January 22, 2020

Attorney General William P. Barr U.S. Department of Justice 950 Pennsylvania Avenue NW Washington, DC 20530-0001

## Dear Attorney General Barr:

We are a coalition of organizations and individuals from across the ideological spectrum working to protect election security and preserve the integrity of our election process. We write to express our concern with your recent comments calling on companies to weaken the encryption of personal electronic devices.<sup>1</sup>

Encryption is a critical tool for many aspects of our national security, including election security. It is vital that our nation's election systems have the strongest possible shield against malicious hackers, especially given the resources that hostile foreign powers could deploy to undermine confidence in our democracy.

Even in regard to electronic devices and communication systems for consumers, encryption provides strong protections for election security. The breach of personal devices and private communication systems can serve as stepping stones for malicious hackers attempting to infiltrate other sensitive systems, such as election systems. Further, the 2016 election showed that hostile foreign powers can cast doubt on our electoral process simply by targeting personal devices and private communications. Any effort to diminish the effectiveness of encryption will inherently diminish the security and, potentially, the integrity, of our elections. Hostile actors will likely direct similar efforts at campaign officials, political organizations, and politically engaged individuals in future elections. Additionally, an increasing number of the over 3 million eligible Active Duty Military & civilian overseas (UOCAVA) voters depend on encryption to safeguard their ballots when they are transmitted electronically

While encryption does not guarantee safety from all forms of malicious hacking, it is a vital safeguard to minimize risk. The Department of Justice has previously asked companies to create a "backdoor" through encryption that would be accessible to law enforcement—but it is simply not possible to create a "backdoor" that could not also be accessed by malicious hackers.<sup>2</sup> Reducing the effectiveness of encryption means opening the door to unauthorized access by good and bad actors alike.

We strongly urge the Department of Justice to cease its calls to undermine encryption, as weakening encryption will weaken our election security.

If you have any questions or wish to discuss this issue further, please contact Jake Laperruque, senior counsel at the Project On Government Oversight, at jlaperruque@pogo.org.

<sup>&</sup>lt;sup>1</sup> Katie Benner, "Barr Asks Apple to Unlock Pensacola Killer's Phone, Setting Up Clash," *New York Times*, January 13, 2020. <a href="https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html">https://www.nytimes.com/2020/01/13/us/politics/pensacola-shooting-iphones.html</a>. On January 13, 2020, Attorney General Barr asked Apple to unlock phones belonging to the shooter who killed several people at a naval air station in Pensacola, Florida, in December. Apple is unable to unlock these phones because of the encryption of its devices. The attorney general said Apple had given the government no "substantive assistance," and that "it is critical that the public be able to get access to digital evidence." However, as the *Times* noted, Apple said it had given "investigators access to the gunman's iCloud account and transaction data for multiple accounts."

<sup>&</sup>lt;sup>2</sup> Attorney General Barr's statements on January 13 are the latest in a series of similar statements from the Justice Department that companies should provide the government a "backdoor" through encrypted devices and communication systems. See, for example: Jack Corrigan, "DOJ Makes Another Plea for Encryption Backdoor," Nextgov, October 4, 2019. https://www.nextgov.com/cybersecurity/2019/10/doj-makes-another-plea-encryption-backdoors/160389/

## Sincerely,

Americans for Tax Reform

Center for Democracy & Technology

Digital Liberty

E. John Sebes, Chief Technology Officer, OSET Institute, Inc.

Freedom House

FreedomWorks

Gregory A. Miller, Chief Operating Officer, OSET Institute, Inc.

J. Alex Halderman, Director, Center for Computer Security and Society, University of Michigan National Election Defense Coalition

Philip B. Stark, Associate Dean, Mathematical and Physical Sciences, University of California Berkeley Project on Government Oversight

Verified Voting