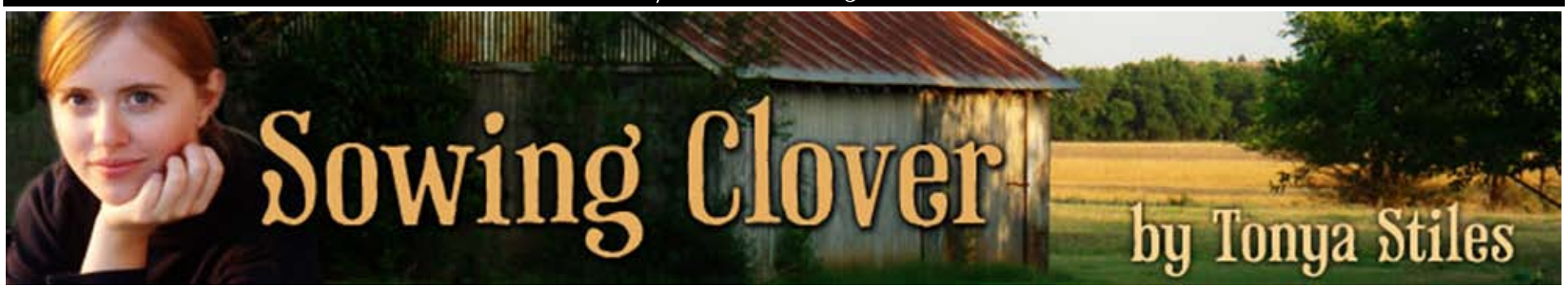


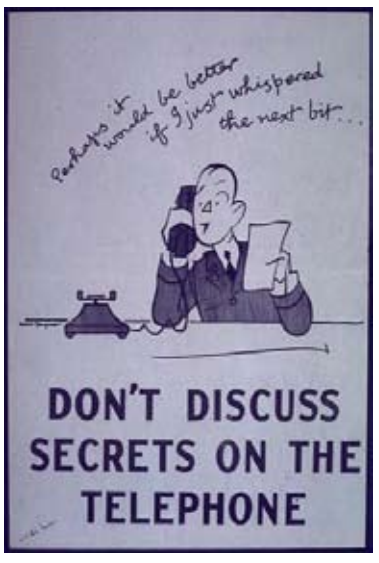
WHO CAN KEEP YOUR SECRETS?

"If privacy is outlawed, only outlaws will have privacy."
--Philip R. Zimmermann. Creator of PGP (Pretty Good Privacy) Encryption

A senate hearing like any other. The FBI Director leans down to his microphone and announces that he will be speaking today about a "vital public safety issue." He explains that law enforcement is united in its fear of the "looming spectre of the widespread use of robust, virtually uncrackable encryption." The only way to protect public safety is to give the government access to all encryption keys, allowing them to "unlock" encrypted communications in the course of "proper legal progress." Otherwise, encryption will "devastate our ability to fight crime and prevent terrorism."

Sound familiar? If you were watching the news in the aftermath of the November Paris attacks, it should. On November 18th, the current FBI director, James B. Comey, reiterated that "we're drifting to a place" where the government is "ineffective" in its attempts to access text messages and online communications, due to widespread encryption on smartphones. Comey has stated his desire to break encryption a number of times this year. He spoke before the Senate in both July and again in October, pressing for laws to force Silicon Valley to hand over encryption keys. And he wasn't making up his arguments on the fly. His predecessors practically wrote his script for him. The senate hearing referenced above? It took place in 1997.

And, in response to that 1997 effort to break encryption, a Senator from Missouri laid out a clear argument in opposition:



The primary tool in the arsenal of those who want to break encryption is the fact that most people don't understand what they're talking about.

"J. Edgar Hoover would have loved this...In a proposal that raises obvious concerns about Americans' privacy, President Clinton wants to give agencies the keys for decoding all exported U.S. software and Internet communications..Granted, the Internet could be used to commit crimes, and advanced encryption could disguise such activity. However, we do not provide the government with phone jacks outside our homes for unlimited wiretaps. Why, then, should we grant government the Orwellian capability to listen at will and in real time to our communications across the Web?

The protections of the Fourth Amendment are clear. The right to protection from unlawful searches is an indivisible American value...Every medium by which people communicate can be exploited by those with illegal or immoral intentions. Nevertheless, this is no reason to hand Big Brother the keys to unlock our e-mail diaries, open our ATM records or translate our international communications."

That Senator? None other than John Ashcroft, who would backpedal 180 degrees on that position once he was appointed Attorney General.

Ashcroft isn't the only ambivalent government official with regard to encryption. Hillary Clinton was a staunch advocate of strong encryption as Secretary of State, stating in 2010 that "Governments and citizens must have confidence that the networks at the core of their national security and economic prosperity are safe and resilient." She argued for the rights of dissidents in China and Iran to communicate securely, without fear of government surveillance.

But, floating with the tide of "official opinions" after the Paris attacks, she suggested that Silicon Valley companies should "compromise" with government on encryption. Citing warnings from law enforcement "that impenetrable encryption may prevent them from accessing terrorist communications and preventing a future attack," she suggested that the public and private sector "work together" to both "keep us safe and protect our privacy."

