National District Attorneys Association
Staff Contact: Frank Russo
703-519-1655 or frusso@ndaajustice.org
www.ndaa.org

June 23rd, 2020

The Honorable Lindsey Graham
Committee on the Judiciary
United States Senate
Washington, D.C., 20002

Dear Chairman Graham,

I am reaching out on behalf of the National District Attorneys Association (NDAA), the oldest and largest national organization representing state and local prosecutors in the country. Today, I write in support of the *Lawful Access to Encrypted Data Act*.

As you know, NDAA and its law enforcement partners have long sought a legislative solution to lawful device access and encryption that appropriately balances privacy and public safety. Our job as prosecutors is, in part, to protect the constitutional rights of all of our citizens, including those charged with crimes. Our Constitution provides a privacy right in peoples' homes and, of course, in their cell phones and computers. This right, however, gives way to a lawful search warrant backed by probable cause and authorized by a neutral and detached judge. Every day, law enforcement officers execute lawful court orders that allow them to search through the most intimate areas of criminal suspects' homes and effects.

Yet, technology companies have chosen to deny law enforcement lawful access regardless of the presentation of appropriate legal process and judicial decision in clear compliance with the Fourth Amendment. For victims across the United States, this means justice is delayed or denied as evidence sits locked on an individual's device or hidden on an end-to-end encrypted application. With the help of legislation like yours, prosecutors will be able to access this valuable information only when the constitutionally mandated probable-cause evidentiary standards are met. Our members are confident that your legislation will take the necessary steps to provide law enforcement access to both data-at-rest and data-in-motion, while upholding the constitutional privacy rights of our Nation's citizens.

The Senate Judiciary Committee's commitment to improving public safety, while respecting constitutional rights, has been displayed by hearings held on this issue over the past year. I participated on behalf of NDAA in a hearing on "Protecting Innocence in a Digital World" on July 9th, 2019. During this hearing, I highlighted the substantial risk the internet and online platforms pose to the wellbeing of our children. As I stated in my testimony to the Committee, "*If we want our law enforcement to investigate child exploitation, we must allow them to effectively execute search warrants on criminals' smartphones… by mandating cell phone companies comply with court orders and not evade them by refusing to provide give law enforcement security codes*." Following the hearing, the Senate Judiciary Committee came to the correct conclusion that additional hearings and, subsequently, legislation would be required to

ensure these online providers and technology companies take reasonable steps to protect the public that interfaces with their products on a daily basis.

Following the Committee's first hearing on the issue of digital challenges for law enforcement and prosecutors, the Senate Judiciary Committee once again addressed the importance of lawful access in a hearing on "Smartphone Encryption and Public Safety" on December 10th, 2019. NDAA Board Member and New York County District Attorney Cyrus R. Vance, Jr. participated at the request of the Committee and accurately summarized the reality facing law enforcement as they seek lawful access to digital evidence, testifying that, "*[t]he single most important criminal justice challenge in the last ten years is, in my opinion, the use of mobile devices by bad actors to plan, execute, and communicate about crimes. Just as ordinary citizens rely on digital communication, so do people involved in terrorism, cyber fraud, murder, rape, robbery, and child sexual assault*." At the conclusion of this critical hearing, Committee leadership asked technology companies and law enforcement agencies to discuss potential compromises to the problem of lawful access to encrypted smartphone data.

NDAA, alongside our partners in the New York County District Attorney's Office, the Santa Clara County District Attorney's Office, the New York City Police Department, and the United States Secret Service, traveled to Silicon Valley to meet with technology companies on February 24th, 2020 to improve avenues of dialogue and attempt to solve the fundamental problem of device inaccessibility. Representatives from our organizations had the opportunity to sit down with both Google and Apple to explore compromises that would provide law enforcement with lawful access for both data-at-rest and data-in-motion. The common theme from both Apple and Google was that any solution that interferes with maximizing device security was undesirable and unacceptable. Therefore, despite the good-faith efforts of both the companies and law enforcement representatives, it was our conclusion from these meetings that federal legislation remained the only path forward.

The introduction of the *Lawful Access to Encrypted Data Act* reflects the immediate need for a legislative solution to the issue of smartphone device encryption and lawful access to digital evidence. By accounting for detailed processes that require a valid warrant and court order, while also accounting for the resources needed to ensure that technology community is able to comply with these orders, your legislation represents a realistic path forward to solving this complicated problem.

We thank you for your tireless efforts to address the issue of encryption and lawful access and look forward to working with your staff to move this historic legislation forward.

Sincerely,

Duffie Stone,
President