

Smart Guns and Government

by

Phil Rasmussen

Like many technological advances, the concept of “Smart Guns” began in the minds of science fiction writers. But what is a “Smart Gun?”

According to Wikipedia, a smart gun is a firearm that can only be used by an authorized user(s). These types of guns typically use RFID chips, biometric detection systems, magnetic rings, or mechanical locks. Their purpose is to prevent accidental shootings, usage by persons not authorized to use the guns.

This coming December, America’s first commercially available “Smart Gun” will be released to the general public. The gun, a 9mm caliber, is manufactured by Biofire and uses fingerprint and 3D facial recognition biometrics.

While the debate on gun control goes back to our nation’s founding, it wasn’t until Kennedy’s assassination in 1963 that it became a controversial and emotional political issue driven by gun control lobbyists, the left, and socialists.

Part of the gun control narrative, for decades, has been the push for smart guns. This narrative was bought to the forefront in 2016 by president Obama when he released the findings of DOD, DOJ, and Homeland Security on ways to spur smart gun development.

Smart guns, though seen as a means to prevent accidental shootings, prevent their use by criminal elements, and to ensure that US military firearms are not used by our enemies, are problematic in three major areas – costs, legal issues, and more important, functionality.

Costs

Whenever technology is integrated with non-technical items, the cost increases dramatically. For example, in 1956 the automatic industry was reluctant to install seatbelts into cars because it was difficult to install and back then cost \$30 a pair. Adjusted for an average 3.68% per year inflation rate, the price increase today would be 1,023.86% or \$337.16. The seat belt replacement cost today is between \$150 - \$200 **per** belt.

The cost of buying a Biofire smart gun in December is very high - \$1,499. This is far more than the cost of a comparable 9mm which is \$400-\$800. That is a 187.38% increase above a \$800 standard semi-automatic.

Like the cost of cell phones, smart guns advocates will say that with time the costs will go down as more and more smart guns are manufactured. The problem with this scenario is multi-faceted. For example, the cost of component parts will increase, additional features will be added, overall manufacturing costs will also increase due to outside influences such as insurance, laws and regulations.

Like car and appliance makers, gun manufacturers may look at repair and maintenance, replacement parts and upgrades as a major revenue stream.

Legal Issues

From a legal aspect, firearm laws fall under two jurisdictions, the federal government and state governments. Federal law however does not set safety or design standards for domestic firearms manufactures. However there is considerable push by gun control groups, the left, and socialists to do so. Will this happen? It is likely there will be an attempt to do so, perhaps not directly but rather using circuitous means. While ATF may be involved, we need to remember that most consumer products are regulated by the Consumer Product Safety Commission (CPSC), even though they currently have no authority to do so. Remember Congress and the Executive branch have a history of being sneaky.

Currently only three states have laws addressing smart guns. They are: Maryland, Massachusetts and New Jersey. The laws in these states are broadly worded and will probably come under scrutiny once smart guns are available to the general public. No doubt other states will address smart guns as they become more available.

However, there are many other issues for users, manufacturers, and states.

George W. Bush signed a law that gave broad immunity from lawsuits for gun manufacturers and sellers. At that time, firearms were mechanically driven. However smart gun technology makes guns become both mechanical and technology driven. Consider a computer. The keyboard is mechanical and the technology is the software that allows the keyboard to operate properly. If the keyboard malfunctions, there is little legal recourse. However, if the software malfunctions or is hacked and send your personal data to the dark web, there is a degree of legal recourse. Smart guns operate much in the same way. Consequently, the Bush's law may be overturned and open manufacturers and sellers to litigation for smart gun failures.

Many states currently have laws regarding the securing of firearms in homes and vehicles. These laws do not cover smart gun technology. When a population believes

that technology will protect them, people become lacidasical in maintaining proper security management. Biofire has a photograph of their smart gun sitting in a desktop cradle similar to a phone recharging cradle. Such photos cause people to think that they no longer have to secure the firearm in a locked box. Should the firearm be fired by someone not authorized for it, then the manufacturer and seller can be legally at risk.

Just as smart phones have tracking technology built into them, it is reasonable that smart guns will eventually have similar technology. This technology will allow any smart gun to be tracked by owners **AND** the government. Additionally, if blockchain technology is incorporated, an electronic record of how the guns are used will be kept. Such technology is being applied to firearms, ammunition and other materials as the Arms Trade Treaty aims to regulate the international trade of conventional arms. Currently barcodes are being used but there is no reason why RFID cannot be used, especially in light that RFID is used in tracking imports into the United States.

One other legal aspect of smart gun technology is that such guns will not prevent acquisition by criminals or people intent on carrying out mass shootings. It is naive to think that smart guns will prevent mass shootings. It may become possible to incorporate ethically correct Artificial Intelligence (AI) into smart guns.

There are many other legal issues with smart guns. However, in the long term, the paramount issues will revolve around the 2nd Amendment. The 2nd Amendment, a constitutional right, is embedded in the Bill of Rights. Unknown or forgotten by many, the Bill of Rights is protected under the 14th Amendment as these rights are "deeply rooted in this Nation's history and tradition" and therefore must be shielded from any government infringement.

