SHOULD WE REQUIRE SOFTWARE COMPANIES TO PROGRAM IN "BACKDOORS?"

Why is Privacy Important?

The right to privacy is important and unalienable insofar as it allows for the free and open criticism and debate of the government. When it was famously released by Edward Snowden that the USA government was secretly and indiscriminately collecting all communication metadata in bulk, the response of many citizens was “Well, I don’t have anything to hide; what do I care if my metadata is being collected?”

The importance of privacy is not necessarily to protect citizen engaged in or plotting a criminal act, but rather to protect normal or “innocent” citizens from any state sponsored prejudice. It is to give citizens the right to organize, criticize, and plot against the government (in legal means only of course). Thus, even though they might be 100% satisfied with their governance at the present time, citizens, by word of the founding fathers themselves, need to have the ability to “dissolve the political bands which have connected them with another,” should it become necessary.

By this extension, communication between cell phones and other wireless devices needs to be 100% protected (encryption being one method) unless it can be proved that there is reasonable suspicion of a criminal act. In short, I would vote “NO” on a bill requiring Tech Companies to provide a “backdoor” for their communication hard and soft wares. The rationale here is two fold (listed in order of importance):

1. It is important to protect citizens from the government prejudice
2. The weakening of encryption security that a “backdoor” would entail
    - The more “solutions” there are to a code, the more “hackable” it becomes

To harp on the first of the above points, let’s assume a situation in which the US government is engaging in actions that its citizens deem inappropriate. They need to be able to voice and discuss these opinions free from governmental eyes. Again, this is not because this discourse itself is illegal, but because, if not kept 100% private between parties; it can lead to biases and prejudices. I have confidence that the government of the United States is not going to make dissidents disappear á la Argentina, the Soviet Union, and/or Chile in the late 70s/early 80s. However, exposure of this information or these opinions to the government could result in prejudices (potentially in the form of extra TSA screenings or extra scrutiny on government applications and/or taxes).

Exception Handling: Jury Questions

This is not to say that the government should not be allowed to break into phones under any circumstances. Quite the contrary, I agree that there are times (extenuating circumstances) when the government, with the assistance of tech companies, should be allowed into encrypted communication devices. One example of these events is the FBI wanting to get into the phone of the of the San Bernardino shooter’s phones. Why is this event deemed, as one that should bypass encryption and others are not? Simple – it’s a question for the courts. In the same way that the courts need to approve of a “Search Warrant” in order for an officer to enter the home of a suspect, a court order or Subpoena should be necessary for law enforcement to gain access to encrypted communication. This is why we have the courts and juries, to answer these “Jury Questions;” that is, have the public (under the guidance of our legal system) decide when access is required and when it is not.

Herein lies the major issue in the bulk metadata collection and the “backdoor.” It is indeed necessary, in certain situations; however, those situations need to be public record and approved by the courts. They cannot, as the “backdoor” implies, be an open source of information to be accessed based on the whim of any official. There needs to be a clear and present reason for the access, a decision which needs to be made, and made public, by the court system.

In conclusion, this debate, illuminated between Apple and the FBI, is an important one in terms of shaping the rights of US citizens in out rapid communication age. In looking to the answer for this question, we need to look to the founding fathers and parallels in other laws. It is indeed necessary for Congress to pass legislation on this topic but NOT one that says that all encrypted devices require a “backdoor.” Rather, it should state that, in the event that court approved probable cause exists, these companies should comply in helping the government gain access to the device in question.