Coding Up a Bit of Privacy

Joshua Quittner

This must be how the Founding Fathers looked when they hacked out the Constitution : a roomful of young men, mostly - frazzled hair, eager eyes, wild beards, arms flailing and fingers jabbing the air, reaching for big ideas. You can't help but feel it; urgency tempers their voices. The earnest men plan and argue in this corporate conference room as the last sun rays of a winter Saturday afternoon fade in through a skylight.

Time is running out for the Cypherpunks. There is much work to be done before the information highway arrives. The information highway - that 500-channel shopping mall / cineplex championed by cable and telephone companies - is a noxious concept to the people in this room. They are not technophobes or Luddites, these Cypherpunks. Instead, they are a collection of clever computer programers, engineers and wire heads from some of the nation's best-known Silicon Valley software houses and hardware shops.

This is their central question : in a future world where all information is centralized on a network, where all information is tracked by the bit, where every purchase you make and every communication can be monitored by corporate America, how does privacy survive ? If you go to a bookstore now and buy a book, you can pay in cash. No one knows your name or what you purchased. "What happens to cash transactions on the information highway ?" they ask.

The Cypherpunks believe that they can preserve your privacy through good cyphers, or codes. But they must hurry, must get their codes out and their networks up and running. "The whole information highway thing is now part of the public eye", explains Eric Hughes, a founder of the Cypherpunk movement. "If we don't change it now, it'll be impossible later". The Cypherpunks know what technology is capable of. We visit them today because they represent one edge of the national debate on the structure of the information highway. And as we all know, extreme positions help define the middle.

Many of the Cypherpunks have been heavy Internet users for years and hope to preserve the communal spirit of that freewheeling world of interconnected computer networks. They dread the coming commercial network of televisions and computers, saying it will displace the Internet and destroy many of the freedoms they now enjoy.

So the Cypherpunks, with the kind of zeal they professionally bring to marathon, 72-hour sessions hacking computer code, are plotting to keep free networks alive. That's "free" in the sense of unfettered, unmonitored, uncensored.

One way they're going about it is by spreading easy-to-use, cheap cryptography. Cryptography is the science of keeping two-way communication private. Computers, it turns out, are revolutionary cryptographic tools, able to encode and decode files quickly. For the first time, virtually unbreakable codes are now possible, thanks to computers. The Cypherpunks post cryptographic software on the Internet where anyone can access it, and can encode their communications, including electronic mail, pictures and video.

But the U.S. government is concerned, as governments always are, about the spread of powerful cryptography (terrorists could use it, kidnapers could use it, drug dealers could use it, all of them on cellular phones that encode conversations). It currently is pushing its own commercial cryptographic standard, through a special chip known as the **Clipper**. The chip is reviled by Cypherpunks and other civil libertarians because it provides a

back door that law-enforcement agencies could enter, with the proper warrants, for surveillance.

By getting good, unbreakable cryptography out there now, the Cypherpunks hope, whatever the government finally decides will be moot. Software has a wonderful property, the Cypherpunks are fond of saying : once it's created, it can never be destroyed. It can be copied infinitely, from computer to computer, spreading like a secret. Come what may, unbreakable Cypherpunk code, and Cypherpunk networks, will be out there forever, they hope. But just to be safe, the Cypherpunks are toying with different network-related plans to create an economy of "digicash" - network money that, like the dollars in your pocket, isn't tied to a user's credit cards or other personal identification. Digicash will help pay for Cypherpunk networks and will allow people to purchase goods without revealing their identity.

"I'm starting a bank, and it's not going to be a U.S. bank", Hughes says. He's standing at the whiteboard now. A strawberry-blond ponytail dangles down his back and he grasps a magic marker in his hand. "We have several long-term strategies, one of which is the elimination of central banks". He tells the assembled crowd what they already know. Heads nod. Some people take notes.

Hughes is a self-employed programer in Berkeley. His hand flies across the whiteboard, sketching out a schematic diagram, showing how his bank will operate. The bank will store depositers' money (he's thinking a $200 minimum deposit) and disburse payments to anyone - all over the Internet. It will be based abroad, maybe in Mexico. A Cypherpunk network bank is one way to pay for a network of truly encrypted, private communications, you see.

"Is this going to lead the way to portable laptop ATM machines ?" someone asks in the back. People snicker. "Have you thought about its name ?" someone else asks. "First Bank of Cyberspace !" yells one person. "First Internet Bank !" yells another. "The Nth National Bank !" Laughter. Billy goat beards bob. There is much work to be done.