National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

July 2019

National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

Table of Contents

National Domestic Communications Assistance Center (NDCAC)
Executive Advisory Board (EAB)
Report to the Attorney General

Executive Summary

The ability of law enforcement to fulfill its public safety and national security mission is deteriorating as communications services and technology companies introduce barriers to critical investigation materials—obstacles that, at the very least, add complexity, and, at worst, are insurmountable. These obstacles include, but are not limited to, end-to-end encryption, anonymization, and service mobility. Numerous groups have written reports[1] identifying these law enforcement challenges; however, most reports focus exclusively on issues associated with encryption, while several others claim advancements in communications devices and services represent a greater benefit than detriment to law enforcement. Regardless, while the debate continues as to how best to address these obstacles, the gap between law enforcement's court-ordered authority to collect evidence, and the ability to gain access to that evidence from technology companies, grows ever wider.

Any resolution to the encryption debate requires all stakeholders' willing participation, and represents a significant undertaking both in time and in resources. Law enforcement must pursue a solution to address encryption and should devote the necessary resources needed to move ahead. However, it need not be the only path pursued. Immediate action to adopt mitigation strategies to address non-encryption issues can yield short-term, as well as lasting results. Law enforcement can only pursue these strategies with adequate resources, which, at the time of this Report, are severely lacking.

The Executive Advisory Board (EAB) of the National Domestic Communications Assistance Center (NDCAC) previously provided the Attorney General a 2017 Report[2] (2017 EAB Report) that identified technical, resource-based, and statutory challenges faced by the law enforcement community concerning digital evidence. In addition to identifying the encryption challenge, the 2017 EAB Report highlighted the following issues, which, as noted above, are still present today: service mobility, anonymization, outdated statutes that have not kept pace with changing communications technology, the lack of a mandate regarding data retention, and the lack of investment in necessary digital evidence infrastructure. The tension between the law enforcement mandates and segments of the technology industry often hamper the ability to collaborate on the fundamental processes of information exchange. Despite these challenges, funding for NDCAC has been substantially decreased, with funding for Fiscal Year 2020 being the lowest yet because of a projected 11 percent reduction. The EAB urges the Attorney General ensure NDCAC receive at least its current level of funding in the next year and look to enhance its resources as more of the law enforcement community comes to rely on NDCAC. The EAB knows significant digital evidence challenges are imminent (e.g., 5G wireless services, Internet of Things) and needs NDCAC to be robustly prepared to help with more resources.

In this second Report, the EAB identifies the general categories of challenges, describes the factors influencing law enforcement's ability to address those challenges, and outlines approaches and types of solutions the EAB has contemplated to the challenges noted above. The EAB believes NDCAC can continue to play an essential role in addressing several of the

substantial challenges faced by the law enforcement community, and stands ready to contribute to the Department of Justice's (DOJ) formulation of a path forward to address the challenges faced by the entire law enforcement community.

Introduction

Today's investigative environment requires all levels of law enforcement to be knowledgeable of multiple forms of evidence, especially digital evidence. Specifically, law enforcement must know how to gain access, collect, process, and preserve digital evidence. This expertise is necessary for the collection of evidence intercepted as it is transmitted from one user to another (or to the cloud), extracted from seized devices, or gleaned from provider records returned in compliance with legal process. Further, the growing nature of communications services, and the advancing capabilities of devices, require law enforcement agencies to continuously enhance and expand their skills concerning digital evidence. NDCAC is in a unique position to provide essential assistance in carrying out this task.

Executive Advisory Board

The NDCAC EAB is comprised of fifteen senior law enforcement members representing Federal, State, local, and tribal agencies nationwide. To ensure State and local interests are given adequate consideration, the EAB is chartered to have a State and local majority of plus one. Therefore, eight of the fifteen EAB members represent State, local, and/or tribal representatives, and are agency heads such as a Chief of Police, Police Commissioner, Sheriff, Colonel, Superintendent, other officially designated executive, or a prosecutor from the State or local level. These eight members represent: the Association of State Criminal Investigative Agencies, the International Association of Chiefs of Police, the Major City Chiefs, the Major County Sheriffs, the National Sheriffs' Association, the National Narcotic Officers' Associations' Coalition, National District Attorneys Association, and the Association of Prosecuting Attorneys.

