



**House Bill 704
Firearms Tracking Technology**

UNFAVORABLE

Radio Frequency Identification or “RFID” chips are often employed for product control, inventory management and tracking. The bill’s use of the term “embedded tracker” term hints at the real purpose of HB 704. The chips can be active or passive in nature. Active chips require a battery and battery life is finite. Passive chips can be activated by the radio frequency generated by a scanning device. Some testing indicates that either type can be read from up to several hundred feet away. This makes them perfect for a “no hands stop and frisk” by law enforcement or anyone else with the proper technology. The military does not use such devices on equipment which may be employed in hostile environments because they can endanger our troops by revealing their locations and exposing them to hostile fire. They can also be used as a clandestine devices to monitor and surveil a person or object. (See attachments)

Except for the ability to be covertly tracked, the “embedded tracker” offers nothing which cannot be accomplished by simply using the serial numbers.

Firearms manufacturers ship their products in varying quantities to firearm distributors in multiple states, those distributors in turn ship firearms in varying quantities to other distributors or licensed firearm dealers in multiple states. In every case, these firearms are transported via common carriers such as FedEx and United Parcel Service.

Article – Public Safety

SUBTITLE 9. FIREARM TRACKING TECHNOLOGY.

§5-901

Page 1, lines 22-23

(B) “BULK FIREARM TRANSFER” MEANS THE SALE OR OTHER TRANSFER OF 10 OR MORE FIREARMS TOGETHER FROM ONE PARTY TO ANOTHER PARTY.

The language of §5-901 (B) is overly broad and the crucial term “transfer” is not defined, the inference is that every time the possession of a firearm changes, a “transfer” occurred. The original source of the firearms being “transferred” is not specified, which means a common carrier may be involved in a “bulk firearm transfer” of firearms from various manufacturers on multiple occasions in various states. Nothing in the bill language limits the scope of the bill to only those “bulk firearms transfers” which occur within Maryland.

§5-901

Page 2, lines 1-6

C) “EMBEDDED TRACKER” MEANS AN OBJECT THAT:

- (1) IS EMBEDDED IN THE FRAME OR RECEIVER OF A FIREARM;
- (2) EMITS UNIQUE TRACKING INFORMATION; AND
- (3) IS NOT READILY CAPABLE OF BEING REMOVED, DISABLED, OR DESTROYED WITHOUT RENDERING PERMANENTLY INOPERABLE OR DESTROYING THE FRAME OR RECEIVER.

The manufacturers do not custom build firearms to comply with the unique and sometimes capricious laws of each state. Nor do they know to which state each firearm will ultimately be shipped and sold, much less whether 10 or more firearms will be shipped together. At what point will the “embedded tracker” be required and who will install it? Aftermarket modifications to a firearm not only void the warranty but may in fact render the firearm unsafe.

How the various common carriers who transport these firearms can be required to transmit tracking information to the Maryland State Police as each firearm makes its way through the supply chain is not addressed by this bill.

Page 2, lines 9-12

(F) “UNIQUE TRACKING INFORMATION” MEANS A UNIQUE RADIO FREQUENCY IDENTIFICATION CODE THAT CAN BE ASCERTAINED AND RECORDED USING EQUIPMENT APPROVED BY THE SECRETARY UNDER § 5–903 OF THIS SUBTITLE.

With multiple manufacturers involved, providing unique codes for each manufacturer, firearm model, caliber, etc., will create a logistics nightmare. The bill requires serial number information on the chip which means either the manufacturer must build the chip info every firearm or someone must code the chip aftermarket. This means each chip must be individually verified against the serial number of each firearm. It also means anyone who adds the chip could easily modify the coding or intentionally mix up the chips so that nothing matches. How this enhances public safety is difficult to understand.

§5-902

Page 3, lines 17-20

(B) A SELLER OR OTHER TRANSFEROR WHO ENGAGES IN A BULK FIREARM TRANSFER SHALL TRANSMIT INFORMATION REQUIRED TO BE ENTERED IN THE DATABASE ESTABLISHED UNDER §5–903 OF THIS SUBTITLE IN A MANNER REQUIRED BY THE SECRETARY.

The unqualified language used will include the common carrier or carriers who transported the firearm because they were in possession of the firearm and thus became engaged in the overall process.

§5-902

Page 2, lines 21-23

(C) THERE IS A REBUTTABLE PRESUMPTION THAT A PERSON WHO SELLS OR OTHERWISE TRANSFERS 10 OR MORE FIREARMS TO ANOTHER WITHIN A 30-DAY PERIOD HAS ENGAGED IN A BULK FIREARM TRANSFER.

This section expands on the definition of a “bulk firearm transfer” under §5-901 (B) by placing a 10 firearm per month limit on transfers. Limiting a dealer to less than 10 firearm sales per month unless the firearms are equipped with the tracking device will have a chilling effect on legitimate businesses. It is doubtful that firearms with intrusive tracking devices will be well received by the citizens. The next result will be far fewer firearms dealers in Maryland which is probably a secondary reason for this bill being filed.

§5-903

Page 3, lines 1-5

(B) FOR EACH BULK FIREARM TRANSFER, THE DATABASE SHALL INCLUDE:
 (1) THE DATE, TIME, AND LOCATION OF THE BULK FIREARM TRANSFER;
 (2) THE NAME AND ADDRESS OF EACH PERSON WHO IS A PARTY TO THE BULK FIREARM TRANSFER;

The unqualified language used is similar to that used in §5-902 (B) and will include the common carrier or carriers who transported the firearm because they were in possession of the firearm and thus became engaged in the overall process.

Page 3, lines 16-25

(D) (1) THE SECRETARY SHALL ADOPT REGULATIONS TO CARRY OUT THIS SUBTITLE.
 (2) THE REGULATIONS ADOPTED BY THE SECRETARY SHALL:
 (I) SPECIFY THE MINIMUM REQUIREMENTS FOR AND CAPABILITIES OF EQUIPMENT THAT MAY BE USED FOR SCANNING AND RECORDING UNIQUE TRACKING INFORMATION; AND
 (II) ESTABLISH PROCEDURES AND REQUIREMENTS FOR SELLERS AND OTHER TRANSFERORS WHO ENGAGE IN BULK FIREARM TRANSFERS TO TRANSMIT INFORMATION REQUIRED TO BE INCLUDED IN THE DATABASE ESTABLISHED UNDER THIS SECTION.

