The Orwellian legacy of 9/11:
Unprecedented Mass Surveillance

After the 9/11 attacks, one big concern was connecting the dots. Failing to do so was why we missed the warning signs of the attacks and how we would prevent the next ones, the thinking went. One solution, according to the Pentagon, was a project to gather as much data as possible, to look for signs of future bad behavior. It was called **Total Information Awareness.**

If the name evoked **George Orwell**, and the concept echoed **Philip K. Dick**, the logo, an all-seeing eye atop a pyramid, Illuminati-style, capturing the entire earth in its gaze. With the Latin Motto: Knowledge is Power.

By late 2002, news reports revealed that TIA was the brainchild of **John Poindexter**, who a previous generation would remember as the head of President Ronald Reagan's National Security Council, and who was convicted in 1990 on five felony counts for his role in the Iran-Contra scandal. The convictions were later overturned because he had been given immunity for his testimony during a Congressional investigation.

On January 14, Poindexter returned to the government to run TIA—what he'd pitched as a ***"Manhattan Project for counterterrorism"***—under the auspices of the Defense Advanced Research Projects Agency, better known as DARPA. The idea was to integrate components from previous and existing government surveillance projects, including those focused on facial and gait recognition, language translation, and the latest in data mining, using both classified and commercially available information. The goal was to mine every possible piece of data about people's lives, without the need for a warrant. But after enough media reporting on the program and its implications for such mass surveillance were exposed, Congress raced to shut it down in a 2003 amendment, and **the program appeared to disappear.**

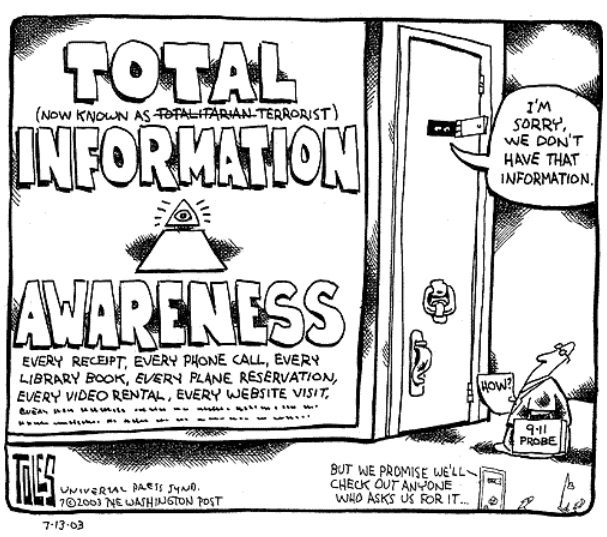
In reality, all that disappeared were its name and its logo. As the War on Terror unfolded, under the authority of a series of secret presidential orders, TIA's systems would be redistributed across the intelligence community. Its core architecture was subsequently developed under the code name "Basketball." One program at the National Security Agency (NSA) would be known as **PRISM**, an effort designed to gather the world's internet communications, alongside phone and internet metadata. Like its private sector analog, **Palantir,** the new name evoked some kind of magical crystal. Technology would advance to the point where the NSA could store a copy of the internet in a data center in the Utah desert. Data mining would become machine learning. The motto also evolved: "Knowledge is power" became, as one NSA slide famously put it years later, ***"Collect it all."***

Since the 1970s, Congress has been charged with preventing further abuse of the government's surveillance powers, particularly when it comes to spying on Americans. And few in Congress have questioned these powers as vigorously as Sen. Ron Wyden. The Oregon lawmaker led the effort to kill TIA in 2003; a decade later, when it became clear to him that TIA had not only survived but was thriving in secret and extralegal ways, he posed a famous question to then-director of National Intelligence James Clapper during a rare public hearing.

"Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?"

"No, sir, not wittingly," Clapper responded. You could tell from the senator's incredulous look that he knew this was false, as did a growing number of other people. (The intelligence chief would later explain that he thought Wyden was referring to something other than the NSA's phone metadata program.) The first reforms would begin in earnest a few months later, after NSA contractor Edward Snowden revealed to journalists a TIA-style surveillance system that many had long suspected existed but could have never quite imagined. Snowden said that Clapper's response to Wyden was one of the reasons he decided to go through with it.

