# PGP creator defends right to encrypt emails

**Mike Ingram**
**1 October 2001**

Philip Zimmermann, the creator of Pretty Good Privacy (PGP) encryption software, has issued a statement aimed at clarifying his attitude towards encryption in the aftermath of the September 11 terrorist attacks in New York and Washington.

The statement, published on the technology site *Slashdot*, begins:

"The Friday September 21 *Washington Post* carried an article by Ariana Cha that I feel misrepresents my views on the role of PGP encryption software in the September 11th terrorist attacks."

Referring to a claim in the article that he was "overwhelmed with feelings of guilt", Zimmermann says, "I never implied that in the interview, and specifically went out of my way to emphasise to her that was not the case, and made her repeat back to me this point so that she would not get it wrong in the article. This misrepresentation is serious, because it implies that under the duress of terrorism I have changed my principles on the importance of cryptography for protecting privacy and civil liberties in the information age."

Zimmermann says that due to the political sensitivity of the issue, he had the reporter read most of the article back to him by phone, before she submitted it for publication. He insists, "the article had no such statement or implication when she read it to me. The article that appeared in the *Post* was significantly shorter than the original, and had the above-mentioned crucial change in wording. I can only speculate that her editors must have taken some inappropriate liberties in abbreviating my feelings to such an inaccurate soundbite."

He says he told Cha, "I felt bad about the possibility of terrorists using PGP, but that I also felt that this was outweighed by the fact that PGP was a tool for human rights around the world, which was my original intent in developing it ten years ago."

Speculating on the reason for the misrepresentation in the *Post* article, Zimmermann says, "It appears that this nuance of reasoning was lost on someone at the *Washington Post*. I imagine this may be caused by this newspaper's staff being stretched to their limits last week."

Zimmermann concludes his statement; "I have always enjoyed good relations with the press over the past decade, especially with the *Washington Post*. I'm sure they will get it right the next time."

Given the seriousness of the distortion that had appeared, this reporter contacted Cha to ask if the *Post* would be issuing a retraction of the article. Cha said in reply, "What I did not realise was that some people would take the idea that he was feeling 'guilty' would imply that he felt he did something wrong, despite the fact that the story says he doesn't feel he made a mistake. That was not my intention and I apologise for any misunderstanding. The way we were thinking about 'guilt' was simply in terms of people feeling bad or somehow responsible, even though there may be no reason for that.

She added, "I've talked to Mr. Zimmermann about this story several times since it ran—in fact the day after the story was in the paper he called me to thank me for it and tell me how much he liked it. He did not mention any possible problem until this weekend when he reached me at home." Cha said she accepted that Zimmermann, "needed to put out a statement to clarify that he had not changed his views that allowing the public to have strong encryption does more good than harm."

Whatever the facts about Zimmermann's initial thoughts on the article, his attributing the misrepresentations contained in the article to editorial laxity is clearly not credible.

The September 21 *Post* article was published amidst a concerted campaign by the Bush administration and a

compliant media to channel public opinion behind support for anti-democratic measures. The tragic events of September 11 have been used to mount a wholesale attack on civil liberties, one focus of which has been an unprecedented intrusion into peoples' online privacy. Under these conditions, it is hardly accidental that an interview commissioned with Zimmermann is slanted to paint a picture of the man responsible for the development of encryption consumed with grief and regret in the aftermath of the terrorist attack. Such an article fits in with the tenor of official propaganda insisting that so horrific is the tragedy, only the most insensitive would object to a necessary curtailing of civil liberties.

Zimmermann's public stance, as expressed in the *Slashdot* statement, is entirely justified. Saying that the *Post* article "showed that I'm not an ideologue when faced with a tragedy of this magnitude," he continues:

"Did I re-examine my principles in the wake of this tragedy? Of course I did. But the outcome of this re-examination was the same as it was during the years of public debate, that strong cryptography does more good for a democratic society than harm, even if it can be used by terrorists. Read my lips: I have no regrets about developing PGP."

Rather than the response to a terrorist outrage, the present moves to curb encryption and for closer monitoring of Internet use is the outcome of a long held desire by the security services to be able to monitor the movements and correspondence of every individual. Sections of the US political elite have never reconciled themselves to having been forced to abandon the so-called "escrow" plan, requiring decoding keys used for private messages to be given to the government. Neither have they accepted the December 1999 decision to abandon controls on the use of "strong encryption."

Writing in the *Online* section of the *Guardian* newspaper in Britain, Duncan Campbell exposes the claim that encryption played a key role in regard to the terror attacks in the US. Campbell writes, "FBI investigators had been able to locate hundreds of email communications, sent 30 to 45 days before the attack... The messages, in both English and Arabic, were sent within the US and internationally... According to the FBI, the conspirators *had not used encryption or concealment methods.* Once found, the emails could be openly read. [Emphasis added]

Campbell cites Dr Brian Gladman, formerly responsible for electronic security at the Ministry of Defence and NATO, who "believes that the reason that the terrorists didn't use encrypted emails is that would have 'stood out like a sore thumb' to NSA's surveillance network, enabling them to focus on who they were."

For the real reason for the calls for increased surveillance and a ban on encryption, one must look back to the period immediately prior to the terrorist attack when tens of thousands of people were protesting against the injustices of global capital in Seattle, Melbourne, Quebec and Genoa. It was then that media commentators and government spokesmen began talking about the role of the Internet in allowing people to organise on a global scale and demanded an effective means of preventing the free association of millions of people desirous of social and political change.