From past experience, the time and funding required to establish a new database and custom hardware is daunting. There is no evidence that public safety would be improved by creating yet another bureaucratic system to track law-abiding gun owners and lawful sales of firearms.

The bill is silent on who will bear the initial acquisition cost and maintenance cost for the tracking and reporting equipment.

The logistics involved to issue requests for proposals from qualified vendors to create the necessary software, acquire, distribute, set-up and test the hardware make it highly unlikely that the requirements of this bill could be met by the effective date indicated. The net result will be little short of a virtual ban on firearm sales.

We strongly urge an unfavorable report on HB 704.

John H. Josselyn, Director
2A Maryland

Attachments (5)



The history of RFID: where did it come from?

We use RFID every day; sometimes without knowing, for example when accessing public transport, using our passports to board a flight or when making payments in-store.

RFID – Radio-Frequency Identification – uses electromagnetic fields to identify and track objects which carry either a passive or active tag. Unlike passive tags that require energy from nearby RFID readers to be detected, active tags have their own power source to broadcast their unique identification number and thanks to this, the tags can be detected by a reader over a longer distance.

Like barcodes, RFID tags can be used to quickly identify an object, however, unlike barcodes, several tags can be scanned at once and without the need for physical sight of the label, thus reducing time spent on stock management. RFID tags can also hold a lot more information than barcodes and create a more specific identification for items, tracking, monitoring and storing data. Thanks to their small size, RFID tags have been placed into day-to-day objects such as passports, library books, clothes and payment cards.

But where did this technology come from? And when was it created?

A recent article on the [BBC website](#) discusses the Cold War spy technology we all use today.

RFID – the technology on which Near Field Communication (NFC) is also based – is thought to have been created during WWII. One of the forerunners for this technology was the [revolutionary electrical musical instrument](#) developed by Leon Theremin. The instrument could be played without physical touch due to waves generated by the instrument being at a static frequency. The concept of this invention led to the creation of Theremin's Thing following the second World War.



In 1945, a group of boys from the Young Pioneer Organisation of the Soviet Union presented a hand-carved ceremonial seal of the USA to the US ambassador, Harriman. Within the seal was an antenna activated by radio waves that were directed at the US embassy by the

Soviets. This served as a microphone and broadcast private conversations back. The ambassador's security staff would have checked the seal, also known as 'The Thing', for electronic bugs and other spy equipment, however without batteries or wires, nothing was picked up and therefore the seal was placed in Harriman's study. This location was prime for listening into private conversations for the following seven years.

In the 1970s, RFID tags were used to monitor railway carriages. Today, RFID tags are used by many organisations such as the NHS and big retail chains across the world to track assets, manage stock or control quality processes. Due to the technological advancements these tags can be used to track almost anything, thanks to the simple idea created by Theremin decades before.

RFID was, however, officially invented in 1983 by Charles Walton when he filed the first patent with the word 'RFID'. NFC started making the headlines in 2002 and has since then continued to develop.

Slow adoption

However, the technology was not adopted that quickly, in retail in particular. RFID technology has been around for almost 20 years, but with the expense and lack of valuable data proving its benefits originally, many companies didn't see the value of investing. Other challenges that have inhibited the use of RFID for retailers include the integration of the technology into their current stock management systems and the change in culture that needs to occur to support it.

In recent years, however, retailers including Adidas, Decathlon, John Lewis, Tesco, River Island and M&S have introduced RFID into their organisations and have all made a [return on their investment](#), reporting an increase in sales of up to 5.5% and a decrease in stock holding of up to 13%.

What about NFC?

Near field communication (NFC) is a high frequency (13.56 MHz), wireless communication technology that enables two electronic devices to interact with each other when brought into close proximity – about 4cms, thus making NFC more adaptable than RFID and moreover, accessible to all through the use of smartphones. It is already widely used for contactless payment and access control, for example in public transport, but one of the new opportunities for this technology lies in “[smart packaging](#)” and “smart marketing”. NFC can be used to exchange digital content and also increase customer engagement. By placing an NFC tag within a product, customers can scan the tag to find out more about the item, enter competitions or easily reorder.



NFC is a unique, secure technology that provides an outstanding customer experience and is now open to both android and IOS, bringing endless opportunities to brands in terms of customer engagement and satisfaction.

What's next?

RFID is being adopted widely in the retail sector and also brings efficient solution to asset tracking challenges in the air transportation, industry or healthcare markets.

With the growth of multi-channel communication and increasingly demanding customers, the technology, and in particular the NFC, also brings opportunities in other areas such as secure authentication, smart changing rooms and connected packaging. The information marketers can gain from using RFID technology provides a better understand of customers' habits so marketing strategy can be tailored to fit requirements.

Radio Frequency Identification (RFID)

- Description
- Uses
- Information for Health Care Professionals
- FDA Actions
- Reporting Problems to FDA

Description

Radio Frequency Identification (RFID) refers to a wireless system comprised of two components: tags and readers. The reader is a device that has one or more antennas that emit radio waves and receive signals back from the RFID tag. Tags, which use radio waves to communicate their identity and other information to nearby readers, can be passive or active. Passive RFID tags are powered by the reader and do not have a battery. Active RFID tags are powered by batteries.

RFID tags can store a range of information from one serial number to several pages of data. Readers can be mobile so that they can be carried by hand, or they can be mounted on a post or overhead. Reader systems can also be built into the architecture of a cabinet, room, or building.

Uses

RFID systems use radio waves at several different frequencies to transfer data. In health care and hospital settings, RFID technologies include the following applications:

- Inventory control
- Equipment tracking
- Out-of-bed detection and fall detection
- Personnel tracking
- Ensuring that patients receive the correct medications and medical devices
- Preventing the distribution of counterfeit drugs and medical devices
- Monitoring patients
- Providing data for electronic medical records systems

The FDA is not aware of any adverse events associated with RFID. However, there is concern about the potential hazard of electromagnetic interference (EMI) to electronic medical devices from radio frequency transmitters like RFID. EMI is a degradation of the performance of equipment or systems (such as medical devices) caused by an electromagnetic disturbance.

Information for Health Care Professionals

Because this technology continues to evolve and is more widely used, it is important to keep in mind its potential for interference with pacemakers, implantable cardioverter defibrillators (ICDs), and other electronic medical devices.

