HWG | HARRIS WILTSHIRE & GRANNIS LLP

CLIENT ADVISORY
July 26, 2019

Potential Shift in DOJ "Going Dark" Policy

Kent Bressie, Roy L. Austin, Jr., Adrienne Fowler, Shiva Goel, John Amaya and Robert A. Friedman

Attorney General William Barr delivered an emphatic call for government access to plaintext information at the annual International Conference on Cyber Security on Tuesday.

Companies in the communications and technology industries should take note. While there is nothing surprising about a federal law enforcement official pleading for expanded access to user communications, Mr. Barr's comments stand out and could signal a significant shift in Department of Justice (DOJ) policy.

A full-court press late in the game. Mr. Barr's remarks stand out because of their obvious coordination and the decisiveness of the departmental position announced. His speech came on the heels of a June 2019 meeting of the National Security Council Deputies Committee (NSC/DC) over developing a coordinated federal response to the "going dark" issue. Other high-ranking DOJ officials, including FBI Director Christopher Wray and U.S. Attorneys Geoffrey Berman and Richard Donoghue, echoed Mr. Barr's concerns throughout the week.

While past DOJ statements recognized that the right "solution . . . isn't so clear-cut" because of privacy and network security concerns, Mr. Barr's remarks were unambiguous. After balancing the "relative risks," Mr. Barr concluded that the "choice for society is clear": "warrant-proof encryption"—and presumably other "going dark" capabilities—ought simply to be eliminated from all "consumer products and services."

All remedies are on the table—legislative, judicial, and regulatory. The NSC/DC had been exploring "two paths" for expanding lawful access to plaintext information: (1) encouraging private-sector cooperation through statements of administration policy, and (2) pursuing legislation that would require companies to provide government backdoors.

Barr's remarks suggest that DOJ has transcended the NSC/DC debate, perhaps out of impatience. He stated that the "time to achieve" private-sector cooperation "may be limited," and explicitly recognized that we may never "end up with legislation" mandating lawful access to plaintext data. He also referred approvingly to legislative "and regulatory" solutions being pursued overseas. Thus, under Barr's watch, DOJ may not wait for the private sector to "cooperate" or for Congress to act. Instead, it may choose to push the boundaries of existing authorities more aggressively—and without necessarily waiting for the strongest test case.

Industry considerations. Perhaps nothing will come of this. But perhaps not. Either way, companies should be prepared to handle requests for unencrypted data—and to defend their responses in negotiations with law enforcement or even in court.

Regulatory proposals to expand the reach of the Communications Assistance for Law Enforcement Act (CALEA) also fall within the realm of possibility. CALEA requires "telecommunications carriers" to implement lawful intercept capabilities. It also requires manufacturers of transmission and switching equipment and providers of telecommunications support services to assist with such implementation as necessary. While CALEA contains a broad disclaimer of responsibility to decrypt user communications, that disclaimer is not unbounded, and its scope has not been litigated, at least publicly. Moreover,

Congress gave the FCC expansive authority to implement CALEA requirements, and specifically permitted the agency to expand the definition of "telecommunications carriers" to include additional services.

CALEA is not sufficiently flexible to give law enforcement access to the full range of information that DOJ desires. Nevertheless, without movement in Congress, DOJ may view FCC regulatory action as at least one tool in its arsenal. Indeed, Mr. Barr made specific mention of the statute in his remarks, claiming that it would be "absurd" for CALEA to mandate lawful intercept capabilities "for the purpose of obtaining content, while allowing tech providers to block law enforcement from obtaining that very content" through encryption. Moreover, in the past, DOJ and other law enforcement agencies successfully petitioned the FCC to establish government-friendly compliance standards, and to extend CALEA's reach to then-emerging services, specifically broadband internet access and interconnected VoIP services.

* * * *

HWG has extensive experience advising clients responding to law enforcement requests. Our team includes former federal officials with government experience on encryption and related cybersecurity issues, including a former U.S. Deputy Assistant Attorney General and Deputy Assistant to the President, a former senior advisor in the Department of Homeland Security (DHS) and member of the DHS Social Media Task Force, a former DOJ trial attorney who litigated high-profile cases related to cybersecurity and internet fraud, and a former senior policy advisor to the U.S. Ambassador to the United Nations.

For more information on lawful access requirements or legal issues relating to encryption, please contact any of the authors or the HWG lawyer with whom you regularly work.

This advisory is not intended to convey legal advice. It is circulated as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.