Roche loses round in interferon patent battle

Tokyo. A small Japanese biotech company has won round one of a patent battle with Swiss drug company Hoffmann-La Roche over the former's mass-production of the cancer drug interferon using an unusual technique that employs tens of thousands of hamsters.

After three years of deliberations, the Tokyo District Court has rejected Roche's claim that Hayashibara Biochemical Laboratories, a company of 1500 employees in Okayama west of Osaka — as well as two Japanese drug companies marketing its product — are infringing its worldwide patent for interferon. But Roche is set to appeal against the judgement.

At stake is a sizeable slice of Japan's ¥150 billion (US $1.5 billion) market for interferon, which is used in the treatment of cancer and viral hepatitis.

With Hayashibara's technique, human lymphoblastoid cells are implanted into newborn hamsters which have been immunosuppressed so as not to reject the cells. The cells proliferate into a large lump which is removed after 3 or 4 weeks, killing the baby hamster. After separation, the cells are suspended in a sterilized culture tank and stimulated by Sendai virus to produce interferon, which is then isolated and purified.

Each year the company sacrifices around 50,000 hamsters in this way, to supply about 10% of Japan's interferon needs. But that share could double if, as expected, the company soon wins government approval to use its interferon in the treatment of patients infected with hepatitus C virus, which is prevalent in Japan and is powering rapid growth of the interferon market (see *Nature* **362**, 6; 1993).

Roche's lawsuit claims the Japanese companies are infringing a patent the company filed in 1978 for interferon based on the company's success in separating very pure samples of the material. And Roche claims this is a substance patent that covers Hayashibara's interferon regardless of the process of production or cell line used.

But Hayashibara says that both its production technology and its interferon are its original technology for which it holds patents. The company also rejects Roche's claim for a substance patent on the grounds that interferon was produced, purified and used for medical treatment long before Roche filed a patent.

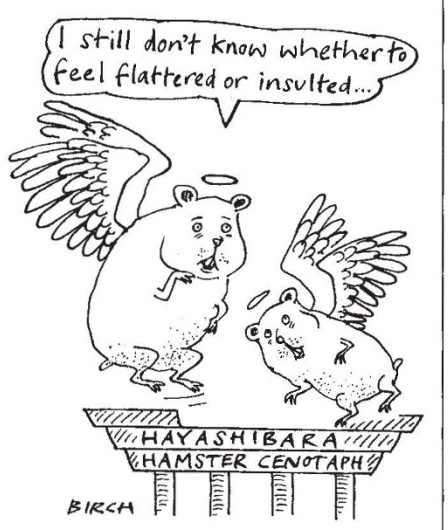
Hayashibara portrays the court decision as a victory for a small company against a big multinational that is trying to take control of a basic element of biotechnology. Eckart Gwinner of Roche's Swiss headquarters says it is "obvious" the company will appeal the court's decision. But, given the slow pace of the Japanese court system, the case seems likely to drag on for several more years.

David Swinbanks

Praying for baby hamster's souls

Employees at Hayashibara Biochemical Laboratories have an unusual way of purging feelings of guilt about sacrificing tens of thousands of baby hamsters to produce interferon.

Every month, workers from the company line up in front of a memorial cenotaph and a priest chants sutras for the souls of the departed hamsters. While clearly uncomfortable with the relentless killing, company officials point out that with an output of 20 to 40 million international units of interferon per hamster, the sacrifice of each hamster yields enough interferon to treat several human patients. D. S.



Spy interests wrecking Internet security, Congress told

Washington. US government fears about national security are blocking efforts to introduce up-to-date security measures for ordinary users of the Internet and other computer networks, a congressional hearing has been told.

Security problems on the Internet are spiralling, the hearing was told, with the arrival of so-called 'sniffer' programs which go out on the network and search for information, including passwords, giving computer hackers unlimited access to systems linked by Internet.

But Stephen Crocker of the Maryland-based Trusted Information Systems, a computer security specialist, told a hearing on Internet security before the House of Representatives science subcommittee that the US government's wish to stop the proliferation of encryption technology means that Internet users cannot protect their data.

"The government has a strong desire to be able to read the mail," said Crocker. "This takes precedence over security on the information superhighway." Crocker claimed that the National Institute of Standards and Technology (NIST), a government agency charged with releasing standard security protocols, faced a conflict of interest because it was also supposed to protect encryption technology for government use. "The government priorities are unfortunate, and unless they are changed they will damage computer security and retard the industry," he said.

Industry and government witnesses at the hearing agreed with Crocker that the ability of 'sniffer' programs to sniff out fixed passwords — driving a train through the sole security measure most computer users employ — meant that more sophisticated measures are urgently needed. The sniffers "signal the end of the usefulness of reusable passwords," says Dain Gary of Carnegie Mellon University.

These passwords could be replaced by devices that recognize signatures or fingerprints — or else by far more straightforward software-based encryption techniques which the government wants to keep for itself. NIST stands accused of wasting time by concentrating exclusively on the former set of techniques. Many in the computer industry believe that signature recognition is a red herring because it requires new hardware which the millions of users already hooked to the Internet do not have and will not buy.

Some witnesses at the hearing were also worried about the likely effects of the government's plans to keep tabs on phone and computer messages by backing a standard encryption chip known as Clipper.

Congressman Rick Boucher (Democrat, Virginia), chairman of the subcommittee, warned that security hazards on the Internet could mean that scientists "cannot be sure that their data will not be tampered with". But witnesses at the hearing acknowledged that most Internet users were oblivious to security risks. This view may change as the number of security incidents on the Internet continues to grow. **Colin Macilwain**