Physicians should stay informed about the use of RFID systems. If a patient experiences a problem with a device, ask questions that will help determine if RFID might have been a factor, such as when and where the episode occurred, what the patient was doing at the time, and whether or not the problem resolved once the patient moved away from that environment. If you suspect that RFID was a factor, device interrogation might be helpful in correlating the episode to the exposure. Report any suspected medical device malfunctions to MedWatch, FDA's voluntary adverse event reporting system.

FDA Actions

The FDA has taken steps to study RFID and its potential effects on medical devices including:

- Working with manufacturers of potentially susceptible medical devices to test their products for any adverse effects from RFID and encouraging them to consider RFID interference when developing new devices.
- Working with the RFID industry to better understand, where RFID can be found, what power levels and frequencies are being used in different locations, and how to best mitigate potential EMI with pacemakers and ICDs.
- Participating in and reviewing the development of RFID standards to better understand RFID's potential to affect medical devices and to mitigate potential EMI.
- Working with the Association for Automatic Identification and Mobility (AIM) to develop a way to test medical devices for their vulnerability to EMI from RFID systems.
- Collaborating with other government agencies, such as the Federal Communications Commission (FCC), the National Institute for Occupational Safety and Health (NIOSH) and the Occupational Safety and Health Administration (OSHA) to better identify places where RFID readers are in use.

Reporting Problems to FDA

Prompt reporting of adverse events can help the FDA identify and better understand the risks associated with RFID. If you suspect a problem, we encourage you to file a voluntary report through [MedWatch: The FDA Safety Information and Adverse Event Reporting Program](#) ([/medwatch-fda-safety-information-and-adverse-event-reporting-program](#)).

Health care personnel employed by facilities that are subject to [Reporting Adverse Events \(Medical Devices\) requirements](#) ([/mandatory-reporting-requirements-manufacturers-importers-and-device-user-facilities](#)) should follow the reporting procedures established by their facilities.


Manufacturers, distributors, importers, and device user facilities (which include many health care facilities) must [notify the FDA](#) ([/radiation-emitting-products/getting-radiation-emitting-product-market-frequently-asked-questions/submitting-reports-and-requirements-maintaining-records-radiation](#)) immediately by [Reporting Adverse Events \(Medical Devices\)](#) ([/mandatory-reporting-requirements-manufacturers-importers-and-device-user-facilities](#)).

Resources

- [Medical Device RFID Susceptibility Program](#) (<http://www.metlabs.com/Industries/RFID/Medical-Device-RFID-Susceptibility-Program.aspx>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)
- [MET Labs Press Release: Program for Testing Medical Devices for Susceptibility to RFID Being Launched](#) (<http://www.prweb.com/releases/medical-device/rfid-susceptibility/prweb8900624.htm>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)
- [RFID Journal: MET Labs Announces Program to Test Medical Devices for Susceptibility to RFID Interference](#) (<http://www.rfidjournal.com/article/view/8904>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)

FDA Research

- [Biomedical Engineering OnLine: Adhoc electromagnetic compatibility testing of non-implantable medical devices and radio frequency identification \(2013\)](#) (<http://www.biomedical-engineering-online.com/content/12/1/71>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)
- [Biomedical Engineering OnLine: Electromagnetic compatibility of implantable neurostimulators to RFID emitters \(2011\)](#) (<http://www.biomedical-engineering-online.com/content/10/1/50>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)

- Heart Rhythm: In vitro tests reveal sample radiofrequency identification readers inducing clinically significant electromagnetic interference to implantable pacemakers and implantable cardioverter defibrillators (2010)
([http://www.heartrhythmjournal.com/article/S1547-5271\(09\)01146-1/abstract](http://www.heartrhythmjournal.com/article/S1547-5271(09)01146-1/abstract)) 
(<http://www.fda.gov/about-fda/website-policies/website-disclaimer>).



U.S. Department of Homeland Security

Archived Content

In an effort to keep DHS.gov current, the archive contains outdated information that may not reflect current policy or programs.

Radio Frequency Identification (RFID): What is it?

Radio Frequency Identification (RFID) technology uses radio waves to identify people or objects. There is a device that reads information contained in a wireless device or “tag” from a distance without making any physical contact or requiring a line of sight.

RFID technology has been commercially available in one form or another since the 1970s. It is now part of our daily lives and can be found in car keys, employee identification, medical history/billing, highway toll tags and security access cards.

The United States government uses two types of RFID technology for border management—vicinity and proximity:

- Vicinity RFID-enabled documents can be securely and accurately read by authorized readers from up to 20 to 30 feet away.
- Proximity RFID-enabled documents must be scanned in close proximity to an authorized reader and can only be read from a few inches away.

No personal information is stored on the RFID card – only a number, which points to the information housed in secure databases.

[Trusted traveler programs NEXUS, SENTRI, and FAST \(/trusted-traveler-programs\)](#) have used vicinity RFID technology to speed travelers through land border entries since 1995.

Topics

[BORDER SECURITY \(/TOPICS/BORDER-SECURITY\)](#)

Keywords

[TRUSTED TRAVELER \(/KEYWORDS/TRUSTED-TRAVELER\)](#)

Last Updated: 06/27/2022

HB 704 Attachment #2 2A Maryland

U.S. News World News



AP: Military units track guns using tech that could aid foes

By JAMES LAPORTA, JUSTIN PRITCHARD and KRISTIN M. HALL

September 30, 2021



Justin Pritchard

Justin Pritchard is an investigative editor and reporter. **Determined** to keep track of their guns, some U.S. military units have turned to a technology that could let enemies detect troops on the battlefield, The Associated Press has found.

The rollout on Army and Air Force bases continues even though the Department of Defense itself describes putting the technology in firearms as a “significant” security risk.

The Marines have rejected radio frequency identification technology in weapons for that very reason, and the Navy said this week that it was halting its own dalliance.

