Amazon and the CIA: a match made in hell

# Part One: Amazon cashes in on war crimes and mass surveillance

**Evan Blake**
**13 July 2017**

*This is the first in a two part series, read part two* here.

In recent years, the multinational corporation Amazon has risen to become the preeminent online retail giant and the fourth most valuable company in the world. One of Amazon's most significant business contracts, which has largely been kept hidden from the public since it was finalized in October 2013, was a $600 million deal for Amazon Web Services (AWS) to build a private computing cloud for the 17 American intelligence agencies known collectively as the "intelligence community" (IC).

The deal initiated Amazon's ever-deepening integration with the American state, and implicates the company in the international war crimes, mass spying and repressive operations carried out by the spy agencies of American imperialism. Similar to the Krupp company, which supplied arms to the German military during World Wars I and II, Amazon today provides the technological scaffolding for the wars waged by American imperialism.

Since reaching its deal with the CIA, Amazon's stock value has more than tripled from $319.04/share to $993.80/share today. In the process, Amazon CEO Jeff Bezos has amassed roughly $55.9 billion, becoming the world's second-richest person with a current net value of $85.3 billion.

Through the contract, known as the Commercial Cloud Service or C2S cloud, the company forged links to all 17 IC agencies. The cloud securely stores large portions of the internet and telecommunications data accumulated by the Central Intelligence Agency (CIA); eight agencies of the Department of Defense, including the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO) and the intelligence wings of the Army, Navy, Air Force, and Marine Corps; the Office of Intelligence and Analysis and Coast Guard Intelligence of the Department of Homeland Security (DHS); and the Intelligence Branch of the Federal Bureau of Investigation (FBI), to name the most prominent agencies of the IC.

Amazon runs the C2S cloud privately, behind the IC's firewall, enabling the IC agencies to securely share data with each other, separate from the internet at large. The C2S cloud is a major component of the Intelligence Community Information Technology Enterprise (IC ITE) program initiated by then-Director of National Intelligence James Clapper in 2011. According to Clapper, the goal of the program is to "improve the ability to securely and efficiently discover, access, and share information" within the IC. Along with the Amazon-built cloud, the NSA constructed its own private cloud to store the swathes of data it continually collects. The two clouds work in complementary fashion, and are gradually replacing the isolated data centers used by each of the 17 IC agencies.

While the specific contents of the data shared between the IC agencies is classified and thus hidden from the public, it is undoubtedly used for all sorts of criminal operations. In a June 2015 speech, Clapper declared, "we have hundreds of millions of records in the cloud from the big six agencies [the CIA, NGA, FBI, NSA, NRO, and DIA] and others."

In April 2016, Beth Flanagan, a leading official at the NGA, revealed that data from IC ITE was used to accuse the Syrian government of carrying out the August 2013 chemical weapons attack in Ghouta. These allegations were exposed as a trumped-up lie by investigative reporter Seymour Hersh, whose arguments were substantiated by a separate investigation by the United Nations. Nevertheless, the Obama administration almost enacted full-scale war against Syria, using these false allegations as a pretext.

The sharing of data—facilitated by Amazon—enables scenarios to take place where the CIA, NSA, NGA and the Air Force collaborate to identify, precisely locate and carry out the drone assassination of anyone deemed to be a "terrorist," including American citizens. Thanks to Amazon, the spy agencies can now more seamlessly conspire to carry out bloody military campaigns, such as the military assault on Mosul, or secretly orchestrate the Saudi-led war against Yemen. They are no doubt using such technology to simulate and prepare for the long-planned wars against North Korea, Iran, China and Russia, which threaten to coalesce into a new, catastrophic World War between nuclear-armed powers.

**“One of the most important technology procurements in recent history”**

In mid-2012, the CIA began conducting negotiations with AWS, IBM and an unnamed third corporation to decide which company would win the 10-year, highly lucrative contract to create the private cloud for the IC, which had to be capable of analyzing 100 terabytes of raw data at a time, an immense figure.

In February 2013, the CIA secretly selected Amazon as the winning bidder. IBM filed a bid protest, claiming they had offered a lower price than Amazon, but in October 2013, the US Court of Federal Claims sided with Amazon, which then began to build the C2S cloud infrastructure. The cloud became operational in the summer of 2014, with then-CIA chief information officer Doug Wolfe praising it as “one of the most important technology procurements in recent history.”

Last month, current CIA CIO John Edwards declared in a speech at AWS’ Public Sector Summit, “It’s the best decision we’ve ever made... It’s the most innovative thing we’ve ever done... It is having a material impact on both the CIA and the IC.”

There were a number of factors that led the CIA to partner with Amazon, one of which was their ability to save money in the long-term. While $600 million is an enormous sum, at that point the IC was spending upwards of $8 billion annually to store and analyze the billions of pieces of metadata, phone and internet records, and other information that it was collecting en masse on its self-built servers, as noted in documents leaked by Edward Snowden.

Amazon’s cloud-based server offered a means to significantly reduce these costs, as it had a unique ability to scale up or down to meet the storage, computing and analytics needs of the IC at a given time. Amazon would also incorporate any innovations or improvements devised by their engineers, which happen on an almost daily basis, directly into the C2S cloud.

Another advantage that AWS had over IBM and the third bidder was its commercial cloud marketplace, which is a place for vendors to sell software infrastructure and other online products to customers. Amazon’s commercial cloud marketplace was established in mid-2012 and rapidly grew over the following year during its bidding with the CIA.

The marketplace allows customers to test software products and developer tools before committing to a purchase. This appealed to the IC, which was tired of having spent large sums of money on inferior products. After signing the C2S cloud contract, the IC gave Amazon the green light to build a classified cloud marketplace solely for the IC, which went live in April 2016.

A third, highly significant reason that the IC transitioned to cloud-based computing and selected Amazon as their contractor stemmed from the increased need for internal security after recurring leaks made by whistleblowers, especially the cables obtained by Chelsea Manning and published by Wikileaks.

Throughout 2010, Wikileaks released the Afghan War Logs and Iraq War Logs, exposing the war crimes committed against those countries’ populations, as well as a dossier of US State Department diplomatic cables provided by Manning that exposed the US government’s foreign intrigues dating back to the 1960s, known as Cablegate. Clapper’s launching of the IC ITE initiative came the following year, in direct response to the evident weakness of the IC’s security systems.

Explaining how she walked away with immense amounts of government data, Manning wrote that she encountered “Weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis... a perfect storm.”

Centralizing data storage onto the private IC ITE clouds—using the advanced encryption methods developed by AWS and the NSA—enables the IC to prevent massive leaks from within. One of the security measures provided by the clouds is the ability to meta-tag all data with information, including where it came from and who is authorized to see it. Analysts are now only able to access data if they have the authorization. Further, if an analyst attempts to download large amounts of data, as done by Manning and Snowden, the cloud automatically flags this activity, halting it and notifying security personnel. Officials have claimed that if the current IC ITE measures had been in place in 2010 and 2013, Manning and Snowden would not have been able to walk away with troves of data.

*To be continued*