We actually lost the crypto wars

Dr. Christopher Kuner is Director of the Brussels Privacy Hub at the Vrije Universiteit Brussel (VUB) and an Honorary Professor at the University of Copenhagen, an Honorary Fellow of the Centre for European Legal Studies, University of Cambridge, and Senior Privacy Counsel in the Brussels office of the international law firm Wilson Sonsini Goodrich & Rosati. He is also editor-in-chief of the journal International Data Privacy Law published by Oxford University Press. In this post he looks at the crypto wars of the 1990s and argues that the Snowden revelations have shown that when it comes to the Internet, we can never be sure we have won privacy battles.

Those of you with a long memory may recall the so-called “crypto wars” of the 1990s that arose in conjunction with the first widespread use of the Internet. These were a series of efforts by the US and some other countries to mandate the use of “key escrow”, which would have required users of encryption technologies to deposit hardware and software keys used to encrypt communications on the Internet with the government, or to build “back doors” into them so that governments could gain access to encrypted data.

I experienced the crypto wars as an opponent of key escrow while working as a lawyer in Germany in the 1990s. The debate in that country and elsewhere was often heated, with law enforcement agencies arguing that key escrow was necessary to maintain their existing capabilities with regard to communications on the Internet. On the other side of the debate were privacy advocates and many (but not all) multinational companies, who opposed these plans.

The US took the lead in the push for mandatory key escrow in international bodies such as the Organisation of Economic Cooperation and Development (OECD), with the support of some other countries (in particular France and the UK). It took a while for the German government to wake up to the industrial and legal importance of this issue, but in the end its opposition proved crucial to undercutting the US government’s campaign (I have translated and posted on my web site a number of key documents regarding the crypto debate in Germany at that time).

In the late 1990s, the US government seemed to drop its key escrow campaign, as it became clear that a number of foreign governments (including Germany) would not support it, and as encryption companies based outside the US began to spring up (see in particular an interesting 1997 article from the New York Times regarding a German company I worked with called Brokat). Thus, it may have seemed at the time that those of us who opposed key escrow had won the crypto wars.

Too quick in presuming victory

The Snowden revelations have shown how naïve we were. No, governments in western democracies have not passed legislation obliging users of encryption technologies to deposit encryption keys with government agencies (at least as far as I am aware). But we have learned that law enforcement agencies are apparently accessing Internet communications on a massive scale notwithstanding the lack of the kind of key escrow framework that some governments lobbied for. Photographs have even been posted on the Internet purporting to show the NSA opening shipments of US-made IT equipment and then implanting bugs and tracking systems in them.

It is thus clear that law enforcement agencies and governments actually won the crypto wars, but did it so cleverly that we did not realize it. The fading of efforts to push mandatory key escrow was not an expression of defeat, but a shift in strategy prompted by a realization that governments could get the massive access to electronic communications data that they wanted without the public debate that the crypto wars produced.

I doubt that the undermining of public trust in encryption technologies and IT security that could have resulted from mandatory key escrow would have been any worse than the damage that has been done by the practices revealed by Snowden. IT companies are now faced with the nearly impossible task of proving a negative, i.e., that the technologies they offer have not been tampered with. These revelations have also seriously undermined trust in transborder data protection regulation (e.g., the US-EU Safe Harbor system, which has come into such disrepute in Europe that it seems to be on its last legs).

The plans put forward years ago for key escrow at least generated a lot of public discussion before they were enacted. But the information that has been emerging post-Snowden reveal that the details of how data access by the intelligence agencies is being carried out are so murky, and the legal theories under which they are conducted are so unclear, that I wonder if we will ever really know what has been going on. And the lack of trust produced by these revelations is fuelling initiatives to mandate local data storage, which may eventually lead to the Balkanization of the Internet.

The crypto wars of the 1990s were a notable episode in the history of Internet regulation, when many companies and privacy advocates worked together to oppose a regulatory scheme that would have been costly, ineffective, and invasive of civil liberties. However, they demonstrate that we can never regard the protection of privacy on the Internet as a problem that has been “solved”, and that we should be vigilant that one set of proposals is not replaced by other practices that may be even more insidious. The lessons of the crypto wars will thus have to be re-learned on a continuing basis.

This article gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics.

November 12th, 2014 | Featured, Guest Blog, Privacy | 1 Comment