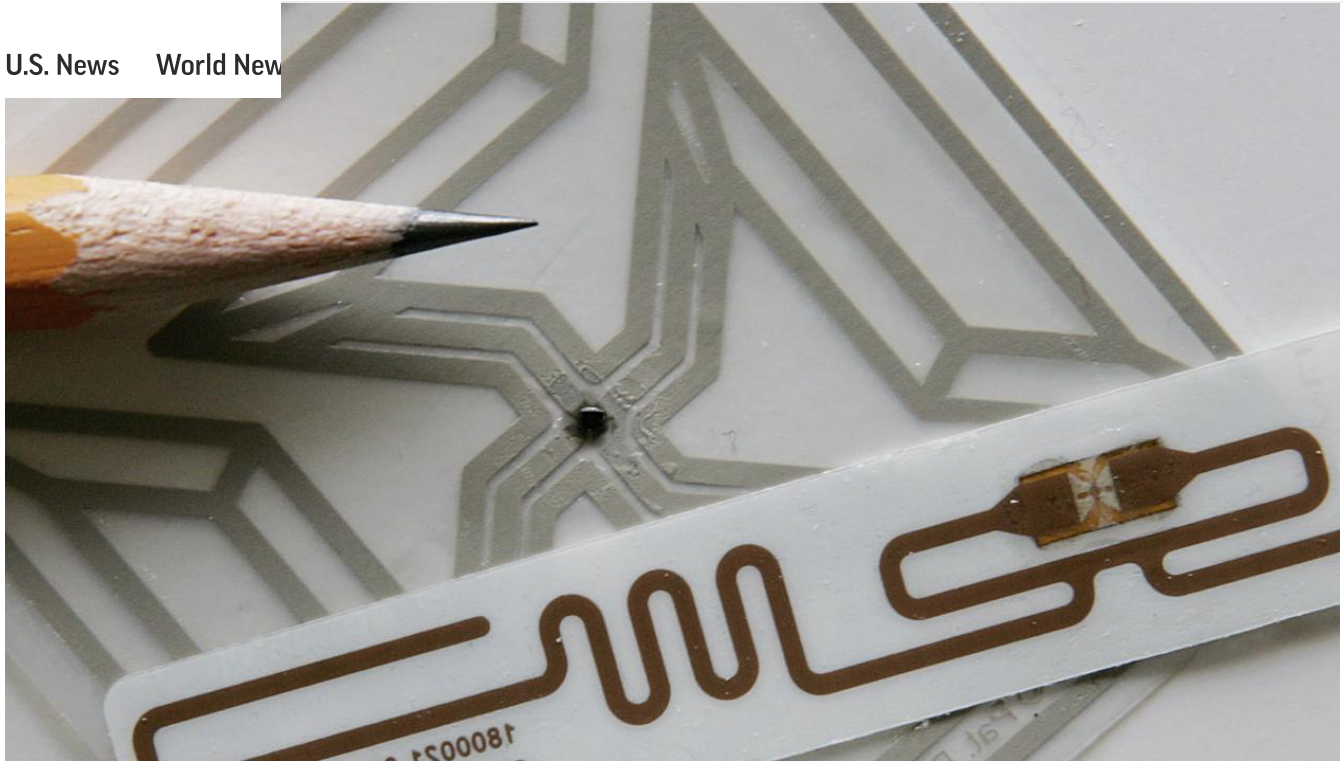
RFID, as the technology is known, is infused throughout daily civilian life. Thin RFID tags help drivers zip through toll booths, hospitals locate tools and supermarkets track their stock. Tags are in some identity documents, airline baggage tags and even amusement park wristbands.

When embedded in military guns, RFID tags can trim hours off time-intensive tasks, such as weapon counts and distribution. Outside the armory, however, the same silent, invisible signals that help automate inventory checks could become an unwanted tracking beacon.

The AP scrutinized how the U.S. armed services use technology to keep closer control of their firearms as part of an [investigation](#) into [stolen and missing](#) military guns — some of which have been used in [street violence](#). The examination included new field tests that demonstrated some of the security issues RFID presents.

HB 704 Attachment #3 2A Maryland

U.S. News World News



This Feb. 24, 2005, file photo shows radio frequency identification tags next to a pencil for scale in Cambridge, Mass. (AP Photo/Steven Senne)

The field tests showed how tags inside weapons can be quickly copied, giving would-be thieves in gun rooms and armories a new advantage.

And, more crucially, that even low-tech enemies could identify U.S. troops at distances far greater than advertised by contractors who install the systems.

Which is why a spokesman for the Department of Defense said its policymakers oppose embedding tags in firearms except in limited, very specific cases, such as guns that are used only at a firing range — not in combat or to guard bases.

“It would pose a significant operations security risk in the field, allowing an adversary to easily identify DOD personnel operating locations and potentially even their identity,” Pentagon spokesman Lt. Col. Uriah Orland told AP.

Spokespeople at the headquarters of the Air Force and Army said they did not know how many units have converted their armories.

AP found five Air Force bases that have operated at least one RFID armory, and one more that plans a retrofit. Executives at military contracting companies said many more units

U.S. News World News in “a few” arms rooms. Special forces soldiers can take tagged weapons aid Maj. Dan Lessard, a special forces spokesman. A separate pilot project at Fort Bragg, the sprawling Army base in North Carolina, was suspended due to COVID-19.

The Navy told AP one armory on a base up the coast from Los Angeles was using RFID for inventory. Then this week, after extended questioning, spokesman Lt. Lewis Aldridge abruptly said that the technology “didn’t meet operational requirements” and wouldn’t be used across the service.

Momentum for RFID built within the Air Force after a 2018 case in which a machine gun disappeared from the 91st Security Forces Group, which guards an installation that houses nuclear-tipped missiles. Authorities recovered the weapon, but the incident reverberated across the service.

With Air Force commanders looking to bolster armory security, defense contractors offered a familiar technology — one with a military pedigree.

The origins of RFID trace to World War II and the development of radar. In the U.S. military, use grew in the 1990s, after the first Gulf War showed a need to untangle vast supply chains of shipping containers.

The U.S. military is not alone in employing RFID for firearms management: Government armories in Nigeria, Saudi Arabia and elsewhere have been outfitted.

Armory conversions cost thousands of dollars, and sometimes more. Convenience is a big selling point. Instead of hand-recording firearm serial numbers on paper or scanning barcodes one-by-one like a cashier, an armorer can read tags in a rack of firearms with the wave of a handheld reader — and without having to see each weapon. The tags tucked inside don’t even need batteries.

