GOOGLE AND AMAZON ARE THE CIA

By Frank Konkel

More than 10 years ago, the Central Intelligence Agency made a groundbreaking $600 million deal with Amazon Web Services to make use of its cloud computing services — a radical departure from IT business as usual for the risk-averse intelligence agency.

To many intelligence officials at the time, the C2S contract — which procured commercial cloud services on behalf of all 18 intelligence agencies — was considered risky, allowing top secret classified data and information onto AWS hardware for tasks like computing, storage and sharing.

Speaking last week at AWS' re:Invent conference in Las Vegas, the tech chiefs for both the CIA and National Security Agency made clear in rare public remarks that those risks a decade prior have more than paid off.

"A lot of people may not realize, but had it not been for the partnership with AWS that CIA took over 10 years ago — really the risk was on AWS, with [then AWS CEO] Andy Jassy saying that they were going to work with the government and work to bring the best-in-breed technology to the national security space — we would not be here today," La'Naia Jones, chief information officer at CIA said. "And so it's just been a phenomenal relationship looking at how fast we've been able to progress…We would not be where we are without AWS stepping in and stepping up and willing to take that risk over a decade ago."

In the years since C2S, the intelligence community's partnership with AWS has only increased. In 2020, the CIA awarded its multibillion-dollar "C2E" cloud contract to AWS and four other vendors — Microsoft, Google, Oracle and IBM — to compete for specific IC task orders. For much of the past decade, however, AWS was the only commercial cloud provider that met the intelligence community's stringent requirements to host top secret classified data, giving it a leg up on competitors in the national security space. According to AWS Vice President of Worldwide Public Sector Dave Levy, the company's relationship with the CIA has made it a better cloud provider.

"For them and for us, this was uncharted territory," Levy told *Nextgov/FCW* at AWS re:Invent. "This was something new for the CIA and this was something new for [AWS] at the time. And when we take a look back over those 10 years, it's really benefited AWS in a sense that we've learned a lot about how

to do things that are really hard and solve difficult problems and become a better provider. It's been a very beneficial partnership."

In addition to being one of four companies to serve Defense Department cloud customers through the multibillion-dollar Joint Warfighting Cloud Capability contract, AWS also won the NSA's $10 billion cloud contract internally dubbed "WildandStormy." It's a core piece of the spy agency's once-secret plans to move its troves of data, including signals intelligence, to a commercial cloud provider. Little else is known about the contract, which the NSA publicly acknowledged for the first time last week.

"We are about three, maybe four years into a journey of moving our capabilities into the Amazon cloud," NSA CIO Scott Fear said, speaking alongside his CIA counterpart. "We are building on the work that La'Naia [Jones] described and have been with AWS for over 10 years now. We are in the process of bringing online new data centers for our work."

Both tech chiefs said the intelligence community is not only embracing cloud computing, but using the cloud as a means to enable both artificial intelligence and generative artificial intelligence tools.

"AI is now being looked at in every aspect and facet of, not just CIA, but really across the intel community," Jones said. "We're very fortunate and honored to play a key role to help lead that relationship and partnership with industry through C2E."

The CIA is "looking at generative AI, not just from the business or operations," Jones added, but also for the agency's open-source enterprise. She also suggested generative AI could be used to improve the digital acumen of code developers.

"We're looking at it for analysis, and it's being used actively," Jones added. "I don't know if everyone realizes that we're actually making use of the technologies, and so we just have to build upon that to even enhance it."

Fear said the NSA is looking to cloud and artificial intelligence tools like large language models "as a means to do our mission better." But beyond that, Fear said the NSA is hoping to use cloud to "lower the barrier of entry for all these new technologies," which had traditionally been difficult to get into the NSA's air-gapped and highly-secure architecture.

"It's really about how do you build partnerships and integration with the industrial base," he said. "How do you access billions of dollars' worth of investment in technology that's not just going to go buy something — that's an integration — and with a company at a level we haven't done before. It's a very exciting new way for us."

AWS' position as the first commercial cloud provider to host classified data has also made it a sought-after partner for both startups and established companies looking to expand their software offerings in the national security space. Palantir, AI firm Anthropic and software behemoth Salesforce are just a handful of important companies that have chosen to partner with AWS, in part because it can deploy software at scale in air-gapped settings.

"We're very proud and happy to announce that we are running on AWS' top-secret region, accredited, and it's truly amazing," Bill Pessin, senior vice president for Salesforce National Security, told *Nextgov/FCW* in Las Vegas.