This sounds great, of course. Everyone wants both safety and freedom. That's why we have the Fourth and Fifth Amendments, after all. We want the government to be able to catch "bad guys" and we want for us, the "good guys," to be left alone. And as long as the argument is framed in such a way—to stop the "bad guys" from using the scary "encryption" technology to kill innocents—you'll find very few average folks arguing against it.

The primary tool in the arsenal of those who want to break encryption is the fact that most people don't understand what they're talking about. They don't know what encryption is, or how a weakening of encryption might hurt them. They're good people, right? So why would they need encryption?

Hopefully you've heard by now that, when buying something online, you should glance up at the web address and make sure it starts with an "https://" and not just an "http://" before entering any private financial information. You should also notice a small lock symbol next to the address. If you hadn't noticed this before, you were probably already protected without your knowing it. Most major shopping sites have been using HTTPS for years now.

And that sounds dangerous—as long as you operate under the assumption that there shouldn't be any communication that the government can't reach.

For the layman, the "S" at the end of HTTPS stands for "Secure" and it means that the site has added a layer of encryption over your communications. If the encryption is working properly, any third person trying to view the page would only see long strings of gibberish. To hide your information, the website uses either SSL (Secure Sockets Layer) or the newer TLS (Transport Layer Security.)

Essentially, encryption now works the same as it has for thousands of years. You have a message and you want to pass it to your neighbor, but, knowing your neighbor might leave the message lying around, you don't want anyone else to be able to read it. So you come up with a code to disguise your message and let your neighbor know the key to reading it. Assuming your key is known only to you and your neighbor, and is difficult for anyone else to guess, your message should be safe.

The "key" to unlock your encrypted data, using SSL or TLS, is a sequence of 256 ones and zeros, in a random combination. Since the number of possible combinations is 2 to the power of 256—a number so big that it can't be written out in numbers understandable to non-mathematicians—it would be impossible for any hacker to test all the combinations required to break the encryption.

So the weakness with this kind of encryption certainly isn't the key itself. The weakness, as it is when passing a message to your neighbor, is that once your neighbor knows the key to unlock the message, that key is no longer a secret. Your neighbor could write down the key someplace accessible to other people. He could slip up and mention it to his spouse, or he could keep it to himself perfectly well until it's coerced out of him by neighborhood thugs or even the police. That's why companies like Apple and Google have been moving to a form of encryption where they themselves do not have a key to unlock your data. That way, even if the companies are hacked by bad actors, or compelled by government warrants, they cannot betray you.

And that sounds dangerous—as long as you operate under the assumption that there shouldn't be any communication that the government can't reach.

First, for the sake of argument, let's assume that the U.S. Government is always interested in doing the right thing. If they are allowed to hold onto the keys for all encrypted information from American corporations, then they will have to store that information somewhere. Hackers from China and Russia have already proven their willingness to break into government serves. What would be a greater enticement to hackers than the

promise of a full store of encryption keys for the entire nation?

And what would be the argument for keeping other governments from storing that information as well? As long as no one can break certain forms of encryption, then dissidents in repressive countries have an assurance that their communication is secret. Members of our government can secretly aide pro-democracy efforts in China, Iran, and other countries without the fear of surveillance. But once we have American keys stored, then what's to stop China from making access to encryption keys the primary sticking point in our next trade negotiations?

Right now, with the newest forms of encryption, there is one door to access your data. And you are the guard of that door. You decide who enters this theoretical room of your secrets.

Now imagine the government shows up with a law saying they get to cut a back door into that room, and also you probably won't get any warning of when they might decide to enter. You might agree, thinking, "I'm a law-abiding person. What do I have to hide?" But now, as you're guarding your front door, that back door is always waiting, outside your view, and you don't know how sturdy the lock is. So, now your secret room doesn't feel so secret anymore.

And then let's acknowledge the fact that we can't always trust our government to do what's right—-particularly those members of the government overseeing "security." We know that the FBI monitored Anti-Vietnam War protesters, and Civil Rights leaders in the 60s. We know that the Pentagon monitored Anti-War protests in the buildup to the invasion of Iraq, including Quaker meetings. They kept tabs on Occupy Wall Street. And we know, as recently as this year, that the government monitors members of Black Lives Matters.

Would you attend a protest if you knew your name would be recorded, and that the government would later track your movements and your social media accounts? That is the reality of life as a Black Lives Matter protester—and those are the forms of surveillance that the government admits to, as part of their "legal" role in protecting public safety. Whether the protesters are actually monitored more closely, through the processes of less public government agencies, we don't know. But we can trust that, when a tool exists, it will be used. And the opponents of encryption are fighting to give surveillance agencies yet another, infinitely more powerful, tool in their arsenal.

Here is the fundamental question: should there be truly private communication in this world? Should you be able to shut a door, close your curtains, and feel safe in the knowledge that you are truly alone. In the past, that privacy was assured. No government could hear what you whispered behind your hand. No government could sit an agent in every root cellar and attic to hear every private conversation. Communication was primarily a physical act, and there were always ways to be alone. But now that we primarily talk through our electronics, where is that private place? When the government can retrieve millions of emails as they're sent and search through them for keywords, where do you have a "private conversation?"

Encryption is the only closed door still recognized in the modern world. And we all need to consider what we might lose before we hand over the key.

Tonya Stiles is the co-publisher of the Canyon Country Zephyr.