Written by **C. Mitchell Shaw** on October 17, 2020

Anger and Courage: Protecting Privacy

metamorworks/iStock/Getty Images Plus

In the ongoing war to maintain liberty, one of the main battlegrounds is that of privacy in the digital age. With powerful computers running powerful algorithms to data-mine everything from everyone and compile it into startlingly accurate profiles, it is easy to lose hope. With lawmakers pushing for more and more surveillance of more and more people, it is easy to lose hope. But there is hope.

St. Augustine of Hippo (354-430 A.D.) wrote, "Hope has two beautiful daughters. Their names are anger and courage; anger at the way things are, and courage to see that they do not remain the way they are." This writer has often said that the issues surrounding the Surveillance State are both political and technological and require a two-pronged solution: While pressuring lawmakers to unmake the Surveillance State, concerned citizens should also learn to use digital tools to protect privacy.

While it is necessary to pressure lawmakers to begin dismantling the apparatus of the Surveillance State, it would be foolhardy to think that politicians who have built their careers building it will suddenly have a "Damascus Road Conversion" and burn the bridges they crossed to get to the powerful places where they now find themselves. It is a fact that one will never slay a beast while suckling its teat. The representatives, senators, and state legislators who have been complicit (or worse) in the illegal spying that has targeted law-abiding citizens know what side their bread is buttered on.

So, at the same time that citizens work for changes to enforce the Constitution's prohibitions against warrantless surveillance (whether that means pressuring existing legislators or replacing them with liberty-minded legislators), it is also their prerogative (and even duty) to use the tools at their disposal to block such surveillance.

To that end, a recent article published by *Reason* addresses the importance of encryption in protecting privacy from government spying. The article — part of a series — begins with a warning from *New York Times* reporter David Burnham from a 1983 C-Span interview. Burham, who had just released his book *The Rise of the Computer State*, said, "Large bureaucracies, with the power that the computer gives them, become more powerful" and "are escaping the checks and balances" put in place to protect liberty.

Burham added to that warning, saying that the world was headed into a "level of automated surveillance unknown in any previous age." In both his book and his C-Span interview, Burham urged

people to work toward a political solution. Others at the time — many of whom would come to be known as cypherpunks (not to be confused with cyberpunks) — placed their hopes for protecting privacy from the ever-watchful eye of Big Brother on a recent breakthrough in the field of cryptography. That breakthrough was public-key encryption.

In 2016, this writer wrote an article for the print edition of this magazine. In that article — later published online — I wrote about the first round of what have been called the "Crypto Wars." From that article:

> In 1991, a 37-year-old software engineer named Phil Zimmermann wrote an encryption program called Pretty Good Privacy (PGP). PGP allowed anyone with a fairly modern computer and the ability to follow instructions to encrypt their e-mails in such a way that (1) the e-mail could be read only by the intended recipient, and (2) the e-mail could be digitally "signed" in such a way that the recipient could be sure it was sent by the sender and not by an imposter. He made it available for download on the Internet — which was fairly young, but quickly growing. He also published the source code of the program in old-fashioned book form and directly exported that book all over the world.
>
> Zimmermann — and those using his new encryption standard — quickly ran into a problem. The U.S. government classified as a munition any encryption program strong enough to actually work, and banned its export. Since the Internet made it possible for anyone in the world to get their hands on a copy of the program (and also made it impossible to prevent them from doing so), Zimmermann soon found himself under criminal investigation by the U.S. Customs Service for alleged violations of the Arms Export Control Act.

Michael W. Lucas literally wrote the book on PGP. In the introduction to his book *PGP & GPG: Email for the Practical Paranoid*, he explains how — by directly exporting the source code in book form — Zimmermann turned what the U.S. government had treated as a software issue into a free speech issue:

> Zimmermann originally wrote PGP in boring old everyday text (or "source code"), just like that used in any book, and used computer-based tools to convert the human-readable text into machine-readable code. This is standard practice in the computer industry. The text is not software, just as the blueprints for a car are not a car. Both the text and the blueprints are necessary prerequisites for their respective final products, however. Zimmermann took the text and had it published in book form.
>
> Books are not considered software, even when the book contains the "source code" instructions for a machine to make software. And books are not munitions; although many books on cryptography did have export restrictions, Zimmermann could get an export permit for his book of source code. Thus, people all over the world were able to get the instructions to build their own PGP software. They promptly built the software from those instructions, and PGP quickly became a worldwide de facto standard for data encryption.
>
> As you might guess, the US government considered this tactic merely a way to get around munitions export restrictions. Zimmermann and his supporters considered the book speech, as in "free speech," "First Amendment," and "do you really want to go there?" The government sued, and over the next three years Zimmermann and the administration went a

> few rounds in the courts.

Zimmermann and the federal government went back and forth in both the investigation and subsequent lawsuits. In the end, Uncle Sam realized that the courts were likely to consider the dissemination of the written code behind the software as protected speech. Rather than risk a verdict — and a precedent — that might make the export of encryption software legally acceptable in almost any case, the federal government dropped the case and relaxed the standards for exporting software used for encryption. In 1996, President Clinton issued Executive Order 13026, essentially removing encryption from the munitions list. This was hailed as the end of the Crypto Wars, and privacy was declared the victor.

But — where government overreach is concerned — it's never quite that easy.

While the cypherpunks and others were early to adopt encryption, it was nearly 20 years before it caught on for most. Only after the Snowden revelations did companies such as Apple and Google start making encryption the default for iPhone and Android. Soon, other devices and services began offering public-key encryption. These days, public-key encryption is part of e-mail services such as ProtonMail and StartMail and text services such as Signal. It is used by millions everyday to protect their privacy, but the Crypto Wars are far from over.

Nearly 10 years before the vicarious legal victory of Zimmerman for everyone who would wind up using public-key encryption, mathematician Chuck Hammill wrote a paper in 1987, arguing that technology, not political action, would be the savior of privacy. In that paper, titled *From Crossbows To Cryptography: Techno-Thwarting The State*, Hammill wrote:

> I certainly do not disparage the concept of political action [but] for a fraction of the investment in time, money and effort I might expend in trying to convince the state to abolish wiretapping and all forms of censorship—I can teach every libertarian who's interested how to use cryptography to abolish them unilaterally.

Again, it's never quite that easy.

Because while many became comfortable with Hammill's idea of ditching the political battle and using "cryptography to abolish" all of the ways the Surveillance State spies on everyone, the political machinery of the Surveillance State has been steadily pushing to reverse Zimmerman's victory. Bills to demand backdoors into encryption are introduced in nearly every session of Congress. And encryption is steadily blamed for allowing terrorists and criminals to "go dark" and child abusers to hide in plain sight.

So, clearly ignoring the political part of the fight is not panning out. Yes, public-key encryption is unbreakable and will protect both data at rest (stored on a hard drive) and data in motion (communications), but if it becomes illegal again, it will offer no protection.

This is where hope's two beautiful daughters come into play. Concerned Americans need to be angry about the way the Surveillance State is and have the courage to see that it does not stay that way. While using tools to protect privacy, they also need to work diligently to protect the right to continue using those tools. That means pressuring lawmakers at every level to vote for laws protecting encryption and against any law that threatens it.