The remaining seven members of the EAB are Senior Executive Service officials from: Bureau of Alcohol, Tobacco, Firearms, and Explosives, Drug Enforcement Administration, Federal Bureau of Investigation, Immigration and Customs Enforcement, United States Marshals Service, United States Postal Inspection Service, and the United States Secret Service. Each of the fifteen executive level members has experience in the management of electronic surveillance capabilities, evidence collection on communication devices, and technical location capabilities within their respective organizations.

NDCAC EAB Members		
Name	**Title**	**Organization**
Preston L. Grubbs, Chairman	Principal Deputy Administrator	Drug Enforcement Administration
James (Al) Cannon, Vice-Chairman	Sheriff, Charleston County Sheriff's Office	Major County Sheriffs
David Bowers	Inspector in Charge, Security & Crime Prevention	US Postal Inspection Service
Michael D'Ambrosio	Deputy Assistant Director, Office of Investigations	US Secret Service
Derrick Driscoll	Acting Deputy Director	US Marshals Service
Alysa Erichs	Acting Executive Associate Director	Immigration and Customs Enforcement
G. Clayton Grigg	Assistant Director, Laboratory Division	Federal Bureau of Investigation

NDCAC EAB Members		
Name	**Title**	**Organization**
Mark A. Keel	Chief, South Carolina Law Enforcement Division	Association of State Criminal Investigative Agencies
Lenny Millholland	Sheriff, Frederick County Sheriff's Office	National Sheriffs' Association
Christopher (C.J.) Noelck	Special Agent in Charge, Investigative Operations, Iowa Department of Public Safety	National Narcotic Officers' Associations' Coalition
Thomas G. Ruocco	Assistant Director/Chief, Criminal Investigations Division, Texas Department of Public Safety	International Association of Chiefs of Police
Michael Sachs	Executive Assistant District Attorney, New York County District Attorney's Office	Association of Prosecuting Attorneys
Henry Stawinski	Chief of Police, Prince George's County	Major City Chiefs
Paul Vanderplow	Chief, Special Operations Division	Bureau of Alcohol, Tobacco, and Firearms
Edwin Zabin	First Assistant District Attorney, Suffolk County District Attorney's Office	National District Attorney's Association

Challenges

In its 2017 Report to the Attorney General, the EAB outlined technical (electronic surveillance, communications evidence, and location capabilities), resource, and statutory challenges impacting law enforcement.[3] In nearly every investigation, it is essential that investigative personnel are trained and equipped to acquire, preserve, and analyze digital evidence and these abilities are contingent upon precursor processes of both law enforcement and service providers to ensure lawful and timely access to digital evidence. These processes vary depending upon the type of digital evidence sought and where it is stored – with the user, with the provider, or with another third party. For instance, law enforcement processes often include the collection and preservation of devices that contain relevant digital evidence at crime scenes, and forensic extraction and analysis of digital evidence from those devices. They also often require the service of legal process on service providers or other mobile messaging application companies to acquire subscriber information, Global Positioning System (GPS) data, cell site or other location data, Internet Protocol (IP) addresses, and other information that is essential to an ever-increasing number of law enforcement investigations.

The challenges introduced by advancing communications services and technologies impact law enforcement at multiple stages of each investigation and law enforcement must obtain proper legal process to lawfully access communications or acquire data from service providers. All-too-often, however, law enforcement does not receive timely responses to their lawful requests due to service provider deficiencies. Frequently, a lack of transparency by the service provider as to the types of data collected and the retention period for that data coupled with an inability to effectively communicate with service providers leads to inefficient or incomplete production of data in response to legal process.

Solutions to any of the challenges associated with communications services and technologies must take into consideration the varied needs of all levels of law enforcement. However, because State and local law enforcement is disproportionally impacted by technological changes based on the volume of investigations and the scarcity of resources that they can devote to addressing the issues, solutions must be practicable, effective, and economical. Notably, reports issued by the Department of Justice, Office of Justice Programs, Bureau of Justice Statistics

found that in 2007 and 2008, there were approximately 765,000 sworn personnel employed by State and local law enforcement agencies and about 2,330 State and local prosecutor offices, compared to nearly 120,000 sworn personnel employed by Federal law enforcement agencies and 93 United States Attorney's Offices.[4] Thus, it is clear that additional technological resources need to be allocated to those State and local law enforcement agencies that investigate the vast majority of crime in this country.

Factors

Several factors influence the capacity of law enforcement to address new and emerging challenges to its ability to fulfill its public safety and national security mission. As noted below, multiple factors exacerbate these challenges. Often, law enforcement cannot influence or limit these factors and, thus, falls further behind in its capability to gain lawful access to information critical to investigations.