Salesforce sought AWS' partnership years ago after running all its software in its own data centers and decided that, in order to grow its government business and "get to the markets that we wanted to be in, we realized we needed to go to public cloud," Pessin said. Soon after, he said the company recognized the opportunity "to piggyback in parallel, and not only go to public cloud for Salesforce at large, which we now call Hyperforce, but also to partner with the government and with AWS and then airgap Salesforce on AWS."

Pessin said Salesforce's decision to take a "cloud native approach" to air-gapping its software — partnering with a hyperscale cloud provider instead of a systems integrator to operate an on-premise version of their software — was the best decision for both the company and its customers.

"It was an inflection point for our company," Pessin said.

As tech companies and savvy users make it harder to infect phones remotely with government-grade spyware, repressive governments abroad are using a product widely marketed to American law enforcement agencies to gain physical access to devices and insert monitoring programs, researchers say.

Recent reports have revealed similar practices in Russia and China, and on Monday Amnesty International exposed a series of incidents in Serbia in which activists and journalists found their phones compromised after coming in contact with police, often without being arrested or charged.

In one case, reporter Slaviša Milanov was stopped near the southeastern Serbian town of Pirot by traffic police earlier this year and taken to a station ostensibly for drug and alcohol tests, which he passed. He was told to leave his belongings — including his phone — outside the room where he was questioned, and got them back 2½ hours later when he was released, according to Amnesty. Noting that

some settings had been changed, Milanov used a security app to determine that new programs had been installed.

Milanov told The Washington Post local authorities had objected to his articles on public money being spent on luxury cars and construction projects with well-connected contractors. “We have temporarily suspended critical content” because of the breach, he said.

Amnesty investigated and found three types of spyware installed on devices from Milanov and others in Serbia who grew suspicious when odd notifications were displayed.

It also found evidence that some of the phones had first been forcibly unlocked with tools from Cellebrite, a company based in Israel that sells to police departments and federal authorities in the United States and scores of other countries. In the United States, law enforcement officials with a warrant can use such tools to legally extract information from devices, including those used by major criminals.

Amnesty, one a handful of nonprofits leading the charge against spyware makers including NSO, the maker of the infamous Pegasus program, condemned the misuse of so-called forensic extraction tools, saying they “can become core enablers of a digital crackdown, likely to be mirrored in other countries and contexts, which may well be happening already.”

The United States has sanctioned multiple spyware makers in the past few years, declaring them threats to national security after they were used against some U.S. diplomats and others. The Amnesty report aims to document a different but related issue.

“While activists have long expressed concerns about spyware infections occurring during police interviews, Amnesty International believes that this report describes the first forensically documented spyware infections enabled by the use of Cellebrite mobile forensic technology,” the group said.

Cellebrite chief marketing officer David Gee told The Post it would be “shocking and disappointing” if the cases were accurately detailed by Amnesty. He said the company was investigating whether Serbia had violated the section of its license agreement that calls for lawful use, adding that it might use a software update to render its installation and data extraction tools inoperable there.

“The use case is a post-crime event,” typically following an arrest, Gee said. “We’re doing the investigation right now.” The company has withdrawn from other countries in the past, including China and Russia.

In a written statement, the company added that it complies with U.S. and United Nations sanction lists as well as Israel’s export control regulations. Beyond that, it said that since 2020, “Cellebrite has voluntarily ceased selling to customers in more than 60 countries.”

John Scott-Railton of Citizen Lab, which recently reported on Russian authorities injecting spyware into a user’s phone, said Amnesty’s report was “an important complement to the progress we have seen in recent years in accountability for spyware.”

“Companies that do this kind of forensic imaging have gotten a bit of a pass, in part because they have been associated with lawfully authorized surveillance,” he said. “But it is no longer possible for the companies that make this technology to act as if they are not aware of abuses.”

Amnesty said the phone-cracking occurred while targets were being questioned by local police or Serbia’s Security Information Agency, known by the acronym BIA. That agency did not respond to a request for comment from The Post.

Amnesty also uncovered evidence of previously unknown security flaws in an Android device driver for phones running on Qualcomm chips that allowed Cellebrite to access more of a device’s innards. Android maker Google confirmed the finding in a blog post Monday and said it notified Qualcomm more than three months ago. Not all of the flaws have been fixed, the company said.

“We are confident that this driver is under active exploitation by real-world attackers and that all the bugs resolved as part of this research had an outsized impact in preventing in-the-wild exploitation,” wrote Google’s Seth Jenkins.

