

Keys Under Doormats: What's wrong with requiring government access to all data and communications?

Speaker: Ross Anderson FRS FREng

Tuesday 7 March, 5:30pm, MR2 (CMS)

The FBI Director Jim Comey and the US Attorney General Jeff Sessions want government access to stored data, to communications and to the cryptographic keys used to protect them. In Britain, the Investigatory Powers Act gives the Home Secretary wide powers to order such access. The scene is set for serious tussles over privacy between governments, the IT industry and others. How are we to make sense of all this?

We have been here before. In the "Crypto Wars" of the 1990s, the US government tried repeatedly to grab control of civilian uses of cryptography. Mathematicians suddenly found ourselves in the trenches in a battle that set freedom against state control, law enforcement against privacy, and countries against each other. We won Crypto War I. What are our chances in Crypto War II?

This talk is held by the C.U. Ethics in Mathematics Society