Still, even after a series of reforms, TIA has become totally normal. Its programs and concepts have spread across the government and private sector, from secret government agencies to local police departments. Today, the frontier of mass domestic surveillance is the wide array of personal data that can be easily purchased on the private market. While there are dozens of U.S. privacy laws, none require government agents to get a warrant if they want to buy Americans' data in bulk from, say, a data broker or a facial recognition company. It's a practice that actually dates back to the days of TIA's inception, and that continues at a number of government agencies. Wyden, together with Sen. Rand Paul, has proposed a bill to fix this, called the ***"Fourth Amendment Is Not For Sale Act."***



The secrecy surrounding government spying programs makes it difficult to debate mass surveillance, to say nothing of challenging their legality in court. Meanwhile, it remains unclear how effective mass surveillance is at thwarting terrorist plots. Before the 2015 USA Freedom Act ended bulk collection of metadata, reports by two independent groups, the extensive Privacy and Civil Liberties Oversight Board and the President's Review Group on Surveillance, found little evidence to support claims that the program was essential to national security.

Even the notion that fueled TIA was a fallacy, the idea that we needed to collect more data. In fact, "The System was Blinking Red" is the title of one of the chapters of the 9/11 Commission Report. We already had many of the dots, and even had many of them connected. The real failures were human ones, related to policy, ideology, bureaucracy.

I recently spoke with Sen. Wyden about the early days of TIA and how he's still fighting its legacy.

What is the legacy of Total Information Awareness?

Senator Wyden: *"Total Information Awareness was an ominous sounding idea to put together as much data on Americans as possible, and when used with what was then so-called predictive technology, identify who to watch as a way to stop terror*

ism. In the fight in Congress, here's the lesson that goes to the concerns we had 20 years ago: Total Information Awareness made it clear that the threat is not just surveillance through the aggressive collection, amalgamating, and mining of information through existing authorities. The bigger problem now is the amount of data on Americans that's available commercially or on social media.

So the government doesn't use Orwell-type phrases like "Total Information Awareness." But for those of us who believe that it's possible to protect liberty as we promote our security—the two are not mutually exclusive—our job is even harder. Because the government doesn't use Orwellian phrases, but the threat to people's privacy is just as great. And the job of getting people's attention is still very, very challenging."

Total Information Awareness got a lot of people's attention back in 2002. How do you look back at the fight against it now, almost two decades later?

"*The fact was that we won an important fight because [TIA] was so encompassing, so sweeping, that it would have been enormously bad defeat for this whole question about whether liberty and security were mutually exclusive. But you can have both…*

"People were furious! Even the most conservative senators came up to me and said, 'You're right. This program is way off the rails.'

Now we're faced with how the government uses commercial data. So I introduced the Fourth Amendment Is Not For Sale Act to prevent the government from going around the courts and violating people's constitutional rights. [These rights] can be diminished just because the government can find a data broker who wants to sell private records without having to go through a court judicial process and get a court order…

The technology showed that it was capable of practically anything. In other words, there was no protection for people's privacy. For instance, Alex [used to] know that there was some protection for his privacy, simply because there were things that the technology simply wasn't capable of getting. But as we raise that bar, the technology can accumulate more and more data, surveillance programs are getting more of your private information, and it becomes more important. Virtually every few months [we had] to make sure that this balance of power between the state and the citizenry wasn't constantly altered because the technology was more capable of expanding the surveillance power of government over the American people."

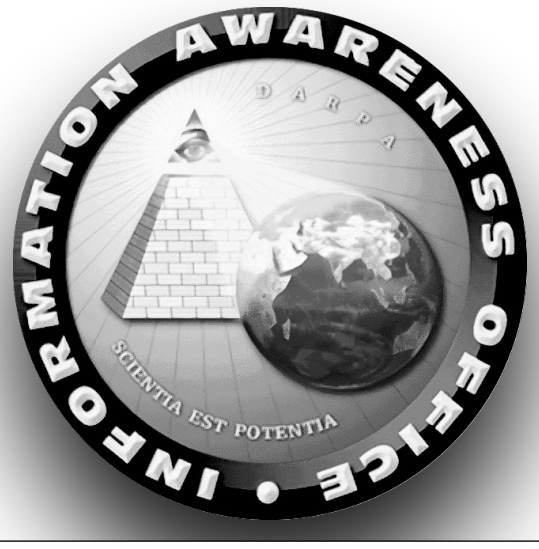
And it was happening in secret.

"James Clapper lied to me in an open public hearing in the Senate about government surveillance authority. I actually sent him the question in advance, because we had tried and tried to get it in an open public forum. So the government was increasingly brazen during those times.

