Google Earth: how the tech giant is helping the state spy on us

▲ Composite: Alamy/Guardian Design

We knew that being connected had a price – our data. But we didn't care. Then it turned out that Google's main clients included the military and intelligence agencies. By Yasha Levine

The internet surrounds us. It mediates modern life, like a giant, unseen blob that engulfs the modern world. There is no escape, and, as Larry Page and Sergey Brin so astutely understood when they launched Google in 1998, everything that people do online leaves a trail of data. If saved and used correctly, these traces make up a goldmine of information full of insights into people on a personal level as well as a valuable read on larger cultural, economic and political trends.

Lose yourself in a great story: Sign up for the long read email

Read more

Google was the first internet company to fully leverage this insight and build a business on the data that people leave behind. But it wasn't alone for long. It happened just about everywhere, from the smallest app to the most sprawling platform.

Uber, Amazon, Facebook, eBay, Tinder, Apple, Lyft, Foursquare, Airbnb, Spotify, Instagram, Twitter, Angry Birds – if you zoom out and look at the bigger picture, you can see that, taken together, these companies have turned our computers and phones into bugs that are plugged in to a vast corporate-owned surveillance net-work. Where we go, what we do, what we talk about, who we talk to, and who we see – everything is recorded and, at some point, leveraged for value. Google, Apple and Facebook know when a woman visits an abortion clinic, even if she tells no one else: the GPS coordinates on the phone don't lie. One-night stands and extramarital affairs are a cinch to figure out: two smartphones that never met before suddenly cross paths in a bar and then make their way to an apartment across town, stay together overnight, and part in the morning.

They know us intimately, even the things that we hide from those closest to us. In our modern internet ecosystem, this kind of private surveillance is the norm. It is as unnoticed and unremarkable as the air we breathe. But even in this advanced,

data-hungry environment, in terms of sheer scope and ubiquity, Google reigns supreme.

As the internet expanded, Google grew along with it. No matter what service it deployed or what market it entered, surveillance and prediction were cooked into the business. The amount of data flowing through Google's systems is staggering. By the end of 2016, Google's Android was installed on 82% of all new smartphones sold around the world, and by mid-2017 there were more than 2 billion Android users globally.

Google also handles billions of searches and YouTube plays daily, and has a billion active Gmail users, meaning it had access to most of the world's emails. Some analysts estimate that 25% of all internet traffic in North America goes through Google's servers. The company isn't just connected to the internet, it *is* the internet.

Google has pioneered a whole new type of business transaction. Instead of paying for its services with money, people pay with their data. And the services it offers to consumers are just the lures, used to grab people's data and dominate their attention – attention that is contracted out to advertisers. Google has used data to grow its empire. By early 2018, Google's parent company, Alphabet, had85,050 employees, working out of more than 70 offices in 50 countries. The company had a market capitalisation of $727bn at the end of 2017, making it the second most valuable public company in the world, beaten only by Apple, another Silicon Valley giant. Its profits for the first quarter of 2018 were $9.4bn.

▲ Google co-founders Larry Page, left, and Sergey Brin in 2004. Photograph: Ben Margot/AP

Meanwhile, other internet companies depend on Google for survival. Snapchat, Twitter, Facebook, Lyft and Uber have all built multi-billion-dollar businesses on top of Google's ubiquitous mobile operating system. As the gatekeeper, Google benefits from their success as well. The more people who use their mobile devices, the more data it gets on them.

What does Google know? What can it guess? Well, it seems just about everything. "One of the things that eventually happens … is that we don't need you to type at all," Eric Schmidt, Google's former CEO, said in a moment of candour in 2010. "Because we know where you are. We know where you've been. We can more or less guess what you're thinking about." He later added: "One day we had a conversation where we figured we could just try to predict the stock market. And then we decided it was illegal. So we stopped doing that."

It is a scary thought, considering that Google is no longer a cute startup but a powerful global corporation with its own political agenda and a mission to maximise profits for shareholders. Imagine if Philip Morris, Goldman Sachs or a military contractor like Lockheed Martin had this kind of access.

Not long after Brin and Page incorporated Google, they began to see their mission in bigger terms. They weren't just building a search engine or a targeted advertising business. They were organising the world's information to make it accessible and useful for everyone. It was a vision that also encompassed the Pentagon.

Even as Google grew to dominate the consumer internet, a second side of the company emerged, one that rarely got much notice: Google the government contractor. As it turns out, the same platforms and services that Google deploys to monitor people's lives and grab their data could be put to use running huge swaths of the US government, including the military, spy agencies, police departments and schools. The key to this transformation was a small startup now known as Google Earth.

