National Domestic Communications Assistance Center (NDCAC)

Executive Advisory Board (EAB)

Final Report to the Attorney General

June 2020

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

I. Executive Summary

This Third and Final Report to the Attorney General from the Executive Advisory Board (EAB) of the National Domestic Communications Assistance Center (NDCAC) provides a Legislative Principle Framework to further consideration of definitive next steps with respect to the issue of law enforcement's decreasing Lawful Access to evidence. The EAB's First Report[1] identified technical, resource-based, and statutory challenges faced by the Federal, State, local, and tribal law enforcement community concerning digital evidence. The Second Report[2] identified the general categories of challenges, described the factors influencing law enforcement's ability to address those challenges, and outlined approaches and types of solutions contemplated by the EAB. The Legislative Principle Framework proposed in this report provides NDCAC EAB members' advice regarding a general path forward for a comprehensive, strategic legislative approach to the Lawful Access issue for all Federal, State, local, and tribal law enforcement.

As a general matter, the NDCAC EAB supports the Attorney General's demonstrated intent to build upon the initiatives already undertaken by the Department of Justice. It is clear to members of the NDCAC EAB that the Department understands the Lawful Access issue based on the information highlighted on its Lawful Access webpage.[3] At the same time, the NDCAC EAB also expresses strong support for the December 2019 Lawful Access Resolution of the International Association of Chiefs of Police (IACP). That resolution referenced the position of Australia, the United Kingdom, and the United States for industry to "…embed the safety of the public in system designs…" and urged the adoption worldwide of "…appropriate regulation or legislation…"[4]

The NDCAC EAB is convinced Lawful Access to evidence is a critical issue that warrants and can only be resolved through affirmative legislative action. Law Enforcement's attempts to resolve the challenges through dialogue with industry alone have proven largely ineffective. The competitive nature of the industry discourages individual providers or group of providers from

---

[1] National Domestic Communications Assistance Center (NDCAC) Executive Advisory Board (EAB) Report to the Attorney General, October 2017. https://ndcac.fbi.gov/file-repository/eab-ag-final-report-20180119.pdf/view

[2] National Domestic Communications Assistance Center (NDCAC) Executive Advisory Board (EAB) Report to the Attorney General, July 2019. https://ndcac.fbi.gov/file-repository/second-report-to-ag-20190716.pdf/view

[3] https://www.justice.gov/olp/lawful-access

[4] *2019 Resolutions, Adopted December 2019*. International Association of Chiefs of Police, Resolution 21, page 45. https://www.theiacp.org/sites/default/files/Adopted%202019%20Resolutions__Final.pdf

initiating a solution for fear of losing market share to competitors who would not be required to adopt the same lawful access capabilities. Legislation is the sole mechanism which will level the playing field for all providers and will likely propagate similar legislative actions in other countries given the market dominance of U.S. providers. Ultimately, legislative action will result in more effective support provided to the Federal, State, local, and tribal law enforcement community by the NDCAC. It will also require more of the NDCAC as its technical know-how will be relied upon to educate industry on law enforcement's needs and educate law enforcement on technical solutions developed by industry. The time to move ahead with concrete steps is now and members of the NDCAC EAB look forward to working with the Department on this critically important issue to the entire law enforcement community.

A. Overview

Federal, State, local, and tribal law enforcement must convey its requirements with respect to lawful access to communications and communications data (evidence in motion) and stored data (evidence at rest). Law enforcement must also ensure its requirements for lawful access conform with the existing proportionality doctrine of the United States Constitution relative to a provider's duty to transfer to law enforcement only that data which falls within the scope of a lawful order. This document sets forth both law enforcement's high level principles and lawful access technical requirements. Establishing principles and technical requirements helps ensure lawful access while maintaining rigorous standards for the disclosure of transparent processes. The high-level technical requirements are basic technical definitions intended to identify and segregate discrete users and their communications and/or data and protect the privacy of users not subject to lawful access.

II. PRINCIPLES OF LAWFUL ACCESS

The following principles offer a general high-level framework for the capabilities and processes associated with lawfully-authorized collection efforts.

