SEPTEMBER 3, 2019

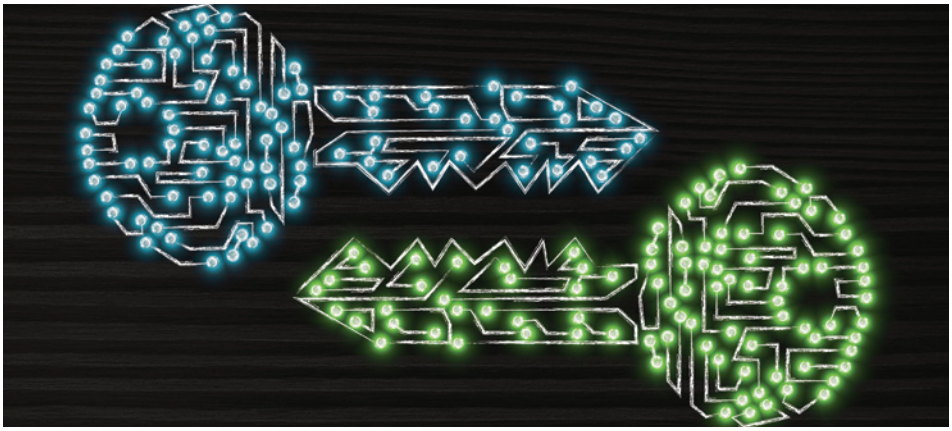
Legaltech news ONLINE

An ALM Publication

Nervous System: Clipping the Wings of the Clipper Chip

In this month's look at the history of cybersecurity, David Kalat examines the government's efforts to come to a consensus with government access to encrypted technologies, only for outside forces to get in the way.

BY DAVID KALAT, BRG



With the aggressive pace of technological change and the onslaught of news regarding data breaches, cyber-attacks, and technological threats to privacy and security, it is easy to assume these are fundamentally new threats. The pace of technological change is slower than it feels, and many seemingly new categories of threats have actually been with us longer than we remember. Nervous System is a monthly blog that approaches issues of data privacy and cybersecurity from the context of history—to look to the past for clues about how to interpret the present and prepare for the future.

As assistant deputy director of the National Security Agency (NSA), Clinton Brooks had watched with growing alarm the rise of strong cryptography. Part of the NSA's mission was to eavesdrop on foreign spies, but widespread use of encryption threatened to put it out of business. Brooks' "Eureka!" moment came in 1992. He had a crazy idea to solve the problem—*an idea so crazy, it just might work*, he thought, hopefully.

Brooks realized the problem was a fundamental tension between two competing public needs. On the one hand, an increasingly digital economy needed reliably secure communications; on the other, legitimate law enforcement needed the ability to conduct wiretaps. For years, the government had tried—ineffectively— to restrict the sale and distribution of cryptographic tools. Once cryptographic technologies began to circulate, they proliferated on their own outside the reach of regulations. Brooks proposed an "if you can't beat 'em, join 'em" solution that would actively encourage people to use encryption—but with a catch. Instead of each user owning her own unique keys, the government would keep a spare set of keys.

Brooks observed that the community most in favor of cryptography consisted of privacy advocates fearful of government surveillance. That community would never accept simply including a backdoor for government surveillance. So Brooks planned to include two enticements. First, this new NSA-approved cryptographic technology would be significantly more powerful than anything already on the market, and thereby would offer a material upgrade in privacy protection. Second, the government's key would be broken into halves, to be held in escrow by two separate agencies (the Treasury Department's Automated

Systems Division and the Commerce Department's National Institute of Standards and Technology). If, for example, the NSA wanted to take advantage of the back door

and decrypt a user's communications, it would first have to get court approval directing both agencies to share that user's key with the NSA for a specific, limited purpose. Unauthorized, warrantless wiretapping would be impossible. For most users, the escrow-based system would offer the highest level of security then available.

Both sides had to buy-in to have any hope of success. The law enforcement agencies had to stand in unison, and the idea had to be presented compellingly to the public. This would take a monumental act of public relations and a slow, prolonged public debate to develop mutual trust between governed and government. To Brooks' chagrin, events outside his control soon short-circuited that public relations campaign and all but ensured the plan would fail.

NSA technicians had developed a secure algorithm, called Skipjack, on which the new system would be based. To execute the complicated technical aspects in the most secure way, it was decided that Skipjack would be managed through tamperproof computer chips to be installed by manufacturers. All parties to any given encrypted communication would have to have these chips installed, and the chips would exchange critical information needed to establish and maintain the cryptographic channel, while also keeping a path open for the escrowed key to be deployed if authorized.

As the country approached the 1992 presidential election, however, no one's list of priorities included introducing a complicated debate about computer privacy. The creators of Skipjack expected to wait for the election to play out first.

Then came the surprise announcement that AT&T had developed a new encryption algorithm of its own, to be installed in new secure phones that were expected to sell in huge volumes to privacy-seeking customers. By the time the Skipjack chips were actually released, however far into the future, they would be an afterthought to a public already happily secure from government snoops.

The Federal Bureau of Investigations (FBI) was concerned that the AT&T phones would all but close off wiretapping options in the future. What self-respecting criminal wouldn't outfit themselves with one?

After some hasty engineering shortcuts to make stripped-down chips available quickly, FBI Director William Sessions personally called AT&T CEO Robert Allen to persuade him to retool the AT&T phones with these rush-order encryption chips, called Clipper Chips. AT&T agreed—so long as the key escrow provision became a national standard, for which AT&T would be a market leader.

Brooks' hope for a thoughtful national debate immediately fell by the wayside. There was no time to carefully build up public support. Instead, government policy had to follow an artificial timetable created by AT&T's production schedule.

Newly elected President Bill Clinton and Vice President Al Gore supported the Clipper Chip but were unprepared for the immediate and intense public opposition that the proposal met. No effort had been made to persuade consumers or businesses that this was a superior cryptographic solution, and the new administration had not rallied any influential voices to rally around the fundamentally problematic concept at its core. As Jerry Berman of the Electronic Frontier Foundation put it, "The idea that government holds the keys to all our locks, even before anyone has been accused of committing a crime, doesn't parse with the public."

Meanwhile, Matthew Blaze, a young computer scientist in AT&T's cryptology division, obtained access to prototype Clipper Chips for testing and discovered fairly quickly an easy, inexpensive hack that disabled the escrow key. In the rush to engineer the chips, some sloppy technological corner-cutting had left a critical vulnerability. The error was fixable, but a *New York Times* front-page story washed away the last slivers of public trust the Clipper Chip had enjoyed.

The passing of the Clipper Chip left agencies like the NSA and the FBI exactly in a world they had most feared—where the private use of encryption increasingly secured communications from government eavesdropping. It was a pointed lesson that the needs of law enforcement do not outweigh individual liberties, even in the digital age.

David Kalat *is Director, Global Investigations + Strategic Intelligence at Berkeley Research Group. David is a computer forensic investigator and e-discovery project manager. Disclaimer for commentary: The views and opinions expressed in this article are those of the author and do not necessarily reflect the opinions, position, or policy of Berkeley Research Group, LLC or its other employees and affiliates.*