Why We Can't Unscramble the Fight Over Encryption

Just hours before two gunmen, armed with assault rifles, opened fire outside an exhibition space in Garland, Texas, last May, one of them exchanged a blizzard of texts, 109 in all, with a third person–someone the FBI later identified as an "overseas terrorist." But that's where the trail goes dark. What did the messages say? Was the overseas terrorist giving instructions? Were other targets or accomplices mentioned? "We have no idea what he said because those messages were encrypted," said FBI Director James Comey, testifying before a Senate committee in December.

Technology known as end-to-end encryption, which is now embedded in apps like Apple's iMessage and Facebook's WhatsApp, makes it impossible to unscramble the content of messages intercepted in transit between users. That means that no one–not even law-enforcement officials or the engineers who created the encryption in the first place–can peek at personal conversations, giving a measure of comfort to millions who trust technology to keep their personal secrets safe from hackers and criminals.

But federal officials say the cost of that security could show up in the next terrorist attack. Which is why some of the Obama Administration's top brass and intelligence officials, including Comey, met in Silicon Valley on Jan. 8 with executives from Apple, Facebook, Twitter and Google. Among the agenda items was the question of encryption: Should tech companies be forced to equip their encrypted platforms with special "back doors" that allow government agents, armed with court orders, to peer in when necessary? Both sides left the meeting mum, but the battle is hardly over. Top tech CEOs have repeatedly promised that they will do nothing to weaken customer protections, while law-enforcement officials insist that spying on suspected terrorists would help them head off horrific acts of violence, like those last year in Paris and San Bernardino, Calif.

It's a powerful emotional argument, and lawmakers from both parties, including Senators John McCain and Dianne Feinstein, have taken it up, promising new legislation to force companies to "pierce" encryption under court order. Most of the 2016 Republican candidates have lined up behind that idea too, arguing that government agencies ought to be given the same access to text messages and data on cell phones that they can get by wiretapping a landline. Meanwhile, Democratic candidates Hillary Clinton and Bernie Sanders have been more circumspect, calling for a balance between civil rights and national security.

The problem is that the nation has been down this road before–and it doesn't lead anywhere good. In the '90s, the federal government launched a criminal investigation against cryptographic whiz Phil Zimmermann, who had developed an early encryption technology, on the grounds that he was exporting a "munition" that could harm national security. In response, Zimmermann published his source code as a book, arguing that he had a First Amendment right to free speech. Eventually the feds backed down and appellate courts supported this claim for later cases. The takeaway? You can't outlaw encryption technology any more than you can outlaw cell phones. The truth is that any technology can be used for good or ill–but once the genie is out of the bottle, it's out forever.

Cryptographers and tech-company CEOs are making the same argument today for strong encryption. Even if every American device was stripped of protected code or fitted with a back door, they argue, Americans would be no safer. In fact, they would be less safe, since hackers, cybercriminals or foreign agents could exploit the same back doors designed for law enforcement. Terrorists, meanwhile, could simply write new encrypted apps, or use different ones–like those made in Switzerland or Russia. It took me less than a minute to download and set up Threema, a Swiss encrypted messaging app, on my phone. Many of the top apps the Islamic State has recommended to its followers are not made in the U.S.

As cryptographer Bruce Schneier says, "I can't build technology that operates differently depending on your morality." It's an uncomfortable trade-off for a new century. And it's not going away anytime soon.

For more on these stories, visit time.com/ideas

This appears in the January 25, 2016 issue of TIME.