MICHAEL CHERTOFF MAKES THE CASE AGAINST BACK DOORS

One of the more interesting comments at the Aspen Security Forum (one that has, as far as I've seen, gone unreported) came on Friday when Michael Chertoff was asked about whether the government should be able to require back doors. He provided this response (his response starts at 16:26).

> I think that it's a mistake to require companies that are making hardware and software to build a duplicate key or a back door even if you hedge it with the notion that there's going to be a court order. And I say that for a number of reasons and I've given it quite a bit of thought and I'm working with some companies in this area too.
>
> First of all, there is, when you do require a duplicate key or some other form of back door, there is an increased risk and increased vulnerability. You can manage that to some extent. But it does prevent you from certain kinds of encryption. So you're basically making things less secure for ordinary people.
>
> The second thing is that the really bad people are going to find apps and tools that are going to allow them to encrypt everything without a back door. These apps are multiplying all the time. The idea that you're going to be able to stop this, particularly given the global environment, I think is a pipe dream. So what would wind up happening is people who are legitimate actors will be taking somewhat less secure communications and the bad guys will still not be able to be decrypted.

> The third thing is that what are we going to tell other countries? When other countries say great, we want to have a duplicate key too, with Beijing or in Moscow or someplace else? The companies are not going to have a principled basis to refuse to do that. So that’s going to be a strategic problem for us.
>
> Finally, I guess I have a couple of overarching comments. One is we do not historically organize our society to make it maximally easy for law enforcement, even with court orders, to get information. We often make trade-offs and we make it more difficult. If that were not the case then why wouldn’t the government simply say all of these [takes out phone] have to be configured so they’re constantly recording everything that we say and do and then when you get a court order it gets turned over and we wind up convicting ourselves. So I don’t think socially we do that.
>
> And I also think that experience shows we’re not quite as dark, sometimes, as we fear we are. In the 90s there was a deb – when encryption first became a big deal – debate about a Clipper Chip that would be embedded in devices or whatever your communications equipment was to allow court ordered interception. Congress ultimately and the President did not agree to that. And, from talking to people in the community afterwards, you know what? We collected more than ever. We found ways to deal with that issue.
>
> So it’s a little bit of a long-winded answer. But I think on this one, strategically, we, requiring people to build a vulnerability may be a strategic mistake.

These are, of course, all the same answers opponents to back doors always offer (and Chertoff has made some of them before). But Chertoff's answer is notable both because it is so succinct and because of who he is: a long-time prosecutor, judge, and both Criminal Division Chief at DOJ and Secretary of Homeland Security. Through much of that career, Chertoff has been the close colleague of FBI Director Jim Comey, the guy pushing back doors now.

It's possible he's saying this now because as a contractor he's being paid to voice the opinions of the tech industry; as he noted, he's working with some companies on this issue. Nevertheless, it's not just hippies and hackers making these arguments. It's also someone who, for most of his career, pursued and prosecuted the same kinds of people that Jim Comey is today.

Update: Chertoff makes substantially the same argument in a WaPo op-ed also bylined by Mike McConnell and William Lynn.