In 2003, a San Francisco company called Keyhole Incorporated was on the ropes. With a name recalling the CIA's secret 1960s "Keyhole" spy satellite programme, the company had been launched two years earlier as a spinoff from a videogame outfit. Its CEO, John Hanke, told journalists that the inspiration for his company came from Neal Stephenson's Snow Crash, a cult science-fiction novel in which the hero taps into a programme created by the "Central Intelligence Corporation" called Planet Earth, a virtual reality construct designed, as the book describes,

to “keep track of every bit of spatial information that it owns – all the maps, weather data, architectural plans, and satellite surveillance stuff”.

Keyhole had its roots in videogame technology, but deployed it in the real world, creating a programme that stitched satellite images and aerial photographs into seamless 3D computer models of the Earth that could be explored as if they were in a virtual reality game world. It was a groundbreaking product that allowed anyone with an internet connection to virtually fly over anywhere in the world. The only problem was Keyhole’s timing: it was a bit off. It launched just as the dotcom bubble blew up in Silicon Valley’s face. Funding dried up, and Keyhole found itself struggling to survive. Luckily, the company was saved just in time by the very entity that inspired it: the CIA.

Google at 20: how two 'obnoxious' students changed the internet

Read more

In 1999, at the peak of the dot-com boom, the CIA had launched In-Q-Tel, a Silicon Valley venture capital fund whose mission was to invest in start-ups that aligned with the agency's intelligence needs. Keyhole seemed a perfect fit.

The CIA poured an unknown amount of money into Keyhole. The investment was finalised in early 2003, and it was made in partnership with the National Geospatial-Intelligence Agency, a major intelligence organisation with 14,500 employees and a $5bn budget, whose job was to deliver satellite-based intelligence to the CIA and the Pentagon. Known as the NGA, the spy agency's motto was: "Know the Earth … Show the Way … Understand the World."

The CIA and NGA were not just investors; they were also clients, and they involved themselves in customising Keyhole's virtual map product to meet their own needs. Months after In-Q-Tel's investment, Keyhole software was already integrated into operational service and deployed to support US troops during Operation Iraqi Freedom, the shock-and-awe campaign to overthrow Saddam Hussein. Intelligence officials were impressed with the "videogame-like" simplicity of its virtual maps. They also appreciated the ability to layer visual information over other intelligence. The possibilities were limited only by what contextual data could be fed and grafted on to a map: troop

movements, weapons caches, real-time weather and ocean conditions, intercepted emails and phone call intel, and mobile phone locations.

Keyhole gave intelligence analysts, field commanders, air force pilots and others the kind of capabilities we take for granted today when we use digital mapping services on our computers and smartphones to look up restaurants, cafes, museums, traffic or subway routes.

Military commanders weren't the only ones who liked Keyhole. So did Sergey Brin. He liked it so much that he insisted on personally demoing the app for Google executives. According to an account published in Wired, he barged in on a company meeting, punched in the address of every person present, and used the programme to virtually fly over their homes.

In 2004, the same year Google went public, Brin and Page bought the company outright, CIA investors and all. They then absorbed the company into Google's growing internet applications platform. Keyhole was reborn as Google Earth.

The purchase of Keyhole was a milestone for Google, marking the moment the company stopped being a purely consumer-facing internet company and began integrating with the US government. When Google bought Keyhole, it also acquired an In-Q-Tel executive named Rob Painter, who came with deep connections to the world of intelligence and military contracting, including US Special Operations, the CIA and major defence firms, among them Raytheon, Northrop Grumman and Lockheed Martin. At Google, Painter was planted in a new dedicated sales and lobbying division called Google Federal, located in Reston,

Virginia, a short drive from the CIA's headquarters in Langley. His job was to help Google grab a slice of the lucrative military-intelligence contracting market. Or, as Painter described in contractor-bureaucratese, "evangelising and implementing Google Enterprise solutions for a host of users across the intelligence and defence communities".

Google had closed a few previous deals with intelligence agencies. In 2003, it scored a $2.1m (£1.7m) contract to outfit the National Security Agency (NSA) with a customised search solution that could scan and recognise millions of documents in 24 languages, including on-call tech support in case anything went wrong. In 2004, Google landed a search contract with the CIA. The value of the deal isn't known, but the agency did ask Google's permission to customise the CIA's internal Google search page by placing the CIA's seal in one of the Google logo's Os. "I told our sales rep to give them the OK if they promised not to tell anyone. I didn't want it spooking privacy advocates," wrote Douglas Edwards, Google's first director of marketing and brand management, in his 2011 book I'm Feeling Lucky: The Confessions of Google Employee Number 59. Deals such as these picked up pace and increased in scope after Google's acquisition of Keyhole.

In 2006, Google Federal went on a hiring spree, snapping up managers and salespeople from the army, air force, CIA, Raytheon and Lockheed Martin. It beefed up its lobbying muscle and assembled a team of Democratic and Republican operatives.

