Pretty Good Privacy Gets Pretty Legal

No matter who's involved, public key encryption never fails to create its own controversy. While the US Congress and the National Security Agency duke it out with folks like Whit Diffie over where to draw the bounds of privacy, two of the leading figures in the encryption movement have been locked in a grudge fight over who has the right to provide public key protection to the masses.

It all comes down to a fight over Phil Zimmermann's program called Pretty Good Privacy, or PGP. Combining Diffie's concepts with patented algorithms that implement those concepts, Zimmermann created a personal computer-based program that renders files and electronic mail almost spy-proof. He then gave it away free. All well and good, except for one minor point: those patented algorithms had already been licensed to RSA Data Security Inc., which has no intention of letting Zimmermann corrode its markets.

In PGP's documentation, Zimmermann called his program "guerrilla freeware." Jim Bidzos, president of RSA and its sublicensee Public Key Partners, has called Zimmermann "an intellectual property thief. He offered to give away something that wasn't his to give." The 39-year-old Bidzos, a burly Greek national, could easily pass for a Hollywood version of an arms dealer – and that's how he's categorized under US law, which classifies cryptographic software as "munitions" and forbids its export.

Since its free release into the Net world in June 1991, PGP has become the bane of law enforcement officials, who say it lets criminals and would-be terrorists hide the evidence of their illegal activities. Recent, stronger versions of PGP have emboldened a new generation of civil libertarians and self-proclaimed cypherpunks, who say that strong cryptography is a fundamental requirement for free speech among law-abiding citizens in the electronic age.

Perhaps so. But, free speech or no, anybody who used early versions of PGP in the United States could be sued – not for trying to protect their privacy, but for patent infringement. The patent for the basic algorithm at the heart of PGP – the RSA public key encryption algorithm – is assigned to MIT, which has licensed it exclusively to RSA Data Security.

Unless you have a license, you can't distribute an invention based on someone else's patent, and Phil Zimmermann, PGP's 40-year-old author, didn't have one. But he gave away the software anyway, by passing it out on floppy disks to other people who, in turn, made it available for download on bulletin board systems around the Net. (For more on how Zimmermann created PGP, see "Crypto Rebels," *Wired* 1.2, page 54.)

Quick-tempered and unshakable in the belief that RSA Data Security is fighting the holy war to bring cryptography to the world, Bidzos has nevertheless tried to block PGP at every possible opportunity. Bidzos pressured online services like CompuServe and America Online to take copies of PGP off their systems. 165 ▸

Cypher Wars

◄129 He went after universities, demanding that they take PGP off their computers and keep it away from their students. But he could not keep the program from spreading: it was already on the Net and impossible to contain.

Early History

Before he released PGP, Zimmermann asked Bidzos for a free license for the patents. Bidzos refused, noting that he had already sold licenses to third parties and didn't want to undercut their business. Zimmermann says that he released PGP because the US Senate's 1991 omnibus crime bill had a measure buried within it that would have directed manufacturers of secure communications equipment to insert "trapdoors" into their products so that messages could be decrypted by the government. Releasing PGP, Zimmermann claims, was a preemptive strike against such an Orwellian future. (Zimmermann has since become the subject of a criminal investigation focusing on PGP's export overseas.)

After PGP's release, Bidzos and Zimmermann came to an agreement – of sorts. Bidzos sent Zimmermann a letter, saying that his company would not sue Zimmermann if Zimmermann stopped distributing PGP in the US. Because the RSA patent is in force only in the US, Bidzos had no way to stop the international distribution of PGP. Zimmermann signed the letter and sent it back. But soon thereafter, PGP cropped up again – this time on several ftp sites in Europe and Australia. Through the Net, those versions leaked back into the States. Bidzos says that Zimmermann broke the agreement. Zimmermann claims he did not.

However, Zimmermann will admit that he assisted an international team in the development of the second release of PGP. The program was released in the Netherlands.

Back in the United States, cryptography had gone from an esoteric branch of mathematics to front-page news. At the center of the controversy is the Clipper Chip, a key escrow-based encryption system that nearly became the government-approved standard for a wiretap-ready infobahn. "If we wake up one morning with 100 million Clipper phones, it doesn't matter what the laws are," says Zimmermann. Such a vision caused Zimmermann to increase his efforts to make PGP available to anyone who wanted it, particularly in the US. If only the RSA patent weren't in the way!

