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

16 March 2022

The Honorable Margaret C. Hassan
United States Senate
Washington, D.C. 20510

Dear Senator Hassan,

I am writing on behalf of the members of the Fraternal Order of Police to ask that you vote ***against*** the nomination of Gigi B. Sohn to serve as a Commissioner on the Federal Communications Commission (FCC).

The FOP is very concerned that Ms. Sohn played such an active role as a board member of the Electronic Frontier Foundation (EFF)—an organization with some pretty extreme views on law enforcement technology. We are particularly troubled by their, and by extension, her, forceful advocacy of end-to-end encryption and "user-only-access"—often referred to in the law enforcement world as "going dark." 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. Because service providers have embraced encryption technology that makes the encrypted data completely inaccessible—even from the providers themselves—law enforcement agencies are prevented from obtaining historically accessible information, making it extraordinarily more difficult to protect the public, investigate crime, or prevent imminent violence.

For years, the FOP and other law enforcement organizations have urged the Federal government to develop and adopt standards for carriers so that they can lawfully comply with law enforcement requests, especially when lives are on the line and time is of the essence. 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. Christopher Wray, Director of the FBI, testified before the House and Senate Homeland Committees last September 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.*

Director Wray highlighted the need for lawful access in cases like 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 and other devices 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.

Director Wray also noted that this is not just a Federal law enforcement problem, nor is it just a national problem. It is the policy of the United States that technology companies should have the means to comply with lawful orders or requests for information. 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.*

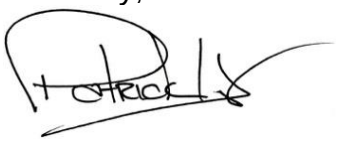
Technology companies have responsibilities when it comes to public safety, which includes cooperating with lawful and legitimate law enforcement orders, but the EFF has been the leader in the efforts to thwart lawful access to digital data and evidence. Based on the fact that Ms. Sohn holds a leadership position with the EFF, we have no confidence in her ability to objectively perform the duties of an FCC Commissioner.

We are also very troubled that the EFF has celebrated and lionized Edward J. Snowden, whom they characterize as a "whistleblower" and a patriot. The fact is that Mr. Snowden was entrusted with highly classified intelligence used to protect and defend the United States, and he chose to unlawfully share that data—putting American lives at risk and seriously damaging our national security. Mr. Snowden has been charged with three Federal felonies—including two counts of violating the Espionage Act. He is currently a wanted fugitive who has sought and received permanent residency in Russia and has applied for citizenship in that country. As far as we know, she has not distanced herself from those who believe this man to be a hero.

It is for these reasons that the FOP so strongly opposes this nominee. We urge you and all of your colleagues to vote ***against*** the nomination of Gigi B. Sohn.

On behalf of the more than 364,000 members of the Fraternal Order of Police, I thank you 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