



warrant. The government could then use any information obtained that was considered evidence of a crime in either of these examples in domestic criminal assessments, investigations or prosecutions, and the bill fails to make clear that such use would require the government to fulfill its obligation to provide notice to defendants of the government's use of Section 702 data.

Second, the bill's current language leaves room for the government to conduct queries and access content for law enforcement purposes without a warrant. For example, the current language does not make clear that the government must have a warrant to access content for law enforcement searches where the purpose may not be to specifically obtain evidence of a crime, or in cases where there may be a dual foreign intelligence and criminal purpose. As such, the bill could still permit the government to conduct queries and access content without a warrant in cases involving criminal investigations and prosecutions.

Third, the bill's consent and emergency exceptions are too broad. For example, the emergency provision does not parallel analogous provisions in FISA and require imminence or that the government go back to the FISA court for a warrant after beginning the emergency surveillance. At the same time, the consent provision could be read to allow individuals who are not a party to a communication to consent to its access.

Fourth, the bill fails to require any court approval to access what it terms "noncontents" information. This is at odds with current law, including the reforms passed as part of the *USA F eed Ac* , which recognized the need for a court order to access metadata. Compounding this concern is the fact that the bill does not exhaustively list the types of

