Martin E. Hellman
Professor Emeritus of
Electrical Engineering

730 Alvarado Court
Stanford, CA 94305

Tel: 650.857.1377
Fax: 650.433.4248
hellman@stanford.edu

February 12, 2018

Senator Ron Wyden
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

I and my colleagues listed below are writing to you as experts in cryptography to thank you for your letter of 25 January to FBI Director Christopher Wray concerning his remarks on encryption at Fordham University.

We understand and sympathize with the frustration that law enforcement has to deal with when evidence may exist but cannot be accessed due to security mechanisms. At the same time, our extensive experience with encryption and computer security makes us cognizant of how much the details matter: a seemingly minor change in an algorithm or protocol can completely undermine the security aspects of the system.

The FBI has been urging Silicon Valley to build an “exceptional access” system to enable law enforcement to access encrypted communications and open secured devices under court order. But in asking for that capability, the FBI is asking engineers to design a highly complex, yet secure, system. Just because a non-technical person believes that such a system can be developed does not make it so. In fact, and as your letter notes, many experts have warned that security would be weakened by exceptional access mechanisms.

Thus your effort to find out with whom the Bureau has been consulting, and which cryptographic experts believe an exceptional access system can be built securely, is extremely important. Instead of vague proposals that sound reasonable yet lack details, the FBI needs to present the cryptographic research community with a detailed description of the technology that it would like implemented. That would allow the technology to be analyzed in an open and transparent manner so that its advantages and disadvantages can be weighed.

Thank you for your letter. We very much hope that the FBI will respond, and clarify the technical underpinnings of their requests.

Sincerely,

Martin E. Hellman, Professor Emeritus of Electrical Engineering, Stanford University; Member National Academy of Engineering; 2015 ACM Turing Award winner “for inventing … public-key cryptography.”

Steven M. Bellovin, Percy and Vida Hudson Professor of Computer Science, Columbia University; Member National Academy of Engineering; 2007 NIST/NSA National Computer Systems Security Award.

Paul C. Kocher, Member National Academy of Engineering; founder of Cryptography Research Inc.; designer of SSL 3.0 cryptographic and security functions.

Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School; author of "Applied Cryptography" and "Cryptography Engineering."