Détente

Help came to Zimmermann not in the form of a gang of crypto anarchists, but from the

Massachusetts Institute of Technology, the birthplace of the RSA public key encryption algorithm. Last year, Jeffrey Schiller, MIT's network manager, and James Bruce, both an MIT professor and its vice president for information systems, decided to work with Bidzos to find a way to get PGP out in a form that did not violate Bidzos's patents. "MIT had the strong belief that heavy-duty cryptography, or the ability to encrypt something so that it remains private, needed to be in the hands of the general public," recalls Bruce. "PGP met that need."

In January 1994, Bidzos met with Schiller, MIT Professor Ron Rivest (the "R" in RSA), and John Preston, who oversees MIT's Technology Licensing Office. But they could not come to an agreement. A month later, Phil Zimmermann met with Schiller and Bruce. Again, nothing came of it. Bidzos would not budge. Zimmermann did not have a license the first time he wrote PGP, and he was not going to get a free license now.

Then came the breakthrough. Amazingly, it was unwittingly handed to Zimmermann by the man who had been trying the hardest to stop him. While his sublicensee Public Key Partners had been fighting Zimmermann on the legal front, Bidzos's other company, RSA Data Security, had released a cryptography toolkit of its own, complete with free (but noncommercial) licenses to the same algorithms that PGP had violated. Called RSAREF, the kit was created by RSA Data Security as freeware to help people implement versions of an emerging Internet standard called Privacy Enhanced Mail. (Although PEM provides features similar to PGP, many people had been slow to adopt it because programs that implement the PEM standard are not widely available.) Early versions of RSAREF could only be used for PEM. But in March, Bidzos released RSAREF version 2.0, which contained enough programmatic "hooks" so that it could be used for other purposes as well.

"It became clear that you could build PGP on top of RSAREF," says Bruce, who is convinced that Bidzos never intended his program to be used for those purposes.

Seizing the opportunity, the MIT crew contacted Zimmermann with an elegant proposition: take the encryption engine from RSAREF and drop it in PGP. This way PGP would inherit RSAREF's license for the RSA algorithm in noncommercial applications. At long last, Zimmermann saw his chance to legitimize his guerrilla encryption program. He took the current version of PGP from Europe, version 2.3, ripped out the patent-violating software and plugged in RSAREF's patent-friendly code, dubbing it PGP version 2.5.

In early May, Schiller sent out a message on the Internet announcing that MIT "will shortly distribute PGP version 2.5, incorporating the RSAREF 2.0 cryptographic toolkit under license from RSA Data Security Inc. PGP 2.5 strictly conforms to the conditions of the RSAREF 2.0 license of March 16, 1994." But there was yet another hitch. Bidzos did not want any "unlicensed" copies of PGP in use. In a flurry of telephone calls and e-mail messages, Bidzos asserted that if MIT distributed PGP version 2.5, it would be inducing people with older versions of PGP to infringe upon PKP's patents, since version 2.5 worked with earlier versions of PGP.

Two weeks later, MIT announced that it would no longer distribute version 2.5, but rather a new, "improved" version 2.6. There were a few bug fixes, and at Jim Bidzos's request, this version was modified to work with RSAREF 1.0 rather than version 2.0. But the big change was this: after September 1, 1994, earlier versions of PGP – the ones that infringed upon PKP's patents – would not be able to read messages encrypted by version 2.6 (version 2.6 would still be able to decrypt files encrypted by earlier versions, however). Bidzos says "making trouble for Zimmermann is not the reason" he forced MIT to make the change. "If version 2.6 won't talk to infringing versions, you can't use it to induce infringement."

Zimmermann, predictably, feels otherwise: "I don't think that it was necessary to do it, but we did it anyway as an olive branch to Bidzos," he said.

"Finally we have been able to bring to the public a noncommercial version of PGP that really does not have any sword of Damocles hanging over its head – or over the head of its users," said Schiller. "Anybody in the US can get a copy of this, and RSA is not going to object."

Despite munitions export laws, PGP version 2.6 quickly made its way to Europe via the Net. Zimmermann sees the spread of PGP as a symbol of people's determination to defend their right to privacy. The solution, he claims, isn't fighting whatever key escrow encryption system eventually replaces Clipper as the government standard, but making something better. And, he adds, PGP is it. ■ ■ ■

PGP 2.6 is available from *ftp://net-dist.mit.edu /pub/PGP/*.
RSAREF is available on the Internet by sending e-mail to *rsaref@rsa.com*.

Simson L. Garfinkel's (simsong@mit.edu) *book about PGP will be published in November by O'Reilly & Associates.*