1. *A growing diversification of industry.* In 1994, recognizing a law enforcement need for a standardized means to intercept communications and collect the associated identifying information, Congress passed the Communications Assistance for Law Enforcement Act (CALEA). The law required telecommunications companies to design their equipment and services to ensure law enforcement access. At the time of its enactment, CALEA applied to landline and cellular telecommunications carriers, and was later expanded by the Federal Communications Commission (FCC) to include Voice over IP (VOIP) and broadband internet access providers. FCC regulations[5] further define the obligations of certain providers to retain data. However, CALEA has not kept pace with innovation, and a large and growing number of mobile applications perform the same or similar functions to telecommunications companies, yet they are not covered by CALEA. In many instances, these new communications companies have little or no familiarity with law enforcement needs, do not institute processes to facilitate agency requests in a timely manner, or dispute having any responsibilities to interact with law enforcement altogether.

2. *A smaller segment of industry is required to comply with a solution mandate*. As the evolution and diversification of the communications and technologies industries continues unabated, the portion of the industry which must comply with CALEA's mandate to facilitate law enforcement access grows increasingly smaller and less significant. Without intervention, the proportion of providers who are responsive to law enforcement with pre-defined and implemented capabilities to access communications will continue to decline.

3. *Communications devices and services have become increasingly more sophisticated*. Additional training and resources, like those provided by NDCAC, are needed to adequately acquire, preserve, and analyze digital evidence because digital evidence training has not kept pace within the law enforcement community. This is true despite law enforcement increasingly encountering digital evidence that impacts the resolution of an investigation. For example, concerning mobile devices and wireless services, Americans used a record 15.69 trillion megabytes (MBs) of mobile data in 2017—nearly quadrupling the amount used in 2014 and representing 40 times the volume of traffic in

2010, according to CTIA's latest Annual Wireless Industry Survey.[6] Further, Americans are projected to use five times more mobile data by 2022 and, by 2025, people will interact with connected devices every 18 seconds.[7] As a reflection of society's widespread adoption of advanced devices and services, these same devices and services are a regular component of most investigations into criminal activity. The future of mobile devices and wireless services will continue to increase the difficulties for law enforcement as 5G networks are expected to pass 100 times more information, connect 100 times more devices, and be 30 to 50 times faster.

The prodigious volume of the data, coupled with the continuous evolution within the communications and technology industries, requires constant and recurring training for law enforcement to keep pace. However, resource constraints, including insufficient funding and a lack of trained personnel, impede law enforcement agencies' ability to keep pace with the profound changes brought about by each of the above factors. Law enforcement, especially State and local agencies, does not have the resources to invest in the necessary infrastructure and training to bridge the gap between its current capabilities and the required level of technical sophistication it must reach and continuously maintain. Thus, a properly funded NDCAC is essential in assisting State and local agencies all over the country keep pace with rapidly developing technological advancements.

Finally, there exists a perception that advancements in communications devices and services will help law enforcement in many unforeseen ways. This perception assumes the development and adoption of devices and services will allow law enforcement to access previously unavailable troves of information, but does not offer any path forward to ensure the devices and services are developed with the requisite capabilities law enforcement needs to access digital evidence. In other words, disregarding substantive mandates under the guise that a future device or service will provide useful information to law enforcement is inconsistent with experience. Rather, this approach will likely result in neither mandates nor solutions.

Approach to Address the Challenges

There are three distinct approaches that address the challenges faced by law enforcement. Each approach has its advantages and disadvantages, but none should be considered in isolation as a potential approach to all the challenges faced by law enforcement.

The first approach is to rely solely on law enforcement self-help, where the law enforcement community uses current and augmented resources to develop and implement solutions. While certain challenges can be addressed by law enforcement (e.g., training on new and emerging communications devices and services), absent additional resources, most agencies will simply fall further behind. Current resource levels are not adequate throughout the law enforcement community, but a centralized, economies of scale, approach may alleviate the need to replicate certain capabilities across all levels of law enforcement. Additional resources are needed to increase training throughout the law enforcement community and to increase participation at educational conferences and seminars. As investigations grow in complexity, there is a need for more investigators and technical subject matter experts, along with increased sharing of knowledge and resources within the law enforcement community. Further, more sophisticated equipment is needed by all agencies, as the useful lifespan of equipment gets shorter because of

technological advancements. However, this approach alone cannot address the issue with law enforcement gaining access to digital evidence, particularly regarding communications services controlled by service providers—many of which are not required to comply with CALEA.