Contractors that retrofit armories say tags can be read only within a limited range, typically a few dozen feet or less. But in field testing for AP, two prominent cybersecurity experts showed that a tag inside a rifle can be read from significantly farther, using inexpensive components that fit inside a backpack.

While the hackers who devised the experiments observed U.S. government restrictions on transmitting signals, enemies who would not be so constrained could detect tags miles

U.S. News World News The Corps has, according to a spokesman, decided across the service not to tag guns.

“The use of RFID tags on individual weapons systems increases the digital signature of Marines on a battlefield, increasing the security/force protection risks,” said Capt. Andrew Wood.

A top weapons expert from the Corps said he saw how tags can be read from afar during training exercises in the Southern California desert in December 2018.

“RFID tags on tanks, weapons, magazines, you can ping them and find the disposition of where units are,” said Wesley Turner, who was a Marine chief warrant officer 5 when he spoke in a spring interview. “If I can ping it, I can find it and I can shoot you.”

Full Coverage: AWOL Weapons

The Air Force and Army did not answer detailed questions about use of the technology in firearms. In written statements, spokespeople said unit commanders can add RFID systems as a further layer of accountability, but no service-wide requirement is planned.

Policy experts within the Office of the Secretary of Defense appeared unaware that the services have been tagging firearms with RFID.

Asked why service branches can field a technology that Pentagon planners consider so risky, Defense Department spokesman Orland first said that the services told the Pentagon they are not tagging guns due to security concerns.

Informed that AP found units which acknowledge using the technology, the Pentagon revised its statement and said it allows service branches to explore innovative solutions. The Defense Department “tries to balance pre-emptive prohibitions due to current security risks with flexibility to adopt new technologies when they mature and those risks decrease,” Orland said.

HACKERS ON THE HUNT

HB 704 Attachment #3 2A Maryland

U.S. News World New
till reading, still reading,” called out one, Kristin Paget, whose prowess has
at tech titans including Apple and Tesla — as well as the nickname
“Hacker Princess.”

Here in California’s San Joaquin Valley, in a sloping field surrounded by almond orchards, Paget and her hacking partner Marc Rogers were testing the limits of an RFID system they’d cobbled together for about \$500. To see how far they could detect a tag in the rifle, they were telling the man, firearms trainer Michael Palombo, to keep going.

By now more than half a football field away, the hackers had to shout or wave hands to communicate.

Because the hackers were following Federal Communications Commission regulations that limit the power of radio signals, their antenna lost the tag at 210 feet (64 meters).

That is nowhere near the farthest distance possible, according to Paget. She theorizes that a reader with enough of a power boost could detect an RFID tag on the outside of the International Space Station, 250 miles (402 kilometers) above.

What’s more, Paget said, it doesn’t take a Chinese or Russian cyber army to take advantage — a tinkerer with YouTube access could learn the needed skills.

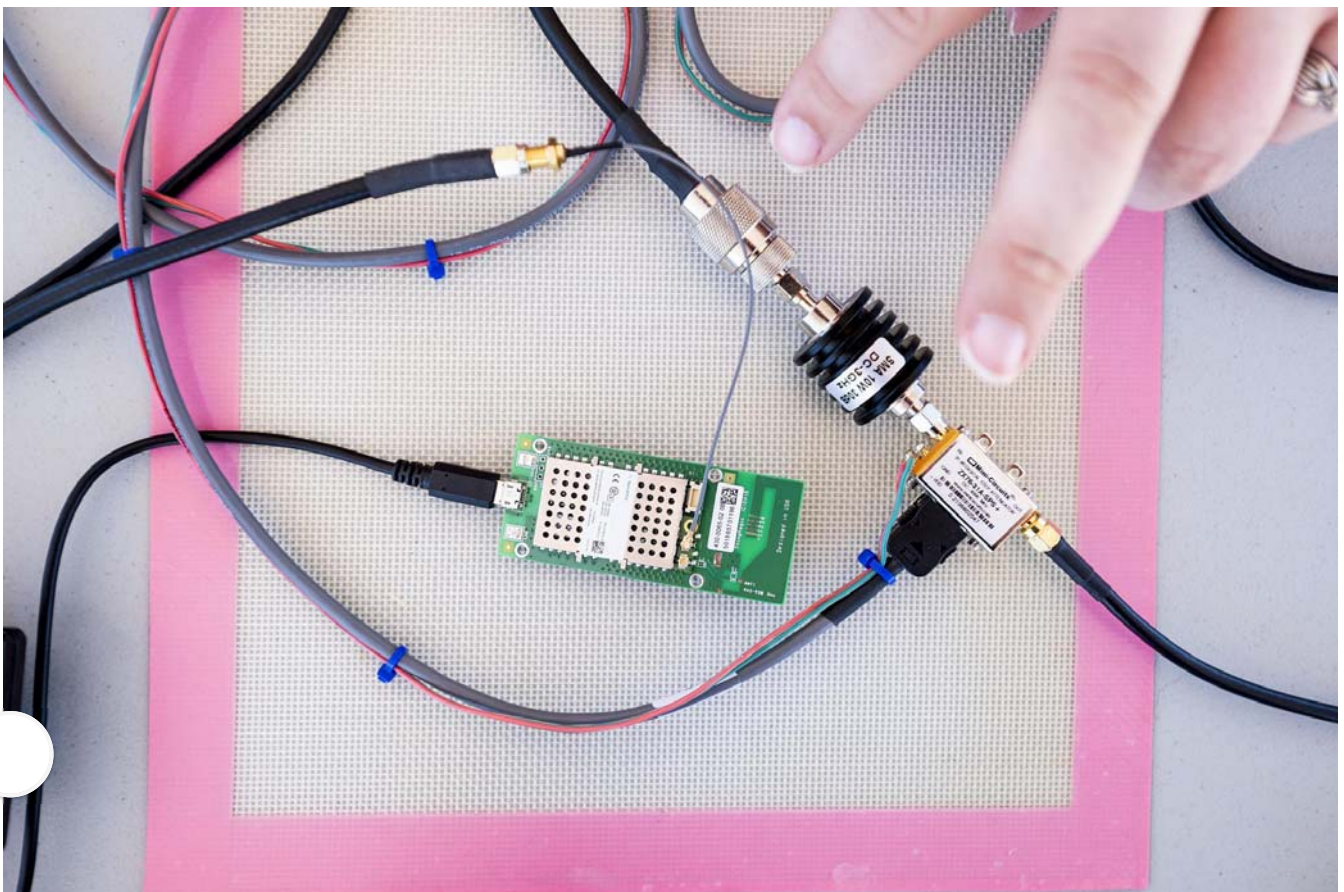
“It’s one of those situations that in the security world we say it keeps honest people honest, or it’s secure unless there’s an attack,” said Paget.



