Intro

Computers are very complex machines with a very long history, but the first actually-functional devices weren't built until WW2, and used for the purpose of cryptography. The most famous of these was the Enigma machine used by the Nazis to encrypt communications.

Crypto AG

So, the Washington Post isn't all bad:
https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/
Actually it's pretty surprising that they published this considering it's owned by Bezos who we will get into later, has a lucrative contract with the CIA.

Crypto AG was formed during WW2 to create encryption devices for the allies:

> The company, Crypto AG, got its first break with a contract to build code-making machines for U.S. troops during World War II. Flush with cash, it became a dominant maker of encryption devices for decades, navigating waves of technology from mechanical gears to electronic circuits and, finally, silicon chips and software.

Crypto AG would go on to sell encryption devices to dozens of states, including Iran, Libya, and others.

West German intelligence (BND) and the CIA partnered in the postwar era to secretly insert backdoors for themselves in these encryption devices.

> They monitored Iran's mullahs during the 1979 hostage crisis, fed intelligence about Argentina's military to Britain during the Falklands War, tracked the assassination campaigns of South American dictators and caught Libyan officials congratulating themselves on the 1986 bombing of a Berlin disco.

Some states were tipped off because the government is dumb as shit:

> There were also security breaches that put Crypto under clouds of suspicion. Documents released in the 1970s showed extensive — and incriminating — correspondence between an NSA pioneer and Crypto's founder. Foreign targets were tipped off by the careless statements of public officials including President Ronald Reagan. And the 1992 arrest of a Crypto salesman in Iran, who did not realize he was selling rigged equipment, triggered a devastating "storm of publicity," according to the CIA history.

This was a profoundly successful program:

> At times, including in the 1980s, Crypto accounted for roughly 40 percent of the diplomatic cables and other transmissions by foreign governments that cryptanalysts at the NSA decoded and mined for intelligence, according to the documents.
>
> All the while, Crypto generated millions of dollars in profits that the CIA and BND split and plowed into other operations.

In 2018 Crypto AG was liquidated and sold to two companies:

> Two companies purchased most of Crypto's assets. The first, CyOne Security, was created as part of a management buyout and now sells security systems exclusively to the Swiss government. The other, Crypto International, took over the former company's brand and international business.
>
> Each insisted that it has no ongoing connection to any intelligence service, but only one claimed to be unaware of CIA ownership. Their statements were in response to questions from The Post, ZDF and Swiss broadcaster SRF, which also had access to the documents.
>
> CyOne has more substantial links to the now-dissolved Crypto, including that the new company's chief executive held the same position at Crypto for nearly two decades of CIA ownership.

The authors ask if the CIA was in the position to prevent numerous assassination plots and ethnic cleansing campaigns. The article hilariously notes the lack of discussion of ethics in the disclosed documents:

> **The papers largely avoid more unsettling questions, including what the United States knew — and what it did or didn't do — about countries that used Crypto machines while engaged in assassination plots, ethnic cleansing campaigns and human rights abuses**.
>
> The revelations in the documents may provide reason to revisit whether the United States was in position to intervene in, or at least expose, international atrocities, and whether it opted against doing so at times to preserve its access to valuable streams of intelligence.
>
> **Nor do the files deal with obvious ethical issues at the core of the operation: the deception and exploitation of adversaries, allies and hundreds of unwitting Crypto**

> **employees**. Many traveled the world selling or servicing rigged systems with no clue that they were doing so at risk to their own safety.

Hahahahaha:

> At one point, the NSA intercepted Libyan communications indicating that the president's brother, Billy Carter, was advancing Libya's interests in Washington and was on leader Moammar Gaddafi's payroll.

It just sounds like everyone involved is really dumb:

> The engineers and designers responsible for developing prototype models often questioned the algorithms being foisted on them by a mysterious external entity.
>
> Crypto executives often led employees to believe that the designs were being provided as part of the consulting arrangement with Siemens. But even if that were so, why were encryption flaws so easy to spot, and why were Crypto's engineers so routinely blocked from fixing them?

In-Q-Tel

In-Q-Tel was started in 1999 by Norman Augustine, a war profiteer from Lockheed Martin, and Gillman Louie, a game designer who privatized Tetris and created the Falcon series of flight simulators. The stated purpose of the company is to make investments in IT to keep the CIA flush with the latest tech.