The second approach consists of open and voluntary cooperation between the technology industry and law enforcement to address the challenges introduced by advancing communications devices and services. In most instances, this approach will only be successful when both sides agree on the scope of the issue and the need to address their respective portions of the issue. There are numerous examples of positive interactions (e.g., making legal process-serving more efficient) between industry and law enforcement.[8] However, the exchange of information is critically important for each side to understand the requirements of law enforcement and the limitations of industry.

The final approach is to mandate responsibilities to ensure the communications and technology industries design, develop, and implement solutions that provide access to digital evidence. This approach— standardizing data that mobile communication companies and service providers are required to keep, requiring data retention periods, and statutorily defining responsibilities of industry to assist law enforcement in gaining lawful access to digital evidence in motion and at rest—has the benefit of ensuring broad consistency concerning capabilities across industry segments. Despite the time necessary for the requisite legislative action, in some instances mandated responsibilities represent the only viable path forward (e.g., access to digital evidence not made available through voluntary cooperation).

Types of Solutions

The set of challenges law enforcement faces today, while both diverse and complex, fall into one of two general categories: technical or process-oriented. Thus, solutions also belong to one of those two categories. Different solutions that address the challenges must be evaluated considering these different approaches.

Technical solutions focus on the ability to acquire, preserve, and analyze digital evidence useful to an investigation. Technical solutions span the spectrum of challenges (i.e., electronic surveillance, communications evidence, and location - for both devices and services), and fall into each of the three types of approaches described above. An important aspect of technical solutions is the requirement that there be consistency across solutions (e.g., efficiency inherent in a standardized approach in identifying the interface between law enforcement and a provider).

Process-oriented solutions concentrate on improving the timeliness and efficiency of interactions necessary for law enforcement to collect evidence. These solutions can span multiple sets of processes: internal to law enforcement, the cooperation between law enforcement and industry, and internal to the industry. Each set of processes can be examined to increase efficiency and timeliness.

Both types of solutions require additional resources. In some cases, only a commitment of substantial resources will be adequate to implement solutions. No proposed solution or solution set exists that does not require additional resources to implement. However, a dedicated source of resources, above those available today, would go a long way in mitigating several of the

challenges faced by law enforcement. Technical and process-oriented solutions need to be adequately funded to address the shortcomings of existing solutions and methods.

Congressional Intent

In 2012, Congress established NDCAC as "…a hub for the management of knowledge and technical expertise regarding lawful electronic surveillance and facilitate the sharing of solutions among Federal, State and local law enforcement."[9] In its 2016 Year End Report, the House Judiciary Committee & House Energy and Commerce Committee, Encryption Working Group identified NDCAC as one of a handful of "ideas [that] could radically improve the ability of the law enforcement community to operate in a digital environment—and also reduce tensions between law enforcement and private industry."[10] Congressional intent was reaffirmed in 2017[11] when it expressed support for continued funding for NDCAC during the annual appropriations process.

NDCAC, EAB, and the Path Forward

Since its establishment, NDCAC has grown in importance to the law enforcement community: amassing more than 20,000 individual clients, answering nearly 100,000 queries, and providing training to over 12,000 students. With each passing year, the rate at which NDCAC provides support has increased. The tools it makes available have enhanced law enforcement's ability to conduct investigations in an era of ever-advancing communications services and technologies. The FBI's support of the entire law enforcement community has played an essential role in NDCAC's success to date. As recently as April 2019, the FBI Director affirmed the Bureau is "… committed to working with our federal, state, local, and tribal partners in a coordinated effort to reduce crime in the United States" and acknowledged "[m]uch of the FBI criminal intelligence is derived from our state, local, and tribal law enforcement partners, who know their communities inside and out."[12] In a recently released report the Intelligence Commanders Group of the Major Cities Chiefs Association (MCCA) and Major County Sheriffs of America (MCSA) recognized NDCAC as "a tremendously valuable resource, since it is not practical or possible for every one of the thousands state and local law enforcement agencies across the country to have, within their own department, adequate access to resources and expertise; federal assistance is needed to supplement the efforts of their local partners."[13] During the National Sheriffs' Association 2019 Conference, Deputy Attorney General Jeffrey A. Rosen remarked that DOJ is "actively working with our community partners to provide technological resources, expand national training, and expand best practice programs"[14] — all of which fall squarely within the NDCAC's mission.