Even as it expanded into a transnational multi-billion-dollar corporation, Google had managed to retain its geekily innocent "don't be evil" image. So while Google's PR team did its best to

keep the company wrapped in a false aura of altruism, company executives pursued an aggressive strategy to become the Lockheed Martin of the internet age. “We’re functionally more than tripling the team each year,” Painter said in 2008. It was true. With insiders plying their trade, Google’s expansion into the world of military and intelligence contracting took off.

In 2007, it partnered with Lockheed Martin to design a visual intelligence system for the NGA that displayed US military bases in Iraq and marked out Sunni and Shia neighbourhoods in Baghdad – important information for a region that had experienced a bloody sectarian insurgency and ethnic cleansing campaign between the two groups. In 2008, Google won a contract to run the servers and search technology that powered the CIA’s Intellipedia, an intelligence database modelled after Wikipedia that was collaboratively edited by the NSA, CIA, FBI and other federal agencies. Not long after that, Google contracted with the US army to equip 50,000 soldiers with a customised suite of mobile Google services.

In 2010, as a sign of just how deeply Google had integrated with US intelligence agencies, it won an exclusive, no-bid $27m contract to provide the NGA with “geospatial visualisation services”, effectively making the company the “eyes” of America’s defence and intelligence apparatus. Competitors criticised the NGA for not opening the contract to the customary bidding process, but the agency defended its decision, saying it had no choice: it had spent years working with Google on secret and top-secret programmes to build Google Earth technology according to its needs, and could not go with any other company.

Google has been tight-lipped about the details and scope of its contracting business. It does not list this revenue in a separate column in quarterly earnings reports to investors, nor does it provide the sum to reporters. But an analysis of the federal contracting data-base maintained by the US government, combined with information gleaned from Freedom of Information Act requests and published reports on the company's military work, reveals that Google has been doing brisk business selling Google Search, Google Earth and Google Enterprise (now known as G Suite) products to just about every major military and intelligence agency, including the state department. Sometimes Google sells directly to the government, but it also works with established contractors like Lockheed Martin and Saic (Science Applications International Corporation), a California-based intelligence mega-contractor which has so many former NSA employees working for it that it is known in the business as "NSA West".

Google's entry into this market makes sense. By the time Google Federal went online in 2006, the Pentagon was spending the bulk of its budget on private contractors. That year, of the $60bn US intelligence budget, 70%, or $42bn, went to corporations. That means that, although the government pays the bill, the actual work is done by Lockheed Martin, Raytheon, Boeing, Bechtel, Booz Allen Hamilton and other powerful contractors. And this isn't just in the defence sector. By 2017, the federal government was spending $90bn a year on information technology. It's a huge market – one in which Google seeks to maintain a strong presence. And its success has been all but guaranteed. Its products are the best in the business.

Here’s a sign of how vital Google has become to the US government: in 2010, following a disastrous intrusion into its system by what the company believes was a group of Chinese government hackers, Google entered into a secretive agreement with the NSA. “According to officials who were privy to the details of Google’s arrangements with the NSA, the company agreed to provide information about traffic on its networks in exchange for intelligence from the NSA about what it knew of foreign hackers,” wrote defence reporter Shane Harris in @War, a history of warfare. “It was a quid pro quo, information for information. And from the NSA’s perspective, information in exchange for protection.”

This made perfect sense. Google servers supplied critical services to the Pentagon, the CIA and the state department, just to name a few. It was part of the military family and essential to American society. It needed to be protected, too.

Google didn’t just work with intelligence and military agencies, but also sought to penetrate every level of society, including civilian federal agencies, cities, states, local police departments, emergency responders, hospitals, public schools and all sorts of companies and nonprofits. In 2011, the National Oceanic and Atmospheric Administration, the federal agency that researches weather and the environment, switched over to Google. In 2014, the city of Boston deployed Google to run the information infrastructure for its 76,000 employees – from police officers to teachers – and even migrated its old emails to the Google cloud. The Forest Service and the Federal Highway Administration use Google Earth and Gmail.

In 2016, New York City tapped Google to install and run free wifi stations across the city. California, Nevada and Iowa, meanwhile, depend on Google for cloud computing platforms that predict and catch welfare fraud. Meanwhile, Google mediates the education of more than half of America's public school students.

▲ New York City mapped in an early version of Google Earth from 2006. Photograph: AP

"What we really do is allow you to aggregate, collaborate and enable," explained Scott Ciabattari, a Google Federal sales rep, during a 2013 government contracting conference in Wyoming. He was pitching to a room full of civil servants, telling them that Google was all about getting them – intelligence analysts, commanders, government managers and police officers – access to the right information at the right time. He ran through a few examples: tracking flu outbreaks, monitoring floods and wildfires, safely serving criminal warrants, integrating

surveillance cameras and face recognition systems, and even helping police officers respond to school shootings.

