NATIONAL FRATERNAL ORDER OF POLICE

PATRICK YOES NATIONAL PRESIDENT JIM PASCO EXECUTIVE DIRECTOR

328 Massachusetts Ave NE | Washington DC 20002

(202) 547-8189 | www.fop.net | legislative@fop.net

9 December 2021

The Honorable Maria E. Cantwell
Committee on Commerce, Science and Transportation
United States Senate
Washington, D.C. 20510

The Honorable Roger F. Wicker
Committee on Commerce, Science and Transportation
United States Senate
Washington, D.C. 20510

Dear Madam Chairman and Senator Wicker,

I am writing on behalf of the members of the Fraternal Order of Police to advise you of our profound concerns with the nomination of Gigi B. Sohn to serve as a Commissioner on the Federal Communications Commission (FCC), and we urge the committee to contemplate the serious public safety considerations at issue here.

Specifically speaking, the FOP and many others in the law enforcement community at large are deeply troubled by the active and enthusiastic leadership role of Ms. Sohn as a board member for Electronic Frontier Foundation (EFF) in their forceful advocacy of end-to-end encryption and “user-only-access”—often referred to in the law enforcement world as "going dark." These new encryption methods for communications are causing Federal, State, and local law enforcement agencies to rapidly lose the capability to obtain information necessary to protect the public from crime and violence. This is because the service providers have embraced encryption technology that makes the encrypted data completely inaccessible—even from the providers themselves, hence the term “user-only-access.” Their continued advocacy of this technology and support for additional barriers and restrictions to prevent law enforcement from obtaining historically accessible information makes it extraordinarily more difficult for law enforcement to apprehend dangerous criminals and protect the public.

Despite the efforts of the FOP and other law enforcement organizations, neither Federal law nor the FCC has any kind of requirement for carriers to comply with law enforcement requests, even when lives are in imminent danger. We are apprehensive of Ms. Sohn’s stance on this issue based on her leadership role at EFF and because she has never moderated her extreme views on this subject.

We have worked with three consecutive Administrations and numerous Federal law enforcement agencies, including the Federal Bureau of Investigation (FBI), to address this issue—this is not new territory for us. The FOP has always weighed in on issues impacting public safety and homeland security. We are the largest and oldest law enforcement labor organization in the country—it would be irresponsible for us not to weigh in on a nominee who would, if confirmed, have such a profound impact on such a critical public safety issue.

In September 2021, Christopher Wray, Director of the FBI, testified before the House and Senate Homeland Committees at a hearing entitled, "Threats to the Homeland: Evaluating the Landscape 20 Years After 9/11" and devoted a part of his testimony to what the law enforcement community calls the need for "lawful access." He stated:

> *What we mean when we talk about lawful access is putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to legal process. We are not asking for, and do not want, any "backdoor," that is, for encryption to be weakened or compromised so that it can be defeated from the outside by law enforcement or anyone else. Unfortunately, too much of the debate over lawful access has revolved around discussions of this "backdoor" straw man instead of what we really want and need.*

He cited as an example the killing of three U.S. sailors at Naval Air Station Pensacola. Following the attack, the FBI was unable to access any information from the terrorist's phone for months because the service providers employed "user-only-access" technology and the phone used an app with end-to-end encryption. Despite lawful search warrants and the potential that additional attacks were imminent, it took the FBI months to retrieve that data from these devices.

In October 2019, Director Wray also noted that this was not just a Federal law enforcement problem:

> *As FBI Director, I've now visited all 56 of our field offices, and I meet frequently with law enforcement leaders from all over the country and around the world. I can tell you that police chief after police chief, sheriff after sheriff, our closest foreign partners, and other key professionals are raising this issue with growing concern and urgency. They keep telling us that their work is too often blocked by encryption schemes that don't provide for lawful access.*

Nor is this issue only of concern for domestic law enforcement; it is also an international issue. In July 2019, the governments of the United States, the United Kingdom, Australia, New Zealand, and Canada issued a communique which states:

> *[T]ech companies should include mechanisms in the design of their encrypted products and services whereby governments, acting with appropriate legal authority, can gain access to data in a readable and usable format. Those companies should also embed the safety of their users in their system designs, enabling them to take action against illegal content.*

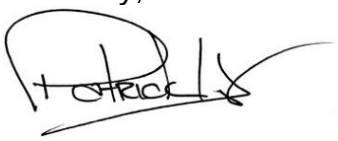
Law enforcement is sworn to protect the public by preventing, investigating, and prosecuting crime. Technology companies, like any other enterprise, also have responsibilities when it comes to public safety and cooperating with lawful and legitimate law enforcement orders. In our view, these service providers have an obligation to ensure that their terms of service for their users provide them authority to protect the public and to comply with lawful court orders. End-to-end encryption and "user-only-access" that precludes lawful access to the content of communications in any

situation creates a grave and potentially life-threatening risk. Yet, the EFF has been the tip of the spear in the effort to thwart lawful access to digital data and evidence. In their transition memo to the incoming Biden Administration, they recommended that the Administration oppose legislative efforts to ensure lawful access and to produce a formal Administration policy—presumably in favor—of encryption. Based on the fact that Ms. Sohn still holds a leadership position with the EFF, we have no confidence in her ability to objectively perform the duties of an FCC Commissioner.

It is for these reasons that we are urging you and the members of the Committee on Commerce, Science, and Transportation to reject the nomination of Gigi B. Sohn to the FCC.

On behalf of the more than 364,000 members of the Fraternal Order of Police, I thank you both for considering our views on this nominee. If I can provide any additional information on this matter, please do not hesitate to contact me or Executive Director Jim Pasco in our Washington, D.C. office.

Sincerely,



Patrick Yoes
National President