To some extent, the shift toward physical access to devices is a result of Apple and Google making phones harder to hack from a distance. After researchers from Amnesty, Citizen Lab and elsewhere began finding hacked phones and dissecting how the attacks worked, they shared the information with Apple and Google, which found more cases and closed some of the holes used for spyware infections. That has made work harder for companies like Cellebrite as well, Gee said.

Recognizing that the authorities with physical access are not always on the side of justice, Apple has continued to harden its phones against that threat. The latest version of its iOS software reboots automatically if the phone has not been unlocked for a period of days, a time when it might be in an evidence locker or moving toward a police tech lab for analysis. That puts the phone into a more secure state, known in the industry as Before First Unlock.

“Our security teams around the world work tirelessly to track these sophisticated threats, and to constantly enhance our security features like Lockdown Mode which offers industry-leading protection,” Apple head of security engineering Ivan Krstic wrote in a statement.

Most local police in the United States would not have the combined physical opportunity, technical ability and legal authority to secure a warrant and install spyware on a suspect’s device, several technical law-enforcement officials said, speaking under the condition of anonymity to discuss operational capabilities. The FBI would have the ability but is unlikely to be applying it at scale, they said. The agency did not respond to a request for comment on the matter.

While using Cellebrite or similar software to break into a phone under a search warrant has not been unusual in the United States, a former FBI supervisor said he had never heard of spyware being installed. Listening to calls would be done under a separate court order and with the cooperation of telecommunications carriers, he said, speaking on the condition of anonymity to discuss sensitive practices.

Senior MPs have warned that revelations about an alleged Chinese spy with links to the highest levels of British public life, including the Duke of York, are the “tip of the iceberg” of Beijing’s meddling.
Tom Tugendhat, a former Tory security minister, said the Chinese Communist Party was “seeking to exert influence” in the UK and urged the Government to introduce a register of hostile state agents.
Sir Iain Duncan Smith, the former Conservative Party leader who has been sanctioned by Beijing, said China represented a “very clear threat”.
Last week, it emerged the Duke had formed a close business relationship with an alleged Chinese spy banned from the UK on national security grounds.
His office said on Friday that he had “ceased all contact with the individual after concerns were raised”, adding that he had “met the individual through official channels, with nothing of a sensitive nature ever discussed”.

On Friday, the Duke of York's office said he had 'ceased all contact with the individual after concerns were raised'

On Monday, the Duke was seen in public for the first time since he became embroiled in the scandal. He was photographed leaving Royal Lodge, his Windsor home, with a member of his protection team. It is thought he was going horse riding.
The alleged spy in question is currently the subject of a court anonymity order. and is referred to only as H6.
As well as his links to the Duke, the suspected agent also met David Cameron and Theresa May, the former prime ministers, on separate occasions.

Asked how concerned he was that an alleged spy had been able to get close to a member of the Royal family, Mr Tugendhat told BBC Breakfast: "Well, I have to say this is really indicative of exactly what the United Front Work Department, what the Chinese Communist Party, is trying to do.
"They are trying to exert influence, they are trying to change the policies of the United Kingdom and other countries around the world, and they are trying to influence individuals, not just in the royal family but in academia, in politics, in business and even sometimes in journalism."

Mr Tugendhat brought forward the foreign influence registration scheme when he was in office, which would compel anyone acting for a foreign power to declare political influencing activity and criminalise those who fail to do so.
The rollout of the scheme has been delayed since Labour took power, and it is currently unclear when it will be introduced. Mr Tugendhat urged the Government to implement it as soon as possible, warning that doing anything else "would frankly be negligent".

As well as his links to the Duke, the suspected agent also met Theresa May, the former prime minister

Asked how worried he was about the alleged spy meeting Lord Cameron and Baroness May, seemingly when the Tories were in power, he said: “I am sure it is happening now.

“I am absolutely certain that there are members of the United Front Work Department who are active right now in attempting to influence journalism, academics, politics and the whole lot.
“This is really the tip of the iceberg. The story, I can understand why it has been about Prince Andrew – but it is not really about Prince Andrew. It is about the way the Chinese Communist Party is seeking to exert influence here in the United Kingdom.”

Sir Iain told BBC Radio 4’s Today programme: “We’re dealing with the tip of the iceberg. The fact is there are many more like him [H6] in the UK.

“There are many more doing the job that he’s been doing, and the fact he was leaving the UK tells you that he realised at some point he was going to get caught.

“The reality is that there are many, many more involved in exactly this kind of espionage that’s taking place. The reality for us is very simple – China is a very clear threat.”