“We are getting this request more and more: ‘Can you help us publish all the floorplans for our school district? If there is a shooting disaster, God forbid, we want to know where things are.’ Having that ability on a smartphone, being able to see that information quickly at the right time saves lives,” he said. A few months after this presentation, Ciabattari met with officials from Oakland, California to discuss how Google could help the city build its police surveillance centre.

This mixing of military, police, government, public education, business and consumer-facing systems – all funnelled through Google – continues to raise alarms. Lawyers fret over whether Gmail violates attorney-client privilege. Parents wonder what Google does with the information it collects on their kids at school. What does Google do with the data that flows through its systems? Is all of it fed into Google’s big corporate surveillance pot? What are Google’s limits and restrictions? Are there any? In response to these questions, Google offers only vague and conflicting answers.

Of course, this concern isn’t restricted to Google. Under the hood of most other internet companies we use every day are vast systems of private surveillance that, in one way or another, work with and empower the state. On a higher level, there is no real difference between Google’s relationship with the US government and that of these other companies. It is just a matter of degree. The sheer breadth and scope of Google’s technology make it a perfect stand-in for the rest of the commercial internet ecosystem.

Indeed, Google's size and ambition make it more than a simple contractor. It is frequently an equal partner that works side by side with government agencies, using its resources and commercial dominance to bring companies with heavy military funding to market. In 2008, a private spy satellite called GeoEye-1 was launched in partnership with the National Geospatial-Intelligence Agency; Google's logo was on the launch rocket and the company secured exclusive use of the satellite's data for use in its online mapping. Google also bought Boston Dynamics, a robotics company that made experimental robotic pack mules for the military, only to sell it off after the Pentagon determined it would not be putting these robots into active use. It has invested $100m in CrowdStrike, a major military and intelligence cyber defence contractor that, among other things, led the investigation into the alleged 2016 Russian government hacks of the Democratic National Committee. And it also runs Jigsaw, a hybrid thinktank/technology incubator aimed at leveraging internet technology to solve thorny foreign policy problems – everything from terrorism to censorship and cyberwarfare.

Founded in 2010 by Eric Schmidt and Jared Cohen, a 29-year-old state department whizz-kid who served under both George W Bush and Barack Obama, Jigsaw has launched multiple projects with foreign policy and national security implications. It ran polling for the US government to help war-torn Somalia draft a new constitution, developed tools to track global arms sales, and worked with a startup funded by the state department to help people in Iran and China route around internet censorship.

It also built a platform to combat online terrorist recruitment and radicalisation, which worked by identifying Google users interested in Islamic extremist topics and diverting them to state

department webpages and videos developed to dissuade people from taking that path. Google calls this the “redirect method”, a part of Cohen’s larger idea of using internet platforms to wage “digital counterinsurgency”. And, in 2012, as the civil war in Syria intensified and American support for rebel forces there increased, Jigsaw brainstormed ways it could help push Bashar al-Assad from power. Among them: a tool that visually maps high-level defections from Assad’s government, which Cohen wanted to beam into Syria as propaganda to give “confidence to the opposition”.

Jigsaw seemed to blur the line between public and corporate diplomacy, and at least one former state department official accused it of fomenting regime change in the Middle East. “Google is getting [White House] and state department support and air cover. In reality, they are doing things the CIA cannot do,” wrote Fred Burton, an executive at global intelligence platform Stratfor and a former intelligence agent at the security branch of the state department.

But Google rejected the claims of its critics. “We’re not engaged in regime change,” Eric Schmidt told Wired. “We don’t do that stuff. But if it turns out that empowering citizens with smartphones and information causes changes in their country … you know, that’s probably a good thing, don’t you think?”

Jigsaw’s work with the state department has raised eyebrows, but its function is a mere taste of the future if Google gets its way. As the company makes new deals with the NSA and continues its merger with the US security apparatus, its founders see it playing an even greater role in global society.

Why Silicon Valley can’t fix itself

Read more

“The societal goal is our primary goal. We’ve always tried to say that with Google. Some of the most fundamental questions people are not thinking about … how do we organise people, how do we motivate people? It’s a really interesting problem – how do we organise our democracies?” Larry Page ruminated during a rare interview in 2014 with the Financial Times. He looked a hundred years into the future and saw Google at the centre of progress. “We could probably solve a lot of the issues we have as humans.”

This is an edited extract from Surveillance Valley: The Secret Military History of the Internet by Yasha Levine, which will be published by Icon on 3 January, and is available to preorder at guardianbookshop.com