- Lawful access shall respect the right to privacy and freedom of expression as bounded by the United States Constitution;
- Lawful access shall be consistent with the authorities granted to law enforcement under applicable Federal and State statutes;
- Lawful access shall conform with the specificity and particularity requirements of United States Constitution so as to be proportionate to the information sought;
- Lawful access shall be supported by statutorily-mandated safeguarding and/or oversight structures to include a mechanism for ensuring compliance;
- Lawful access processes shall be simply and clearly explained;
- The capabilities and processes associated with lawful access shall be consistent with due process precepts of the United States Constitution; and
- Law enforcement shall have lawful access through an efficient and secure system.

III. GENERAL TECHNICAL LAWFUL ACCESS REQUIREMENTS

A. Scope of Requirements

Any entity subject to technical lawful access requirements must be specifically and unambiguously identified to include:

1. Providers of wire or electronic communications services not already subject to the Communications Assistance for Law Enforcement Act (CALEA), or Communications Service Providers (CSP);
2. Manufacturers of equipment, management and other software providers, data storage providers, and any other service necessary for the CSP to make its services available;
3. Communications and stored data user device manufacturers;
4. Remote Computing Service (RCS) providers; and
5. Operating System (OS) providers.

B. Technical Requirements

The following are general descriptions of requirements CSPs shall meet in creating, maintaining and executing those lawful access capabilities they design, implement and control for their own services and products:

1. Authentication[5] and Isolation: The CSP shall ensure to the maximum degree reasonably possible that only those communications associated with the subscriber or user's accounts, devices, instruments, equipment, facilities, or services are lawfully accessed by the provider and delivered to law enforcement. The CSP shall ensure that all data, which may lawfully be disclosed and which may be used to authenticate the communications as originating from or being destined to a specified subscriber or user is provided to law enforcement.
2. Proportionality: The CSP shall ensure that only communications of the identified subscriber or user or facility which are authorized for interception be provided to law enforcement.
3. Completeness: The CSP shall ensure all the subscriber or user's communications, both to and from the subscriber or user's equipment, facilities, or service, shall be provided to law enforcement for the entire period authorized by a lawful access order.
4. Transparency/Unobtrusiveness/Security: The CSP shall lawfully access communications services in such a manner that the subscriber or user cannot detect that his/her services are accessed. The CSP's lawful access capability shall also be undetectable to all non-authorized persons (e.g., employees, other users).

[5] Authentication is an aspect of security that, in this context, confirms the identity of a user.

5. Confidentiality/Access Control: Only authorized persons shall have knowledge of lawful access capabilities, related equipment, and access to communications and data in the service provider's network.
6. Correlation: The CSP shall ensure lawful access of specific communications is accomplished in a manner that provides the ability to associate the communication-identifying information with the communication to which it pertains.
7. Availability and Reliability: The CSP shall use appropriate performance and reliability mechanisms and parameters to enable lawful access to be performed in a manner that ensures that lawfully accessed data or information required to be provided to law enforcement will be timely transmitted will not be corrupted.
8. Location: When authorized, the geolocation information of the subscriber or user's device or facility shall be reported. If there are multiple forms of location information available, all shall be reported in accordance with the authorization.
9. Non-Repudiation: The CSP shall maintain sufficient records of service subscriptions to document that lawfully accessed communications were associated with the subscriber or user's equipment, facilities, or service.
10. Encoding/Encryption/Compression: If the CSP provides, controls, utilizes or facilitates its own or third party encoding, compression and/or encryption for the subscriber or user or at least is knowledgeable of this processing, the service provider must either transmit the communication content in a decoded, decompressed and/or decrypted form, or provide the information (e.g., encoding method, compression method, encryption keys) necessary to obtain the clear, readily comprehensible form of the communication content or communication-related information.
11. Non-Alteration of Communication Content: The CSP shall ensure against unreasonable alteration of the format of the communication content. The CSP must not intentionally alter the meaning of any communication content (other than what is necessary based on the requirement concerning encoding/encryption/compression).
12. Timing and Time Format: The CSP shall ensure lawful access to the subscriber or user's communications upon transmission to or from the subscriber or user's equipment, facility, or service is conducted in a manner that includes specification of the time zone as an offset from Coordinated Universal Time (UTC).

