. New York,* 388 U.S. 41 (1967); *Title III, Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-2522, as amended by the *Electronic Communications Privacy Act of 1986*.

[7] Federal Bureau of Investigation, *Criminal Justice Information Services (CJIS) Security Policy,* Version 5.2, August 9, 2013, CJISD-ITS-DOC-08140-5.2, at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view. Accessed December 30, 2013.

[8] Additional guidance regarding safeguarding personally identifiable information can be found in the Office of Management and Budget (OMB) Data Breach notification policy (M-07-16), at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf, and state data breach notification laws available from the National Conference of State Legislatures, at http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Accessed December 30, 2013.

[9] *See, e.g.,* International Association of Chiefs of Police, *Model Policy: License Plate Readers*, August 2010 http://iacppolice.ebiz.uapps.net/personifyebusiness/OnlineStore/ProductDetail/tabid/55/Default.aspx?ProductId=1223; Paula T. Dow, Attorney General, *Directive No. 2010-5, Law Enforcement Directive Promulgating Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data,* (Trenton, NJ: Office of the Attorney General, December 3, 2010), at http://www.state.nj.us/oag/dcj/agguide/directives/Dir-2010-5-LicensePlateReadersl-120310.pdf; Office of the Police Ombudsman, *2011 Annual Report: Attachment G: Body-Worn Video & Law Enforcement: An Overview of the Common Concerns Associated with Its Use*, (Spokane, WA: Spokane Police Ombudsman, February 20, 2012), at http://www.spdombudsman.com/wp-content/uploads/2012/02/Attachment-G-Body-Camera-Report.pdf; ACLU, *Model Policy: Mobile License Plate Reader (LPR) System,* (Des Moines, IA: ACLU, September 19, 2012), at http://www.aclu-ia.org/iowa/wp-content/uploads/2012/09/Model-ALPR-Policy-for-Iowa-Law-Enforcement.pdf. Many of these policy elements are also addressed in the National Research Council's report, *op. cit.,* specifically in chapter 2, "A Framework for Evaluating Information-Based Programs to Fight Terrorism or Serve Other Important National Goals," at pp. 44-67. All accessed December 30, 2013

[10] A privacy impact assessment (PIA) is "a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme." Roger Clarke, "Privacy Impact Assessment: Its Origins and Development," *Computer Law & Security Review,* 25, 2 (April 2009), pp. 125-135, at http://www.rogerclarke.com/DV/PIAHist-08.html. Law enforcement agencies should consider using the Global Advisory Committee's *Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Entities* at https://it.ojp.gov/gist/47/Guide-to-Conducting-Privacy-Impact-Assessments-for-State--Local--and-Tribal-Justice-Entities. This resource leads policy developers through appropriate privacy risk assessment questions that evaluate the process through which PII is collected, stored, protected, shared, and managed by an electronic information system or online collection application. The IACP published *Privacy Impact Assessment Report for the Utilization of License Plate Readers,* (Alexandria, VA: IACP, September 2009), at http://www.theiacp.org/Portals/0/pdfs/LPR_Privacy_Impact_Assessment.pdf. For a list of PIAs completed by the U.S. Department of Justice, *see* http://www.justice.gov/opcl/pia.htm; Department of Homeland Security, *see* https://www.dhs.gov/privacy-office-privacy-impact-assessments-pia. All accessed December 30, 2013.

APPENDIX B

July 6, 2015

The Honorable Kevin Yoder
Third District, Kansas
United States House of Representatives
214 Cannon House Office Building
Washington, DC 20515

RE: HR 699 – Updating the Electronic Communications Privacy Act (ECPA) and Reducing the Effects of Non-Technical Barriers on Lawful Access of Electronic Evidence

Dear Congressman Yoder:

We, the undersigned organizations representing federal, state and local prosecutors, chiefs, sheriffs, and rank and file officers, understand the intent of HR 699 - the "Email Privacy Act" - is to update the law to ensure that Americans' privacy rights are reinforced in the digital age. While we support efforts to guarantee the privacy rights of all citizens, it is imperative that we ensure that law enforcement, with appropriate judicial supervision and approval, maintain its ability to access and recover digital evidence in order to protect the public and successfully prosecute those guilty of crimes.

Therefore, we ask that any legislation relating to this issue also address the very real challenges that law enforcement faces as it attempts to gather electronic evidence. Failure to address these challenges will result in more missed leads, longer investigative timelines, less safety for Americans and less justice for victims of crime.

The amount of evidence that exists in the digital space is growing explosively. Our society is powered by data that lies at rest and moves across a vast range of devices. Some of that data becomes evidence every time a crime is committed, and this electronic evidence is critical to investigators who need it to generate leads, corroborate stories, identify suspects and conspirators, challenge alibis, exonerate the innocent, and obtain justice for victims of crime.

Evidence takes a variety of forms in the digital space. Evidence can be found in the content of communications and in the data that surrounds communications events. Evidence can be gathered while at rest on devices and in real time while it is in motion across networks. Law enforcement is concerned about anything that creates a barrier to lawfully accessing that evidence. Some of the barriers that degrade our effectiveness are technological, like encryption, and others are non-technological, like elevated legal standards and a lack of responsiveness by private companies who possess electronic evidence.

The attached fact sheet provides an overview of these barriers along with a number of possible solutions that would help ensure that law enforcement maintain access to the critical digital evidence it needs to fulfill its mission. Law enforcement collects much of the electronic evidence it needs by exchanging legal process with service providers like wireless phone companies, internet providers, and

application developers. The logistics of requesting and receiving information from service providers in response to these lawful process demands are antiquated, non-standardized, and often haphazard, causing a very real and under-publicized set of problems. Bringing consistency to the standard of proof that governs law enforcement access to evidence is meaningless if law enforcement cannot obtain the evidence because it hasn't been retained, because the court order is lost after being transmitted, or because the response takes weeks or months to process by the service provider.

To be clear, law enforcement is not asking for new surveillance capabilities above and beyond what is currently authorized by the U.S. Constitution or by lawful court orders, nor are we attempting to access or monitor the digital communications of all citizens. Law enforcement simply needs to be able to lawfully access information that has been duly authorized by a court in the limited circumstances prescribed in specific court orders—information of potentially significant consequence for investigations of serious crimes and terrorism.

We would welcome the opportunity to discuss our concerns and potential solutions to these issues with you at your earliest convenience.

Thank you for your attention to this matter.

Sincerely,

Association of Prosecuting Attorneys (APA)
Association of State Criminal Investigative Agencies (ASCIA)
Federal Law Enforcement Officers Association (FLEOA)
Fraternal Order of Police (FOP)
International Association of Chiefs of Police (IACP)
Major Cities Chiefs Association (MCCA)
Major County Sheriffs' Association (MCSA)
National Association of Assistant United States Attorneys (NAAUSA)
National Association of Police Organizations (NAPO)
National District Attorneys Association (NDAA)
National Fusion Center Association (NFCA)
National Narcotic Officers' Associations' Coalition (NNOAC)
National Sheriffs' Association (NSA)

cc: House Judiciary Committee
Senate Judiciary Committee