Functionality

According to UK's Daily Mail, "The companies see the technologies as a way to reduce suicides, render lost or stolen guns useless, and offer safety for police officers and jail guards who fear gun grabs." Others see them as a means to prevent accidental discharges and children from being shot while playing with an unattended gun.

As mentioned several different approaches have been considered for making smart guns. All of these approaches are flawed. It is a well known fact that anything devised by man, can be hacked, and this is very true with regard to smart guns. In fact for all its technology, the Armatix IPI smart gun was hacked in 2014 using 3 magnets, a screw and a piece of wood.

Another problem with the IPI was that it required 20 minutes to pair with the watch and still needed a minimum of seven push-button commands and a duration of 12 seconds before the gun can be fired, according to the NRA. That is an awful long time when someone is firing at you and you need to defend yourself.

RFID chips or magnetic systems, and mechanical locks are problematic as these systems require a secondary device to activate the smart gun. If the device is not readily available or takes too long to activate, then why have it other than to possibly prevent an accidental death. These approaches do absolutely nothing but hinder your use of a gun if you need it for self defense.

Some companies, such as LodeStar, are integrating biometrics with “a near-field communication chip activated by a phone app, plus a PIN pad.”

Biometric approaches are equally problematic. While these approaches can unlock a gun in microseconds, they rely on two specific conditions – a. a biometric reader that actually works correctly, and b. the battery in the gun has enough juice to activate the reader and the mechanical locking pin.

Biofire integrates two biometric systems into its 9mm smart gun. One is a fingerprint reader and the other is facial recognition. The concept is that if one fails, the other one is used. In 2021 five different fingerprint hacks were discussed on the internet. Any one of these hacks can be applied to Biofire’s gun.

Further, anyone can find how to hack facial recognition biometrics on the Internet. It is fairly easy and even children are doing it today. One reason given for having smart guns is to prevent accidental deaths if a child gets hold of a gun. Television is a great teacher for people to learn how to overcome barriers built/made by adults.

One of the “promises” made by smart gun supporters is that such guns will not be usable by criminals if they are stolen. This is a definite **FALSE** narrative. All current technology that is applied to smart guns simply “locks” the gun to prevent firing. Like a lock on a door, once removed, entry is easy. Similarly once the “lock” on a smart gun is removed, the gun can be fired.

As mentioned above, biometrics relies on batteries to operate. This is problematic in several ways. First, if the gun is needed for self-defense and the battery is dead, so is the owner. Batteries, whether regular or rechargeable, have a specific life-span.

Second, there has been no discussion on what happens if the battery goes dead while the gun is being used. Does the gun remain unlocked, in which case others can use it, or will it automatically lock, rendering it useless?

Third, there has not been any discussion on whether law enforcement and others can render smart guns, especially those using RFID chips, inoperable using some radio frequency device. This can be disastrous for soldiers and law enforcement alike.

Conclusion

The integration of technology with firearms, combined with legal issues will probably make buying or owning smart guns untenable for most people.

In addition, there is a lot of controversy, from both sides, surrounding the technology that is or will be integrated into smart guns, and the legal issues that currently exist and will come about when they hit the commercial market.

Some people think that smart guns can bring more security and reduce cases of robberies with the use of stolen firearms and especially accidental shootings. On the other hand, others believe this is a way for the government to control and even prohibit the sale of firearms to people they don't approve of.

Regardless of belief, there is one clear and absolute mandate that is required for smart guns – they must work as safely and as reliably as current technology. And current technology is not that reliable or safe.

The current concept of smart guns primarily serves only one purpose, to use the weapon for home defense, especially where children live. One other possible venue for ownership is within jails and prisons. However these institutions generally have rules prohibiting firearm possession within the confinement areas.

Instead of concentrating on trying to integrate technology into firearms, gun manufacturers should probably be looking at two alternatives. The first alternative is to create non-lethal firearms for self-defense. There are already several approaches that are being used, but they need a lot of improvement.

The second alternative, where a firearm could be considered a smart gun, would be to develop an entirely new gun concept. We have seen two concepts of this alternative, dating back to the 1930's, in comics such as Buck Rogers. These early science fiction comics and movies introduced ray guns and laser guns. In later years, sonic, magnetic,

microwave, plasma, and light guns were introduced to the sci-fi community. These sci-fi guns are collectively called “directed energy weapons.”

Research and development groups are contracted by the military to develop these energy directed weapons. Such weapons, while having profiles similar to handheld firearms, have to be developed from the ground up. While in development, this would be an ideal time to incorporate the smart technology.

Regardless of whatever approach is used to make smart guns, there will always be the inherent danger of the guns to fail as they are designed. We should keep in mind that the iconic 1911 has several safety features and yet for its 100+ years of manufacturing and use, its mechanical safety features can still fail. Couple that with technology that can easily be hacked, and any smart gun is not truly safer.