U.S. News World New



Hackers Kristin Paget, right, and Marc Rogers adjust an antenna while testing radio frequency identification signal range in Hickman, Calif., June 6, 2021. (AP Photo/Noah Berger)



HB 704 Attachment #3 2A Maryland

U.S. News World News
Publicly about the vulnerabilities of RFID in 2010, during presentation at
CON hacker convention. From a stage in Las Vegas, Paget broke down a
test that read a tag 217 feet (66 meters) away.

Dale “Woody” Wooden, who at the time was part of naval special warfare, saw that
presentation and warned fellow service members.

“If the disease is missing weapons and the cure is RFID tags, then you have a cure that is
worse than the disease,” said Wooden, who after 20 years in the Navy founded Weathered
Security, which teaches digital protection to the military and law enforcement. “They’re
prioritizing convenience over service member lives.”

In the California field tests, Paget and Rogers were prepared to demonstrate what they
see as other vulnerabilities created by putting RFID in firearms. They thought about
showing how a tag could trigger a roadside bomb, but settled on something more
mundane: inventory checks.

- Takeaways: AP's investigation of military gun tracking tech

One benefit of RFID is that it can reduce daily weapon count drudgery. Instead of
cataloging dozens of guns one-by-one, an armorer at the end of an aisle can read all their
tags at once.

Rogers demonstrated his doubts by showing how a thief could defeat the system.

Aiming his RFID reader at a rifle inside a hard carry case, Rogers replicated the rifle’s tag
with the lid still closed. Palombo then removed the firearm and Rogers put the cloned tag
inside. As a clone, that tag had all the same data as the rifle’s tag — and indeed, with the
case again closed, the RFID reader was fooled into thinking the original tag, and thus the
rifle, was still inside.



U.S. News World News



During a radio frequency identification signal range test, firearms instructor Michael Palombo holds a Springfield Armory M25 rifle with an RFID tag inside it about 210 feet (64 meters) from antennas, top, June 6, 2021, in Hickman, Calif. (AP Photo/Noah Berger)

It took Rogers less than two minutes.

“It’s the ultimate false sense of security,” said Rogers, who designed the hacks on the TV show “Mr. Robot” and is now vice president of cybersecurity at Okta. “It lists all the weapons and tells you that they’re there, but you’ve never actually seen the weapon.”

Executives at two companies that have installed RFID armories at Air Force bases agreed that a corrupt insider could trick the technology.

“RFID is not truly an anti-theft system,” said Cody Remington, president of Enasys.

The executives also said they had never heard anything like the 210 feet (64 meters) that the hackers achieved.

Remington suggested there might be ways to mitigate the risk, but said he deferred to the Pentagon. “Our expertise certainly isn’t on the battlefield,” he said, “our expertise is inside the buildings and tracking where items are.”

HB 704 Attachment #3 2A Maryland

U.S. News World New

Collins said RFID in weapons poses “absolutely no risk at all,” especially if the guns stay on base.

He said he didn’t believe a tag could be detected from more than 100 feet (30 meters), making the Pentagon’s security concerns invalid. “The leadership needs their staff to give them better guidance,” Collins said, “because that’s not good guidance.”

THE LURE OF RFID

RFID is a relatively expensive solutions for armory management, but the payoff is enticing.

Consider normal inventories. Between physical inspections and voluminous paperwork, counting all the guns on just one base can stretch to days or even weeks. Meanwhile, time seems to stop when a weapon is lost or stolen, as the installation shuts down and search parties launch to find it.

RFID offers a simpler, more efficient system. Which is why two airmen went to an Air Force [2020 Innovation Rodeo](#) — an ideas competition patterned after the TV show “Shark Tank” — to pitch a project to a panel of senior officers.



U.S. News World News



This 2020 image from video made available by the U.S. Marines shows weapons in an armory at the Yuma Marine Corps Air Station in Arizona. (Lance Cpl. Joseph Exner/U.S. Marines via AP)

The airmen offered another scenario, one service members dread and that RFID promises to eliminate: A thousand troops suddenly need to deploy overseas, fast. To get the weapons they will carry, each must wait in a line that snakes around the building and barely seems to move.

“We need to get on board with the 21st century,” Staff Sgt. Nicholas Mullins said from the stage.

Though the proposal didn’t win that competition, with the support of another federal program it found a home at an armory for security forces that patrol Eglin Air Force Base in Florida’s Panhandle.

Open with “full operational capability,” the RFID armory is a success as promised, according to spokeswoman Jasmine Porterfield. The new system cuts inventory time in half, limiting the need for two armorers and creating more schedule flexibility and training opportunities.

The maximum distance tags can be read, according to experts on the base: about 8 feet (2 meters).

HB 704 Attachment #3 2A Maryland

U.S. News

World News

from Nashville, Tennessee. Also contributing were Serginho Roosblad in
and Martha Mendoza in Santa Cruz, California.

Contact LaPorta at <https://twitter.com/jimlaporta>; contact Pritchard at
<https://twitter.com/JPritchardAP>; contact Hall at <https://twitter.com/kmhall>.

Email AP's Global Investigations Team at investigative@ap.org or
<https://www.ap.org/tips/>. See other work at <https://www.apnews.com/hub/ap-investigations>.

AP NEWS

Top Stories

Video

Contact Us

Accessibility Statement

[Cookie Settings](#)

DOWNLOAD AP NEWS

Connect with the definitive source for global and local news



MORE FROM AP

[ap.org](#)

[AP Insights](#)

[AP Definitive Source Blog](#)

[AP Images Spotlight](#)

[AP Explore](#)

[Books](#)

[AP Stylebook](#)

FOLLOW AP

HB 704 Attachment #3 2A Maryland



[Home](#) [Support](#) [Careers](#) [Terms & Conditions](#) [Privacy](#)

[U.S. News](#) [World News](#) © 2023 The Associated Press. All rights reserved.