Investments

The most well-known company In-Q-Tel has investments in is a little mom & pop shop called Google. Early in the 2000s, they bought a simulation of the globe from a game company called Intrinsic Graphics. The product was called Keyhole and it later became a quaint gewgaw called Google Earth. Up until 2005, IQT had $2.2M in Google shares.

It seems Google's origins may have other connections to intelligence agencies: https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance/

IQT's portfolio has grown substantially since then: https://www.iqt.org/portfolio/
There's 7 pages of 40 companies each, so close to 300 companies just out of the ones that are actually disclosed.

Some highlights:
Echodyne: Absolutely evil-sounding company. They make radar-based ground sensors for autonomous vehicles. “Echodyne is a privately held company backed by Bill Gates, NEA, Madrona Venture Group, Vulcan Capital, and Lux Capital among others.”

Expect Labs: Created an API to enable any app to be voice-enabled. Hmm I wonder why the CIA might be interested in an app that interprets speech.

Synapse Technology Corporation: Automates analysis of x-ray scanners like the ones used at airports. Automatically laughs at how small your pecker and beans are.

Tamr: A “data unification company” that touts its use by Toyota, GE, Thompson Reuters, and GlaxoSmithKline. It basically sounds like they take all of the disparate types of data that corporations have been collecting on us for the past 20 years and integrates them to find new ways to label you a terrorist or sell you boner pills or whatever.
Hey what you know! Case study of Tamr using data unification to label people terrorists:
https://jdp491bprdv1ar3uk2puw37i-wpengine.netdna-ssl.com/wp-content/uploads/2017/07/Tamr_DHS_Case_Study.pdf
And here’s the boner pill one!
https://www.forbes.com/sites/tomdavenport/2018/01/08/biting-the-data-management-bullet-at-glaxosmithkline/#73b341dd5577

Gitlab: A git-based software repository service. If you thought Github was bad because it’s owned by Microsoft, wait till you hear who’s got equity in Gitlab!

Amazon, Oracle, Microsoft, IBM

Amazon currently has a $600M contract with the CIA to provide it with cloud computing services (most people probably know what the cloud is by now but just in case you don’t, it’s basically just a corporation running massive farms of computers on behalf of other people). The CIA has a new program that it’s creating called Commercial Cloud Enterprise (C2E) which will award tens of billions of dollars to companies for running huge server farms that they can use to read all your Signal messages.

This is about a similar DoD program but I wanted to read it anyway because I really really hate it:

> If the CIA follows through on its intention to use multiple companies, it may avoid the industry criticism that has plagued the Defense Department’s plans to award its $10-billion Joint Enterprise Defense Infrastructure contract, or JEDI, to a sole company.

These little turds literally think they’re the scrappy rebels fighting the evil empire. Amazing.

https://www.latimes.com/business/technology/la-fi-cia-amazon-cloud-computing-20190403-story.html

General Atomics

General Atomics is a nuclear power company based out of San Diego, CA. It has been passed through a lot hands since its inception in 1955, such as: Gulf Oil, Royal Dutch Shell (oil company), and Chevron (oil company). In 1986 it was bought by Neal & Linden Blue for $60M using god knows what fucking money.

Holy shit:

> The Blues' inevitable ascent within the aviation industry dovetailed with a developing hatred for communism. Eventually the brothers set up shop in Nicaragua, running a cocoa and banana plantation with the family of former President Anastasio Somoza, the notorious dictator who was overthrown by the Sandinista Liberation Front, the socialist party that prompted the Reagan administration to illegally funnel weapons to the Contras.
>
> So it was an urge to help their friends fend off freedom fighters in Central America that had the Blues first warming up to drones. "You could launch them from behind the line of sight," said Niel, figuring that light aircraft could be used to destroy Sandinistan oil pipelines. "You would have total deniability."

Later in the article they say that drones had a "public relations problem". Who fucking solved that fucking problem? Obama. Thanks asshole.
https://www.vice.com/en_us/article/dp4xvw/how-general-atomics-won-the-west

Civilian Encryption

Signal is an app that a lot of you probably use now developed by Moxie Marlinspike, a weirdly-named sort-of-anarchist programmer that has been making privacy tech for at least a decade now.
https://www.wired.com/story/signal-encrypted-messaging-features-mainstream/

They are slowly making their way through the other parts of your phone that Google and the CIA can spy on, such as your contacts:
https://www.wired.com/story/signal-contact-lists-private-secure-enclave/
Donate to the Signal Foundation: https://signal.org/donate/