Imagine owning an impregnable safe, which is to say no manner of subterfuge or skill is capable of accessing the safe’s contents without explicitly knowing the combination. To achieve this level of security the safe is not only cleverly designed, but the dial contains 256 different numbers and the combination must be at least 32 long. This presents you with a conundrum: either choose a truly random combination and write it down, or pick one you can commit to memory. The former case burdens you with the problem of protecting the combination from theft and the latter with the possibility that the combination is guessable. Either way, you make yourself vulnerable to a determined thief. Fortunately, there is another option for protecting your valuables. You can store them in a safe deposit box at your bank, using the bank’s (presumed) superior security in place of your own. With the bank’s stringent requirements for proving identity, you can even feel secure if your safe deposit key is stolen.

This vignette exactly describes the state of encryption today. The role of your safe is played by the Advanced Encryption Standard, a time-tested and international standard for encrypting everything from your online purchases to governmental Top Secret communications. Your various Internet service providers, from social media to email, play the role of the bank. They securely store your information and assure that all your transactions, such as sending and reading email, are protected from eavesdroppers.

Encryption alone does not make this possible, because there remains the sticky problem of making it possible to reliably and securely share the “safe combination” between both sender and receiver. The sender needs it to encrypt messages (i.e., put the message in the safe), the recipient to decrypt them (i.e., remove them from the safe). Fortunately, some beautiful mathematics called Public Key Cryptography makes this possible. Think of Public Key Cryptography as a special safe with two doors and two different, but mathematically linked, combinations. The safe works like this: the front door of the safe opens to reveal a slot through which an encryption combination can be deposited. The safe contents can only be retrieved by opening the second door. With such a safe in hand, one can publish the combination to the front door of his Public Key Cryptography safe for all to see. To send a message, you use the recipient’s publicly available combination to deposit your encryption combination through the slot, and send the safe to the recipient. The recipient opens the rear door, recovers the combination, and now both of you can encrypt and decrypt messages with the encryption combination you hold in common. There are several variations of this two-door safe that go by acronyms such as DH, RSA and ECDH. All have specific combination sizes to guarantee impregnability and, as for the Advanced Encryption Standard, are time-tested and codified in international standards.
Virtually all Internet encrypted communications use this model of secure encryption coupled with one of the choices of Public Key Cryptography described above. Put simply, communications that follow these standards are completely secure in transit.

This leaves the issue of what to do when messages arrive. Whether you host your own data, or trust it to a service provider, there is a choice to be made: either store the data unencrypted or encrypt it with a 32-long combination (the term of art for this is a “key”) that must be protected.

Over the last few years a public policy debate has gained steam to codify the role and responsibilities of service providers to provide access to keys and messages in the case of being served a warrant. Similarly, there is a debate to define the authorities, laws, and oversight for government agencies in issuing and executing these “cyber” warrants. In essence, service providers want to get out of the business of providing user information and have proposed they get out of the “bank” business altogether. More specifically, they want all encryption to be “end-to-end,” which means the sender and recipient negotiate the encryption exclusively; the service provider holds no keys. Serving them warrants would only result in delivering impregnable encrypted messages. The government and various law enforcement agencies want the ability to access such messages in cases for which they can successfully argue to a judge a warrant is justified. The service providers argue that they cannot compete globally with providers in other countries that do not hold keys. Similarly, law enforcement agencies fear losing a powerful tool in the fight against crime and terrorism.

Lost in these arguments is the responsibility that may befall to average individuals to store and protect keys on everything from their smartphones to laptops and tablets. With end-to-end encryption users must protect their own data (and encryption keys) using software and devices over which they have less and less control. Indeed, according to a recent Ponemon Institute study, fifty-three percent of U.S. corporations have no confidence in their ability stop hacking.

What confidence can you have in protecting your own devices from hacking? Will this spawn a new generation of ever more sophisticated hacking software aimed at user devices? What authorities does government have or seek to have in such a scenario? In a future blog post I will delve into this debate and lay out the some of its consequences for you and me.

Michael Wertheimer is a School of Public Policy professor of the practice. Wertheimer previously served as director of research for the National Security Agency (NSA). In 2009 he was selected as technical director for the Data Acquisition Office in the NSA’s Signals Intelligence Directorate.

Prior to that, he was the assistant deputy director and chief technology officer of the Office of the Director of National Intelligence for Analysis. Wertheimer oversaw the coordination of intelligence community efforts to bring increased depth and accuracy to analysis through technology.

Wertheimer spent two years in industry building a research group focused on the intelligence community. From 1982 to 2003 he was a cryptologic mathematician at the National Security Agency where he trained in the design and analysis of cryptology with special emphasis on cryptanalysis digital signals processing, reverse engineering, software development, supercomputing and algorithm optimization.

Wertheimer received his PhD and MA in mathematics from the University of Pennsylvania. He received BA degrees in mathematics and philosophy from the University of Rochester.