It sounds superinnovative, but security experts aren’t too hot on the idea. Just in time for the midterm elections this fall, the state will be the first in the U.S. to allow voters to submit their federal general election ballots via a smartphone app, and claims it’ll be secure enough by a blockchain (even from meddling). The program stems from a pilot project with overseas military members, and will be available to all those overseas registered in the state. But it’s still drawing criticism from election security experts who aren’t convinced the design will alleviate
cybersecurity concerns with online voting. **MIT Technology Review**

**It’s Hard but Possible to Hack an Amazon Echo**

Alexa may not be the only one listening in on your conversations. Hackers at the DefCon conference in Las Vegas found a way to hack into an Amazon Echo speaker and turn it into a spy bug. They used a modified Echo that has parts swapped out to hack into other Echos that haven’t been tampered with by connecting both Echos to the same local area network. So, the modified Echo became a personal listening bug, playing audio from the other Echos’ speakers. Plus, the hacked Echos had no idea it was happening. It wasn’t easy, but it shows there may be some exploits to Amazon’s speaker. **TechCrunch**

**NASA’s Going to the Sun**

Thanks to its Parker Solar Probe, which has finally left Earth and is making its way seven times closer to the sun than ever before. It’s been decades in the making, but the spacecraft is now safe enough to start flying closer to the sun, which means it’s off the ground and soon scientists will be able to start exploring its data, which will continue to be collected for the next seven years. It’s been stuck on Earth because it needed a bunch of speed to leave our orbit, so its initial launch will take it to Venus in six weeks. From there, the spacecraft will need to pull off a gravity assist to get closer to the sun and begin its first of 24 orbits around the big star. Its first close approach will be Nov. 1. **Space.com**

**Is Google Never Not Tracking You?**
Now there’s a double negative for you. And the answer is probably yes, even when you turn off tracking location abilities, according to an Associated Press report. The investigation found that Google services on Android and iPhones track and store your location even if you turned off location history, because the apps will continue to store your time-stamped location data. And then, Google uses this location information to target ads. So, what does turning off the location history do? According to AP, it removes your location from the Google Maps Timeline feature. You can turn off web and app activity tracking as a whole and delete your location data in Google account settings if that makes you feel better.  

CNet

DOD Has Another Bug Bounty in the Books

The Defense Department is on its sixth bug bounty program with HackerOne, with the announcement of Hack the Marine Corps this week. This program will focus on the Marine Corps’ public-facing sites and services to strengthen the Marine Corps Enterprise Network, and it’ll run until Aug. 26. DOD actually kicked off the bug bounty with a live-hacking event in Las Vegas on Aug. 12 during Black Hat and DefCon, where about 100 ethical hackers from the security researcher community worldwide hacked the Marine Corps’ sites and services for nine straight hours. They filed 75 unique valid security vulnerability reports and were awarded more than $80,000. BusinessWire