HB 704 Attachment #3 2A Maryland





LARRY HOGAN
GOVERNOR

BOYD K. RUTHERFORD
LT. GOVERNOR

STATE OF MARYLAND
MARYLAND STATE POLICE
1201 REISTERSTOWN ROAD
PIKESVILLE, MARYLAND 21208-3899
410-486-3101
TOLL FREE: 1-800-525-5555
TDD: 410-486-0677



COLONEL
WOODROW W. JONES III
SUPERINTENDENT

June 15, 2022

The Honorable Larry Hogan
Governor
State House
100 State Circle
Annapolis, MD 21401

The Honorable Bill Ferguson
President of the Senate
The Senate of Maryland
H-107 State House
Annapolis, MD 21401

The Honorable Adrienne A. Jones
Speaker
Maryland House of Delegates
State House, H-101
Annapolis, MD 21401

RE: Personalized Handgun Technology
Report required by Public Safety Article 5-132(d) (MSAR #2033)

Pursuant to Public Safety Article 5-132(d), the Maryland Department of State Police submits to you the report of the Maryland Handgun Roster Board on the *Status of Personalized Handgun Technology*.

With the passage of the Responsible Gun Safety Act of 2000, the Board is committed to review and report its findings on the subject of personalized handguns. It remains committed in keeping the State of Maryland informed on this vital technology.

Sincerely,

Woodrow W. Jones III
Superintendent

cc: Ms. Sarah Albert, Maryland Department of Legislative Services Library (5 Copies)

2A Maryland - HB 704 - Attachment #4

**Maryland Handgun Roster Board
Twenty-First Annual Report on the
Status of Personalized Handgun Technology**

July 1, 2022

About the Report

The Maryland Handgun Roster Board is legislatively mandated to report annually on the status of personalized handgun technology. This requirement was part of the Responsible Gun Safety Act of 2000, and is now in the Public Safety Article, §5-132(d,) Annotated Code of Maryland. The following report from the Maryland Handgun Roster Board seeks to address and satisfy this requirement.

The report documents the findings of the review of Personalized Handgun Technologies as conducted by the Maryland Handgun Roster Board. The Board conducted the review through research and examination of publicly available resources including articles, reports, and documents that the Board was able to identify, and did not commission any independent analysis. The Board reviewed a set of references that was as comprehensive as possible given the Board's limited resources, but the references reviewed should not be considered an exhaustive list of all possible items related to personalized handgun technology.

Executive Summary

Review completed by the Board indicates there is currently no reliably available personalized handgun technology as of June 2022. The Handgun Roster Board continues to note that although the technology to produce personalized handguns does exist it is still not a commercially available and reliable 'handgun package'. However, in the past year two companies have made announcements that may indicate that firearms with personalized handgun technology may be available in the near future.

The National Institute of Justice continues to provide the most detailed analysis and reporting on personalized handgun technology and their report "Review of Gun Safety Technologies" published in June of 2013 is the most recent report of significance that stakeholders should reference on the topic. While some parties have exited the personalized handgun technology

arena and other parties have entered, the overall number of parties and effort working in this area does not appear to have changed significantly from recent years.

Section 1 – Personalized Handgun Technologies Available for Sale

As of June 2022, there is currently no personalized handgun technology that is commercially available for sale in Maryland or any other State. A few companies have expressed interest in bringing their technologies to market, and one company has even begun taking pre-sale orders, but to date no firearms with personalized handgun technology are available to consumers.

It has been observed that all the parties currently developing personalized handgun technology are smaller companies and that no major firearms manufacturer has publicly disclosed current or future plans to develop or bring to market personalized handgun technology. While major firearms manufacturers like Colt, Remington, and FN have previously indicated they were working on personalized handgun technology at this time it does not appear that any of them have continued such work. The reason(s) for this are not objectively known, but it does support the broader observation that personalized handgun technology is not likely to be widely commercially available in the near future.

In 2021, the Kansas based company SmartGunz, LLC announced that they would begin taking pre-sales of their 9mm 1911 style Sentry pistol¹. The Sentry pistol has SentryGunz’s patent pending lock-out technology which utilizes RFID worn by the user to achieve personalized handgun functionality. Currently the Sentry pistol is available for pre-sale at a cost of \$2,195.00 with expected delivery in Q3 of 2022². In December 2021, the company announced that they had made their first sale of the product to a law enforcement agency as part of the company’s evaluation program to gain feedback from law enforcement users³. The company has not disclosed the total number of pre-sales to civilians or law enforcement agencies, but this product appears to be the product closest to being commercially available.

In January of 2022, the Pennsylvania based company Lodestar Works Inc. announced the introduction of a 9mm pistol with personalized handgun technology called the LS9. This firearm

1. Holland, “SmartGunz, LLC Announces Ordering Availability of 9mm 1911 Sentry Pistol for \$1,995”, SmartGunz LLC, Jul 12, 2021, <https://smartgunz.co/2021/07/smartgunz-llc-announces-ordering-availability-of-9mm-sentry-pistol-for-1995/>
2. SmartGunz LLC, Civilian Products, June 1, 2022, <https://smartgunz.co/products/civilian/>
3. Holland, “ SmartGunz, LLC Announces First Sale of 9mm 1911 Sentry Pistol to Law Enforcement:”, SmartGunz LLC, Dec 17, 2021, <https://smartgunz.co/2021/12/smartgunz-llc-announces-first-sale-of-9mm-1911-sentry-pistol-to-law-enforcement/>

reportedly utilizes grip sensor, RFID, and Bluetooth technologies to implement personalized handgun functionality. The company is beta testing the product and hopes to have it commercially available in 2022, but it not yet currently available⁴.

The German company Armatix GmbH has expressed interest in selling their .22 caliber iP1 pistol model in 2014, and their 9mm iP9 in 2016, however to the best of the Board's knowledge the company never sold the product in the United States, and it is unclear if the company has any further plan to pursue sales of their product⁵.

In 2013, the Utah based company Kodiak Industries expressed interest in selling their .45 caliber *Intelligun* technology using fingerprint recognition⁶, however to the best of the Board's knowledge the company never sold the product and it appears the company does not have any further plan to pursue sales of their product as it appears the company is no longer in business.

In the late 1990's, iGun Technology Corporation of Florida developed a shotgun using an RFID ring that could be classified as personalized handgun technology, however to the best of the Board's knowledge the company never sold the product, and it is unclear if the company has any further plan to pursue sales of their product⁷.