C. Data Retention Requirements

The following are general data retention requirements for CSPs to retain subscribers' communications identifying information and for providers of RCS to retain subscriber or user information:

a. Duration: CSPs and providers of RCS shall retain information for a period of 18 months.
b. Completeness: All information that identifies or assists in identifying a user or device accessing a CSP's or a provider of RCS service.

c. Authentication and authorization: Information reasonably necessary to assist in identifying and isolating a subscriber or user to the exclusion of all other devices and users.
d. Identifiers should include, but need not be limited to the following categories of information:
    1. Transactional logs that correlate public and local source and destination addressing information assigned to a subscriber or user for routing and addressing on public networks;
    2. Global Device Identifier, or similar unique identifier, used by providers to identify a subscriber or user or device or to authenticate a subscriber or user or device on a service offering and all information to correlate the global device identifier with any other identifier;
    3. Advertising Identifier used by a provider to identify a subscriber or user or device or to authenticate a subscriber or user on a service offering and all information to correlate the advertising identifier with any other identifier; and
    4. Any identifiers used by the provider to establish and maintain continuity of usage associated with the device or service offering.
e. Encoding/Encryption/Compression: Furnish the decoding, decrypting or decompression information necessary for lawful access to retained information in an intelligible format, if the means of encoding, encryption or compression was implemented or facilitated by the entity receiving an order.

D. Device-based Access Requirements

The following are general requirements for lawful access to a device (for a device manufacturer or an operating system provider):

a. Completeness: Furnish all information, facilities, and assistance necessary to access information stored on an electronic device or to access remotely stored electronic information.
b. Isolation: Ensure lawful access only to devices or information associated with the subscriber or user that is the subject of lawful process.
c. Encoding/Encryption/Compression: Furnish the decoding, decrypting or decompression information necessary for lawful access to stored data in an intelligible format, if the means of encoding, encryption or compression was implemented or facilitated by the entity receiving an order.

IV. Description of Implementation Specific Principles

A. Standards and Testing

It is important that both industry and the Federal, State, local, and tribal law enforcement community are involved in establishing foundational specifications to ensure transparency into the capabilities developed to ensure lawful access to evidence. To this end, a Lawful Access strategy should include elements of the following:

1. Provide for the standardization of capabilities developed by industry for similar services or products which comply with the technical requirements.
2. Mandate a role for law enforcement in the standards-setting process to ensure lawful access needs are incorporated into technical specifications.
3. Allow for the testing and validation of provider solutions at the discretion of the government.
4. Provide a mechanism for law enforcement to identify deficiencies in industry specifications with a neutral arbiter.

B. Lawful Access Systems Security and Integrity

Any entity subject to technical lawful access requirements shall institute processes, procedures, and/or systems to ensure the efficacy of lawful access methods.

1. An important aspect of ensuring lawful access to evidence is to protect subscriber or user privacy by requiring lawful access processes, procedures, and/or systems ensure that communications not authorized to be intercepted not be transmitted or provided to law enforcement or others. Entities shall ensure that lawful access can be activated only in accordance with a court order or other lawful authorizations and only by authorized personnel of a provider.
2. Entities shall integrate information security measures and controls to ensure the integrity, reliability, and availability of their lawful access capabilities.
3. Entities shall designate an officer or agent who shall be located within the United States, be available to receive lawful requests and legal process seven days per week and 24 hours per day, and timely respond to lawful requests and legal process reasonably and promptly.
4. Entities shall ensure lawful access is implemented at a location within the United States.

C. Enforcement and Penalties

Institute a mechanism for ensuring compliance (i.e., enforcement and penalties) based on factors deemed relevant:

1. The needs of Federal, State, local, and tribal law enforcement and impact on public safety, national security, and cybersecurity of a deficiency.

2. The reasonable predictability of the deficiency.
3. The commitment of resources to and persistence of good faith efforts made to date by a provider to remedy or mitigate a deficiency.
4. The specific adverse effects on the nature, cost, and operation of the service at issue.
5. Designation of a reasonable period of time and conditions for compliance.

V. CONCLUSION

The NDCAC EAB fervently supports the launch of a Lawful Access legislative strategy that will restore the decision-making process that evaluates and mitigates the public safety impacts and harms caused by emerging communications capabilities. Advancements in technology should not diminish our Constitutional due process-based structure that can ensure the founders' historic balance between personal privacy and society's need to lawfully obtain evidence in support of the maintenance of public safety and the timely delivery of justice for victimized citizens. To that end, we proffer as hopeful assistance our views on the broad principled parameters and technical requirement that could underlay such a strategy.

With this, our third and final recommendation report, the members of the EAB note that it has been both our pleasure and honor to have been of service to the Attorney General and the Department. We look forward to providing whatever service the Attorney General or the Department may in the future call upon us individually to provide.