However, despite all its maturation and progress, NDCAC may experience the most significant budget cut in its short history. The first full year of funding (Fiscal Year 2013), NDCAC's budget was more than $13 million; the Fiscal Year 2020 budget of NDCAC is proposed to be less than $10 million. With the latest decrease of more than $1.2 million or 11 percent, NDCAC's budget will have decreased more than 25 percent over eight years. Over the same time, the EAB notes the FBI's budget increased nearly 16 percent, or by a sum of more than one billion dollars.

The EAB urges the Attorney General ensure NDCAC receive at least its current level of funding in the next year and look to enhance its resources as more of the law enforcement community

comes to rely on NDCAC. The EAB knows significant digital evidence challenges are imminent (e.g., 5G wireless services, Internet of Things) and needs NDCAC to be robustly prepared to help with more resources. Growth in the NDCAC's budget is critically important as communications services and technologies are increasing in complexity and law enforcement relies on the NDCAC to be more robust than ever before.

The EAB recognizes certain capabilities of the NDCAC are enhanced by support provided by the FBI's Operational Technology Division (OTD) which are external to the NDCAC's budget and encourages OTD to continue supporting the NDCAC. For example, OTD supports the NDCAC mission with various types of subject matter expertise, digital forensics and electronic surveillance procedures, and the development and fielding of protocol processing capabilities. Further, the EAB understands the NDCAC has historically addressed challenges of scarce resources and competing priorities through cost savings, efficiencies, and prioritizing support to law enforcement in areas such as research of emerging services and technologies, training, tool and website content development, and analysis and validation of industry technical solutions. Even with a return to previous funding levels, the NDCAC will be challenged to meet the needs of the law enforcement community as communications services and technology companies continue to introduce barriers to once effective investigatory methods.

In its July 2018 report entitled "*Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*," the Center for Strategic and International Studies (CSIS) identified NDCAC as "the sole federal entity with an explicit mission to facilitate more efficient cooperation between law enforcement and industry." CSIS concluded that "NDCAC's budget is both small and divided among multiple different training and support programs—making it inadequately resourced to service the 18,000 federal, state, and local law enforcement entities spread across the country."[15] It recommended that "Congress can and should adequately resource NDCAC to serve the training and technical roles that already fall within its mission."[16]

The EAB agrees with CSIS with respect to its NDCAC conclusions and believes NDCAC can continue to play an essential role in addressing several of the substantial challenges faced by the law enforcement community. In its short history, NDCAC has proven to be a valuable training and technical support center for law enforcement. A future NDCAC, if augmented with the necessary resources to expand its reach, could help mitigate what will otherwise be an overwhelming crisis for the State and local law enforcement community. To that end, NDCAC is accomplishing a significant portion of the functionality envisioned by the CSIS recommendation of a centralized National Digital Evidence Office. The EAB, representing a cross-section of Federal, State, local, and tribal agencies—many of which are at the forefront of critical issues facing the law enforcement community—is willing and able to contribute to the DOJ in its role of policy development, oversight, and coordination.

As currently chartered, the NDCAC EAB provides advice to the Attorney General on several vital issues. Two of the most significant are: 1) trends and developments with respect to existing and emerging communications services and technologies; and 2) technical challenges faced by all law enforcement agencies with respect to lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities. Other reports and proposed legislation suggest the formation of another advisory board with

largely similar functions as that of the existing NDCAC EAB. An expansion of the current Charter can be considered by the Attorney General as an effective alternative to having two (or more) mostly redundant advisory committees.

The EAB is confident the recent creation of a State and Local Law Enforcement Coordination Section[17] within DOJ's Office of Legislative Affairs will foster a deeper relationship between DOJ and the law enforcement community. The EAB looks forward to playing a critical role in keeping DOJ leadership informed of state and local law enforcement's top digital evidence priorities through active and ongoing involvement with this new Section.

Recommendation

The EAB advises the Attorney General that the challenges enumerated above warrant the DOJ's immediate attention, and for the Attorney General to ensure the role of the *entire* law enforcement community in determining a path forward that addresses the challenges and any potential remedial initiatives undertaken by the DOJ. Because the challenges faced by the State and local law enforcement community do not always align precisely with those of its Federal partners, the EAB recommends the DOJ institute a comprehensive assessment of implications for all levels of law enforcement and integrate State and local perspectives when pursuing changes to statutes at the Federal level. The EAB further recommends the DOJ endorse the CSIS conclusion regarding increased funding for NDCAC, and work with Congress to adequately fund NDCAC—taking into consideration projected budget reductions—so it can continue to serve the training and technical roles within its mission, both today and in the future. The EAB stands ready to contribute to the DOJ's formulation of a path forward to address the challenges faced by the entire law enforcement community regarding digital evidence and looks forward to its interaction with the State and Local Law Enforcement Coordination Section.

