BRAD KING SCIENCE OCT 19, 2002 2:00 AM

Professor's Case: Unlock Crypto

A University of Illinois professor won't stop until cryptography is available free to the American masses. But the government isn't keen on deregulating a technology that helps terrorists and federal agents alike hide information. By Brad King.

SAVE

DANIEL BERNSTEIN SEEMS intent on striking the deathblow to U.S. government regulations on cryptography.

The latest chapter in his decade-long battle began to unfold on Friday, when lawyers representing both the Department of Commerce and Bernstein, a University of Illinois associate professor of mathematics, statistics and computer science, prepared to ask federal district court judge Marilyn Hall Patel to grant a summary judgment. At stake: the last remnants of a system that once prevented U.S. citizens from releasing software code that creates secure, electronic communications.

Bernstein is trying to eradicate the last of the export laws that previously kept Americans from distributing any work related to cryptography.

It's a bit confusing to some in the cryptography arena who feel that the current laws allow anyone to distribute their programs without fear of reprimand. Bruce Schneier, security expert and author of *Applied Cryptography,* said the future battle over encryption won't be trying to free software code, but rather preventing corporations from using it to limit rights.

"We always thought about cryptography as being a tool to protect the little guy versus the big guy," said Schneier. "It never occurred to us that the Digital Millennium Copyright Act would get passed."

Even with the looming fight over the DMCA, many are still uncomfortable with the court battle Bernstein continues to wage.

"When you empower people to do things, we empower them to do bad things," said Mike Godwin, staff council at the Center for Democracy and Technology. "It's a hard problem: What do you allow people to do in a free society? This is the hard part of democracy. You have to end up trusting people."

The problem, the government claims, occurs when the technology falls into the hands of people outside democracies. Earlier this year, for example, *The Wall Street Journal* bought a computer in Kabul, Afghanistan, that held encrypted files. The news organization broke the security -- with the help of the government -- revealing a wealth of information about al-Qaida activities.

The security was relatively easy to break, since the al-Qaida operatives who owned the computer used an off-the-shelf, 40-bit encryption program. However, if they had used one of the newer, more powerful encryption programs, those messages would likely have been lost forever.
That has been the heart of the government's fight to limit general access to cryptography for the last 30 years. It does this by requiring people to apply for a license called a commodities jurisdiction. Without this license, nobody can export any cryptography product, which includes publishing it on the Web -- and, for good reason, according to Stewart Baker, an affable Washington lawyer with Steptoe &amp Johnson.

Baker, who was general counsel for the National Security Agency from 1992 until 1994, said there is strong evidence, for example, that World War II was won because we had better cryptographers than Germany and Japan. Behind tight security at Fort Meade, Maryland, the NSA has teams of mathematicians and programmers working on the some of the world's most powerful supercomputers, making and cracking codes.

Making the knowledge freely accessible to everyone, Baker said, takes away one of the United States' strategic advantages.

Bernstein has repeatedly beaten back the government's attempt to restrict cryptographic technology. But, Baker said, much of that battle was waged during a different political climate.

"If it had come up 10 years later, this battle probably could have been won," Baker said. "But even then it would have been a very hard battle because there are so many valuable uses for encryption.... My guess is that at the end of the day, we would have ended up here."

Here is a place where very strong public encryption technology is available to the public, thanks to a handful of people, working in a loose collective led by Dr. Whitfield Diffie. The group developed their own system for secure communication that was so strong the NSA deemed it a threat to national security to sell it commercially. That started an epic battle between the government and the technology community, which is chronicled in Steven Levy's book *Crypto.*

The legal flare-up began in 1995 when Bernstein filed suit against the State Department, claiming the export laws that limited where academics could publish their research were unconstitutional.

With the help of Cindy Cohn, now a staff attorney with the Electronic Frontier Foundation, Bernstein successfully challenged the government's ability to restrict publishing code. In 1999, Patel agreed with Cohn. Three years later, the 9th Circuit Court of Appeals upheld Patel's ruling.

Since then, the government has eased restrictions on export technology, although the government still maintains the right to limit certain exports.

MORE FROM WIRED

The US Supreme Court Will Decide the Fate of Medication Abortion

The Supreme Court will hear a case to determine access to the abortion pill in the US. If the court decides to curtail the availability of mifepristone, it would be a major blow to reproductive health care.

KATE KNIBBS

A Brilliant COP Agreement? It Depends Who You Ask

The agreement at COP28 satisfies no one. But it’s probably the best that countries could have hoped for.

MATT REYNOLDS

Dr. Nergis Mavalvala Helped Detect the First Gravitational Wave. Her Work Doesn’t Stop There

The dean of MIT’s School of Science embraces skepticism and failure, and she wants the next generation of scientists to jump right in.

SWAPNA KRISHNA

Want to Store a Message in DNA? That’ll Be $1,000

French startup Biomemory is rolling out a credit-card-sized storage device that uses DNA to encode a kilobyte of text data.

EMILY MULLIN

Dr. Jessie Christiansen Wants to Help You Discover the Next Exoplanet

As project scientist on NASA’s Exoplanet Archive, Dr. Christiansen is a huge advocate for citizen science—and making sure anyone can be a planet hunter.

SWAPNA KRISHNA

Why Deleting Carbon From the Atmosphere Is So Controversial

Delegates just agreed on a historic climate deal at COP28. But without more ambition, humanity will have to rely ever more on a contentious strategy: carbon removal.

MATT SIMON

You Need a Heat Pump. Soon You’ll Have More American-Made Options

The Biden administration is announcing $169 million to supercharge domestic production of a device beloved by climate and energy nerds.

MATT SIMON

Insiders Say Eat Just Is in Big Financial Trouble

Vegan egg and lab-grown-meat startup Eat Just is being sued for more than $100 million. Former employees allege that's just the start of its problems.

MATT REYNOLDS