And I opposed the PATRIOT Act when it came up for reauthorization because of all the things we'd learned—that the PATRIOT Act had been secretly interpreted to permit mass surveillance, and that there was a big gap between what the public thought the law said about domestic surveillance and what the government decided the law said. We debated how to handle it, particularly given the Senate rules that prohibit individual senators from publicly discussing classified information. But we worked for months and months to be able to ask James Clapper that question in an open session."

The legacy of the TIA program

"I never bought the idea that the supporters of that underlying philosophy would say, 'It got killed, let's call it a day, let's move on.' I think privacy is an even bigger problem today, especially given the amount of data on Americans that is available in so many ways, commercially, social media, and you talk about the prospect of foreign governments getting it! So, yes, I managed to kill the Total Information Awareness program, which at that time would have been far and away the biggest invasion of the privacy rights of Americans in history. But I have no illusions that these threats to America's privacy have somehow gone away with the killing of Total Information Awareness…"



Defense Advanced Research Projects Agency:
Office of Information Awareness
"Knowledge is Power"

"After 9/11, I took the threat of terrorism seriously, still do. But also I was concerned about how the new surveillance authorities might be abused. When there was the first expiration date [of the PATRIOT Act], to ensure that Congress could come back and reconsider the authorities after the panic had passed, I opposed the reauthorization. I thought it was too broad. I just think Congress misunderstood how it would be used. And that's why, in the years that followed, I was more and more amazed at what was really going on. And particularly about the secret interpretations that permitted the mass surveillance of millions of Americans."

The Biden White House hasn't asked to reauthorize section 215 of the PATRIOT Act, which previously allowed the NSA and the FBI to collect vast amounts of data on people in the U.S. But section 702 of the Foreign Intelligence Surveillance Act continues to permit this, and allows for the FBI's "***backdoor-search loophole***." And then there's executive order 12333, which also allows for the collection of Americans' data. What do you think of how the government is using its surveillance powers today?

"My job is to hold officials accountable no matter who's the president, and I intend to do it. I've had a number of conversations with [CIA] Director Haines, talking particularly about the Fourth Amendment Is Not For Sale [Act], and how the government is collecting information. And I'm also very troubled about private sector surveillance.

This is a national security issue: The personal data of Americans that the data brokers are selling is a gold mine for foreign intelligence services who can exploit it, to target supercharged hacking, blackmail, and influence campaigns. So I'm leading an effort right now that encompasses the biggest online advertising companies, to ask if they're sharing Americans' web browsing and location data with foreign companies.

I'm very concerned about what's happening there, and you don't have to be a technology expert or a government official to understand the risks of selling sensitive data about Americans to Russia and China. It's a colossally bad idea. In the next two months, I'll be introducing legislation to regulate the export of Americans' data to countries that are likely to exploit it in ways that will harm U.S. national security. I think this is a no-brainer issue, and I'm hoping to get it out on the Senate floor with broad bipartisan support."

How have you seen support in Congress evolve when it comes to addressing surveillance and privacy?

"It's still a small group of us—Sen. Heinrich, Sen. Leahy have been particularly helpful on the Democratic side. On the Republican side, Sen. Lee, Sen. Paul. And we've got new members that are very interested. Sen. Ossoff talked to me about these issues, the new senator from Georgia, and I think he's going to be a real privacy hawk. I'm looking forward to working with him. But we're a smaller group. Sometimes I kid that we're the Ben Franklin caucus. Anybody who gives up liberty for security, according to Franklin, doesn't deserve either.

I was there on January 6th. I saw with my own two eyes what domestic terrorism was all about. Now we know that these Trump people and their supporters are trying to rewrite history as we speak. So I think journalists particularly now have such a strong responsibility. Also, I'm one of the real leaders in the Senate for supporting whistleblowers, which is another key component of getting the truth out. I just can't emphasize that enough in terms of these debates. Because I'll often go to an event or watch an event, and then I'll watch people looking for an ideological advantage, to describe it in a way that is completely disconnected from the facts.

And also, so we are clear, giving federal agencies more power to spy on Americans, bigger budgets, didn't stop the attack. Because the agencies decided that right wing violence wasn't a real threat. So until there's an honest reckoning of some politicians, some in law enforcement, who are willing to tolerate and stoke this, right-wing violent criminals will continue to believe they can act with impunity…you had some measure of security before because there were areas technology couldn't get to in terms of violating your rights.

Now technology can accomplish so much more intrusive data-privacy-violating activities that nobody thought about back then. The challenge is even greater. There's a handful of us, on both sides of the aisle, who've spent a lot of time on it. But I think there's a lot of work to do."

Alex Pasternack
fastcompany.com