Ross Anderson, FIEE, FIMA
Reader, Security Engineering

Robert S. Mueller, III
United States Attorney
450 Golden Gate Avenue., Box 36055
San Franscisco, Ca 94102
Fax: (415) 436-7234

UNIVERSITY OF CAMBRIDGE

Computer Laboratory

July 26, 2001

Dear Mt Mueller,

The Sklyarov case

I lead the security group at Cambridge University. We are recognised as one of the leading research groups in the world in the field of information security.

The research that we do is scientifically important, useful, legitimate and benefits mankind. I wrote the seminal paper on peer-to-peer systems (‘The Eternity Service’) which has since led many companies – from Microsoft down to small start-ups – to work on mechanisms for large-scale distributed data storage and retrieval, in which hundreds of millions of users may share the spare capacity on each others’ hard disks for data backup. I coauthored the seminal paper on physical attacks on smartcards, which has led to a $2m EU research project to develop next generation smartcard processors – in which my team is a major player. I also coauthored the paper that introduced ‘soft tempest’ – the idea of reducing the compromising electromagnetic emanations from electronic equipment using software rather than hardware; this technique is already fielded in the flagship email encryption product from Network Associates Inc. and has the potential to save the military forces of NATO countries over a billion dollars a year. I also coauthored the seminal paper on the vulnerabilities of copyright marking schemes, which has led to a tool (Stirmark) that is now the industry benchmark for testing marking systems. Colleagues in my group coauthored the seminal papers on cryptographic protocols and on protocol verification.

The arrest of Dmitri Sklyarov is of extreme concern to me. Security research at an internationally competitive level is inherently an adversarial business; the field advances through a coevolution of attack and defence. Understanding and documenting the vulnerabilities of existing systems is critical to progress. The prospect that I might be arrested in the USA for research work done here at Cambridge University, and published in a responsible way through the usual academic channels, is alarming.

Computer Laboratory
New Museums Site
Pembroke Street
Cambridge CB2 3QG
England

Tel: +44 1223 334733
Fax: +44 1223 334678
E-mail: Ross.Anderson@cl.cam.ac.uk

The arrest has also alarmed many of my colleagues. I serve on the program committees of a number of leading international conferences, including the Information Hiding Workshop. The DMCA risks have persuaded my colleagues to hold the next workshop in Eindhoven, Holland, rather than at MIT. Another conference on whose committee I serve, the Fast Software Encryption workshop, was held last year in New York and this year in Tokyo; it is unlikely to return to the USA until the freedom of speech issues are resolved. Computer security and cryptography academics in Europe (and elsewhere) are getting the impression that the USA is becoming a hostile place.

A former student of ours, Igor Drokov, has known Dmitry Sklyarov for about ten years, and assures me that he is a talented researcher who is known as a law-abiding citizen rather than as a hacker/cracker.

I am concerned about reports that his arrest was due to a civil dispute between his employer and Adobe, Inc. If a law-abiding serious researcher can face arrest because his work is seen as inconvenient or harmful by a big US company, then many if not most of the top researchers in the field are at risk. For example, my smartcard work is conducted in partnership with the French company Gemplus and the Israeli company NDS. It poses a direct competitive threat to a US company, Atmel. If I publish an attack that breaks their product but not Gemplus's or NDS's product – even unwittingly – then can Atmel have me arrested? Will I be held without bail for years since – as a foreign national – I am considered to be a potential fugitive?

Many countries (including my own) encourage academics to work closely with industry, so that the fruits of research can be realised more quickly for the benefit of the whole economy. Is US policy about to provide a strong disincentive for people in the IT sector to engage in competitive and pre-competitive research? Our whole experience at Cambridge is that good research in science and technology tends to be driven by real problems; academics who retreat into theory tend to be much less productive.

I realise that neither you nor the FBI can change the law. However, I hope that you have, and will exercise, discretion not to prosecute in cases that are highly questionable or marginal, especially where these cases may cause international incidents, harm the US economy, and damage the excellent reputation that your country has earned for the defence of freedom of speech worldwide over the last two generations.

I have for years been an opponent of the anti-Americanism that becomes fashionable in Europe from time to time, and that unfortunately reared its head again recently at Genoa. The Sklyarov case does not help those of us who consider ourselves to be America's friends.

Yours sincerely,

Ross Anderson