Section 2 – Study, Analysis or Evaluation of Personalized Handgun Technologies

The National Institute of Justice (NIJ) is the research, development, and evaluation agency of the U.S. Department of Justice. NIJ has been tracking, studying, and assessing personalized handgun technology dating back to the 1990's. Over the years they have produced detailed reports relating to the various personalized handgun technologies and companies seeking to produce products with these technologies. They have also assessed the impacts, reliability demands, and challenges to adoption within law enforcement and the civilian populations. NIJ's reports are some of the best resources for stakeholder to reference with regards to personalized handgun technology. NIJ reports and documents relating to "Smart Guns" can be found here <https://nij.ojp.gov/taxonomy/term/21231>.

4. Daniel Trotta, "Smart guns finally arriving in U.S., seeking to shake up firearms market", Reuters, Jan 11, 2022, <https://www.reuters.com/technology/exclusive-smart-guns-finally-arriving-us-seeking-shake-up-firearms-market-2022-01-11/>
5. Alex Yablon, "With New Smart Gun, Industry Pioneer Bets Bigger Is Better", TheTrace, Mar 2, 2017, <https://www.thetrace.org/2017/03/new-armatix-smart-gun-law-enforcement/>
6. "Intelligun(R) Brings Innovation and the Next Level of Firearm Safety Technology to the World at the 2013 SHOT Show(R)", Yahoo Finance, Jan 15, 2013, <https://finance.yahoo.com/news/intelligun-r-brings-innovation-next-144500480.html>
7. iGun Technology, <https://www.iguntechnology.com/faq/index>

The most recent notable report from NIJ is from 2013 entitled “Review of Gun Safety Technologies”. This review outlines the products and technologies that were available at the time which include many of the products highlighted above in section 1 of this report. NIJ outlined and assessed various technologies under development but ultimately made similar conclusion to this Board in that there were no commercially available products with personalized handgun technology⁸. The report also provided a perspective on the risk and reliability of personalized handgun technology acknowledging that concerns regarding the reliability and potential performance of personalized handgun technologies will affect user acceptance and that personalized handgun technologies must not adversely affect the reliability of firearms⁹.

While the NIJ report from 2013 remains the most recent and comprehensive study the Board has reviewed, there are several other reports that while dated or less comprehensive, remain worthy of note for reference including:

- Smart Gun Technology Requirements Preliminary Report by Sandia National Laboratories in 1995. <https://www.osti.gov/servlets/purl/71695>
- Secure Weapon System Smart Gun Technology Phase I report by FN Manufacturing in 2001. <https://www.ojp.gov/pdffiles1/nij/grants/189247.pdf>
- Gun Safety Technology Challenge conducted by NIJ in 2015. <https://nij.ojp.gov/funding/gun-safety-technology-challenge#publication>

The Board has not been made aware of any other state, local, law enforcement or other agencies having conducted or publishing studies or evaluations of personalized handgun technology in the recent past. However, given the reported sale of the SmartGunz product to law enforcement for evaluation the Board will be monitoring to see what findings will be made available for future reports.

Section 3 – Additional Relevant Information

This report does not seek to be a comprehensive reporting of all industry development however, the Board has been made aware of various companies working on personalized handgun technology. For reference, a list of companies or groups reportedly working on developing personalized handgun technology can be found below:

-
8. Mark Green, Ph.D., *A Review of Gun Safety Technologies*, National Institute of Justice, June 2013, <https://www.ojp.gov/pdffiles1/nij/242500.pdf>
 9. Mark Green, Ph.D., “A Perspective on Risk, Reliability, and Person-Centric Technologies” in *A Review of Gun Safety Technologies*, Page 19, June 2013, <https://www.ojp.gov/pdffiles1/nij/242500.pdf>,

- SmartGunz LLC - <https://smartgunz.co/>
- LodeStar Works - <https://lodestarworks.com/>
- Armatix GmbH – website no longer active (<http://armatixus.com>)
- Kodiak Industries – website no longer active (<http://kodiakarms.com>)
- Biofire Technologies Inc - <https://biofire.io/>
- iGun Technology Corporation - <https://www.iguntechnology.com/>
- Machine Inc. - <https://machine.tech>
- New Jersey Institute of Technology - <https://www6.njit.edu/news/spotlight/2005/jan/index.php>
- Colt Manufacturing - <https://www.colt.com/>
- FN Herstal - <https://fnherstal.com/en/>

Membership of the Maryland Handgun Roster Board as of July 1, 2022

Colonel Woodrow W. Jones III, Chair	Superintendent, Dept. of State Police
Major Scott Keyser (designee)	Dept. of State Police
Mr. J. Charles Smith	Representative of the Maryland State's Attorney Association
Mr. P. Michael Errico	Citizen member
Mr. Russell Shea	Citizen Member
Ms. My Harrison	Citizen Member
Ms. Jennifer Gill	Mechanical/Electrical Engineer
Mr. Jonathan Maurath	Mechanical/Electrical Engineer
Mr. Carl Roy	Representative of handgun dealer, gunsmith or handgun manufacturer
Colonel (USA Retired) Ira Click	Representative of the National Rifle Association
Mr. Robert Bajefsky	Representative of an organization that advocates against handgun violence
Chief Michael Spaulding	Representative of Association of Chiefs of Police

Appendix

*Maryland Code Public Safety
Title 5 – Firearms
Subtitle 1 - Regulated Firearms
§ 5-132. Handgun safety devices*

(d) Report.

(1) The Handgun Roster Board annually shall:

- (i) review the status of personalized handgun technology; and*
- (ii) on or before July 1, report its findings to the Governor and, in accordance with § 2-1246 of the State Government Article, to the General Assembly.*

(2) In reviewing the status of personalized handgun technology under paragraph (1) of this subsection, the Handgun Roster Board shall consider:

- (i) the number and variety of models and calibers of personalized handguns that are available for sale;*
- (ii) each study, analysis, or other evaluation of personalized handguns conducted or commissioned by:*

- 1. the National Institute of Justice;*
 - 2. a federal, State, or local law enforcement laboratory; or*
 - 3. any other entity with an expertise in handgun technology; and*
- (iii) any other information that the Handgun Roster Board considers relevant.*