GlobalResearch
Center for Research on Globalization

The Death of Privacy: Government Fearmongers to Read Your Mail

By Philip Giraldi
Global Research, July 11, 2019
Strategic Culture Foundation

Region: USA
Theme: Law and Justice, Police State & Civil Rights

It is discouraging to note just how the United States has been taking on the attributes of a police state since 9/11. Stories of police raids on people's homes gone wrong are frequently in the news. In one recent incident, a heavily armed SWAT team was sent to a St. Louis county home. The armed officers entered the building without knocking, shot the family dog and forced the family members to kneel on the floor where they were able to watch their pet struggle and then die. The policemen then informed the family that they were there over failure to pay the gas bill. Animal rights groups report that the shooting of pets by police has become routine in many jurisdictions because the officers claim that they feel threatened.

Indeed, any encounter with any police at any level has now become dangerous. Once upon a time it was possible to argue with an officer over the justification for a traffic ticket, but that is no longer the case. You have to sit with your hands clearly visible on the steering wheel while answering "Yes sir!" to anything the cop says. There have been numerous incidents where the uncooperative driver is ordered to get out of the car and winds up being tasered or shot.

Courts consistently side with police officers and with the government when individual rights are violated while the Constitution of the United States itself has even been publicly described by the president as "archaic" and "a bad thing for the country." The National Security Agency (NSA) routinely and illegally collects emails and phone calls made by citizens who have done nothing wrong and the government even denies to Americans the right to travel to countries that it disapproves of, most recently Cuba.

And traveling itself has become an unpleasant experience even before one sits down in the 17 inches of seat-space offered by major airlines, with the gropers of the Transportation Security Administration (TSA) acting as judge, jury and executioner for travelers who have become confused by the constantly changing rules about what they can do and carry with them. The TSA is now routinely "examining" the phones and laptops of travelers and even downloading the information on them, all without a warrant or probable cause. And the TSA even has a "little list" that identifies travelers who are uncooperative and flags them for special harassment.

Congress is considering bills that will make criticism of Israel a crime, establishing a precedent that will end freedom of speech, and the impending prosecution and imprisonment of Julian Assange for espionage will be the death of a truly free press. Americans are no longer guaranteed a trial by jury and can be held indefinitely by military

tribunals without charges. Under George W. Bush torture and rendition were institutionalized while Barack Obama initiated the practice of executing US citizens overseas by drone if they were deemed to be a "threat." There was no legal process involved and "kill" lists were updated every Tuesday morning. And perhaps the greatest crimes of all, both Obama and George W. Bush did not hesitate to bomb foreigners, bring about regime change, and start wars illegally in Asia and Africa.

The latest assault on civil liberties relates to what used to be referred to as privacy. Indeed, the United States government does not recognize that citizens have a right to privacy. Officials in the national security and intelligence agencies have reportedly become concerned that some new encryption systems being used for email traffic and telephones have impeded government monitoring of what information is being exchanged. As is often the case, "terrorism" is the principal reason being cited for the need to read and listen to the communications of ordinary citizens, but it should be observed in passing that more people in the US are killed annually by falling furniture than by acts of terror. It should also be noted that the federal, state and local governments as well as private companies spend well in excess of a trillion dollars every year to fight the terrorism threat, most of which is completely unnecessary or even counter-productive.

At the end of June senior Trump Administration officials connected to the National Security Council met to discuss what to do about the increasing use of the effective encryption systems by both the public and by some internet service providers, including Apple, Google and Facebook. Particular concern was expressed regarding systems that cannot be broken by NSA at all even if maximum resources using the Agency's computers are committed to the task. It is a condition referred to by the government agencies as "going dark."

Under discussion was a proposal to go to Congress and to ask for a law either forbidding so-called end-to-end encryption or mandating a technological fix enabling the government to circumvent it. End-to-end encryption, which scrambles a message so that it is only readable by the sender and recipient, was developed originally as a security feature for iPhones in the wake of the whistleblower Edward Snowden's exposure of the extent to which NSA was surveilling US citizens. End-to-end makes most communications impossible to hack. From the law enforcement point of view, the alternative to a new law banning or requiring circumvention of the feature would be a major and sustained effort to enable government agencies to break the encryption, something that may not even be possible.

In the past, government snooping was enabled by some of the communications providers themselves, with companies like AT&T engineering in so-called "backdoor" access to their servers and distribution centers, where messages could be read directly and phone calls recorded. But the end-to-end encryption negates that option by sending a message out on the ethernet that is unreadable.

Phone security was last in the news in the wake of the 2015 San Bernardino, California, terrorist attack that killed 14, where the Department of Justice took Apple to court to access a locked iPhone belonging to one of the gunmen. Apple refused to create software to open the phone but the FBI was able to find a technician who could do so and the case was dropped, resulting in no definitive legal precedent on the government's ability to force a private company to comply with its demands.

There is apparently little desire in Congress to take up the encryption issue, though the National Security Council, headed by John Bolton, clearly would like to empower government

law enforcement and intelligence agencies by banning unbreakable encryption completely. It is, however, possibly something that can be achieved through an Executive Order from the president. If it comes about that way, FBI, CIA and NSA will be pleased and will have easy access to all one's emails and phone calls. But the price to be paid is that once the security standards are lowered anyone else with minimal technical resources will be able to do the same, be they hackers or criminals. As usual, a disconnected and tone-deaf government's perceived need "to keep you safe" will result in a loss of fundamental liberty that, once it is gone, will never be recovered.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Philip Giraldi is a former CIA counter-terrorism specialist and military intelligence officer and a columnist and television commentator. He is also the executive director of the Council for the Interest. Other articles by Giraldi can be found on the website of the Unz Review. He is a frequent contributor to Global Research.

Featured image is from Wikimedia Commons