The EAB recognizes the Attorney General may find information in its previously submitted 2017 EAB Report useful to understand law enforcement's longstanding concerns with lawful access to digital evidence. Further, acknowledging the issues presented in both Reports are complex and deeply intertwined, the EAB recommends its members meet with the Attorney General (or his designee) to provide further insight and clarification and to provide answers to any questions that may arise as a result of its Reports.

Endnotes

[1] See *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2017 Report*, Nov. 2018, *available at* https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf; *Third Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 2017, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf; *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report*, Nov. 17, 2016, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf; and *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, Nov. 18, 2015, *available at* https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

Center for Strategic and International Studies (CSIS). July 2018. *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*. Washington, DC: A Report of the CSIS Technology Policy Program, *available at* https://www.csis.org/events/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge

The EastWest Institute. February 2018. *Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions*. New York, NY: The EastWest Institute, *available at* https://www.eastwest.ngo/encryption

National Academies of Sciences, Engineering, and Medicine. February 2018. *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, DC: The National Academies Press, *available at* https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

Center for Strategic and International Studies (CSIS). February 2017. *The Effect of Encryption on Lawful Access to Communications and Data*. Washington, DC: A Report of the CSIS Technology Policy Program, *available at* https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data

Berkman Center for Internet & Society at Harvard University's Berklett CyberSecurity Project. February 2016. *Don't Panic. Making Progress on the "Going Dark" Debate*, *available at* https://cyber.harvard.edu/pubrelease/dont-panic/

[2] NDCAC EAB Report to the Attorney General, October 2017, *available at* https://ndcac.fbi.gov/file-repository/eab-ag-final-report-20180119.pdf/view

[3] Id. at 3-7.

[4] See *Prosecutors in States Courts, 2007 – Statistical Tables*, Dec. 2011, *available at* https://www.bjs.gov/content/pub/pdf/psc07st.pdf; *Census of State and Local Law Enforcement Agencies, 2008*, July 2011, *available at* https://www.bjs.gov/content/pub/pdf/csllea08.pdf; and *Federal Law Enforcement Officers, 2008*, June 2012, *available at* https://www.bjs.gov/content/pub/pdf/fleo08.pdf

[5] See FCC Data Retention Regulation 47 CFR Part 42: Preservation of Records of Communication Common Carriers, *available at* https://www.ecfr.gov/cgi-bin/text-idx?SID=1628649abb41d4b778be13a6c3bcc4e5&mc=true&node=pt47.3.42&rgn=div5

[6] See https://www.ctia.org/the-wireless-industry/wireless-industry

[7] Id.

[8] See, e.g. Lisa Marie Segarra, *Apple is Working on a Portal for Law Enforcement Requests*, Fortune, Sept. 8, 2018, *available at* http://fortune.com/2018/09/08/apple-law-enforcement-portal/

[9] House Report No. 112-169 (2011), Commerce, Justice, Science, And Related Agencies Appropriations Bill, 2012, *available at* https://www.congress.gov/congressional-report/112th-congress/house-report/169

[10] House Judiciary Committee & House Energy and Commerce Committee, Encryption Working Group, *available at* https://energycommerce.house.gov/newsroom/press-releases/encryption-working-group-releases-year-end-report

[11] House Report No. 115-231 (2017) Commerce, Justice, Science, and Related Agencies Appropriations Bill, 2018, *available at* https://www.congress.gov/115/crpt/hrpt231/CRPT-115hrpt231.pdf

[12] Christopher Wray, Director, Federal Bureau of Investigation - Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C., April 4, 2019, *available at* https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2020

[13] Major Cities Chiefs Association, 2019. Richardson, Tara. *Critical Issues for Intelligence Commanders: Preventing Terrorism and Targeted Violence and Maintaining Access to Digital Evidence*, at 43

[14] Deputy Attorney General Jeffrey A. Rosen Delivers Remarks to the National Sheriffs' Association, Louisville, KY, June 17, 2019, *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-jeffrey-rosen-delivers-remarks-national-sheriffs-association

[15] CSIS, *Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge*, at 10.

[16] Id. at 6.

[17] Attorney General William P. Barr Announces Creation of the State and Local Law Enforcement Coordination Section, May 17, 2019, *available at* https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-creation-state-and-local-law-enforcement