Encryption and Globalization

Peter P. Swire

As cyberlaw first unfolded in the 1990's, encryption was a hot button issue, dominating conferences such as Computers, Freedom, and Privacy and the subject of intense popular and political mobilization. Broadly speaking, law enforcement and national security agencies supported limits on the export of strong encryption, in order to maintain their access to communications. On the other side, supporters of strong encryption included civil liberties groups, most academics, and high technology companies that wished to deploy strong encryption for the Internet.

The three stages of the debate in the U.S. were: (1) belief in the law enforcement and national security community that effective encryption should not be employed by civilians; (2) key escrow, through the controversial Clipper Chip, in hopes of enabling both strong encryption and access by law enforcement pursuant to court order; and (3) acceptance of the export of strong encryption. The Clinton Administration adopted the third position in September, 1999, and encryption law and policy largely faded from view.

Encryption issues are now re-emerging as a major topic, most visibly in India and China, but also in Russia and a wide range of other countries outside of Europe and North America. Indian law currently forbids encryption keys of longer than 40 bits, which is far below international standard use. Front pages in India and around the world have this year reported on the efforts of the Indian government to require RIM to change its architecture to allow wiretaps of Blackberry messages. China has adopted a different path for facilitating its government's access to communications. It is trying to insist that hardware and software made or used in China employ cryptosystems that follow Chinese standards, for which global security experts have not had the opportunity to examine the underlying algorithms. This approach is highly objectionable to most encryption experts, who accept Kerckhoff's law that public testing of encryption will lead to more effective security.

This paper examines the lessons from the U.S. debates in the 1990's for the new, globalized debates on encryption. The author chaired the White House Working Group on Encryption in the lead-up to the 1999 change in U.S. policy to adopt strong encryption. He also visited India in the spring of 2011 to meet with government officials, industry leaders, and others about approaches to India's current encryption rules.

The paper in part seeks to add to the literature a readable synthesis of the arguments that were most convincing in the 1999 switch of U.S. policy to supporting strong encryption. Along with arguments against pervasive government surveillance, one strong reason is that the Internet is a known unprotected channel of communication; any serious business or other action over the Internet, therefore, needs to use strong encryption. The paper will also explain the principle technical and legal weaknesses in the key escrow approach exemplified by the Clipper Chip.

In addition to building on the strongest arguments from the U.S. debate, the paper will explain reasons why weak encryption or government back doors are much riskier in a globalized setting of over 200 nations. The U.S. debate focused overwhelmingly on what was the best policy for one major nation, the U.S. One important reason to insist on strong encryption in the U.S. context was a lack of trust that one government, the United States, would escrow the keys safely or use its decryption powers wisely. On the Internet, whose architecture is based on messages being stored and forwarded by unknown intermediaries, there is exponentially greater risk that one of those 200 governments is untrustworthy or a non-nation state party in the middle will compromise security.

The paper will also place the global encryption debates into the context of the need for improved cybersecurity generally. The field of cybersecurity has developed enormously since 1999. Many of the basic precepts of cybersecurity are inconsistent with the weak security that results from weak encryption in communications.

In addition, the paper will address prominent objections to strong encryption, including the (in my view largely incorrect) suspicion that the U.S. government has secret back doors and so has the ability to routinely penetrate strongly encrypted messages.

In sum, governments in India, China, and elsewhere are implementing or contemplating encryption regimes that would weaken cybersecurity for literally billions of persons, and risk creating patterns for Internet communications globally that are far more prone to attack and interception than is desirable. The United States, after intensive debate, came down on the side of strong encryption and that decision has been stable for over a decade, even in the face of September 11 and other challenges. As a fundamental aspect of cyberlaw globally, it is important to set forth the reasoning to support strong encryption in countries that are now seriously considering the issue for the first time.