THE 9/11 SURVEILLANCE STATE

HOW FORTY-FIVE DAYS IN 2001 BUILT A PERMANENT ARCHITECTURE OF MASS SURVEILLANCE

SEPTEMBER 11, 2026

EXECUTIVE SUMMARY

Twenty-five years ago today, nineteen hijackers killed 2,977 people. Within 45 days, Congress had passed — largely unread — a law that rewired American surveillance authority. Within a month of that, the NSA was running a warrantless dragnet on Americans' communications under a secret presidential order. Within four months, a convicted Iran-Contra felon was standing up a DARPA office whose explicit goal was a "virtual, centralized grand database" of every transaction in American life.

This report traces how those first months hardened into permanent infrastructure. The pattern that emerges across every domain — law, technology, institutions, and industry — is a **RATCHET**: emergency powers that only ever tighten, programs that die in public and survive in the classified budget, and a private industry that now performs functions the Constitution would forbid the government to perform directly.

Five findings anchor the report:

1. **THE LEGAL RATCHET NEVER REVERSED.** Of the sixteen PATRIOT Act surveillance provisions given sunset dates, fourteen were made permanent in 2006. The two most abused powers — National Security Letters and sneak-and-peek warrants — never had sunsets at all [10][8]. Section 702, sold in 2008 as a targeted fix, has been renewed three times, most recently in 2024 with an *expanded* definition of who can be conscripted to assist [22].

2. **Total Information Awareness never died.** Congress "terminated" DARPA's TIA program in September 2003 — while a classified annex to the same law moved its core components to the NSA's research arm at Fort Meade, where they were renamed "Basketball" and "Topsail" and kept their funding, sometimes under the same contracts [34][35].
3. **The Snowden disclosures confirmed the TIA vision had been built.** Bulk phone metadata on virtually every American call, PRISM collection from nine major tech companies, backbone taps at AT&T facilities, five billion phone-location records a day — assembled piecemeal under strained readings of statutes passed in the panic of 2001 [54][55][59].
4. **A surveillance-industrial complex now performs the state's collection.** Roughly 70% of the intelligence budget flows to contractors [79]. The CIA seeded Palantir; Booz Allen employed both the DNI who ran the system and the analyst who exposed it; and a generation of companies — Flock, Clearview, data brokers like Venntel — now sells the government data it would need a warrant to collect itself [70][89].
5. **The most durable machinery is the least known.** AT&T's Hemisphere database (four trillion call records, still operating as "Data Analytical Services"), the DEA's parallel-construction training, FBI stingray non-disclosure agreements, and post-*Carpenter* data purchases are all engineered specifically to keep surveillance out of courtrooms [112][116][119][137].

Every factual claim is cited to the references section. The `documents/` folder accompanying this report contains the primary sources: statute texts, inspector general reports, declassified FISA court opinions, leaked slide decks, and court rulings.

---

1. Forty-Five Days: The USA PATRIOT Act

A Bill Nobody Read

The USA PATRIOT Act was not written in October 2001; it was assembled. Attorney General John Ashcroft delivered the Justice Department's draft "Anti-Terrorism Act" to Congress during the week of September 19, 2001, demanded passage within a week, and warned that Congress would bear responsibility for the next attack if it delayed [3]. Many provisions were recycled from DOJ and FBI wishlists that Congress had rejected before 9/11 [3]. The final bill — H.R. 3162, introduced October 23 — reached the House floor the same day it was introduced and passed 357–66; during part of the drafting window, the anthrax attacks had closed congressional office buildings, cutting staff off from their own files [2]. There was no conference report and essentially no hearings on the final text

[2]. Rep. John Conyers said on the floor that members were voting with "only two copies of the bill" available on his side of the aisle [2].

The Senate passed it 98–1 on October 25 [1]. The lone dissenter, Russ Feingold, warned: "We will lose that war without firing a shot if we sacrifice the liberties of the American people" [4]. Bush signed it October 26, 2001 — 45 days after the attacks.

WHAT IT ACTUALLY CHANGED

- **SECTION 215** gutted FISA's requirement of "specific and articulable facts" tying records to a foreign agent, replacing it with a relevance standard and expanding reach from defined business records to *any tangible thing* from any entity — libraries, doctors, ISPs. This became the hook for NSA bulk phone-metadata collection [5].
- **SECTION 206** created roving FISA wiretaps, including "John Doe" taps naming neither target nor facility — with no requirement, unlike criminal wiretaps, that the target actually be using the tapped line [6].
- **SECTION 213** codified "sneak and peek" delayed-notice searches for *any* federal crime, not just terrorism [7].
- **SECTION 216** extended pen-register authority built for phone numbers to internet metadata — email headers, IP addresses, URLs — on a certification a judge is required to grant [7].
- **SECTION 505** put National Security Letters — demands for records with no judge and a categorical gag order — in the hands of every FBI field office head, requiring only "relevance" to a national-security investigation [9].

THE ABUSE ARRIVED ON SCHEDULE

The DOJ Inspector General found the FBI issued 143,074 NSL requests in 2003–2005 — up from roughly 8,500 per year before the Act — with legal violations in 22% of files examined, more than 700 "exigent letters" falsely claiming emergencies, and NSLs used to grab records *after the FISA Court had twice refused* Section 215 orders in the same investigation on First Amendment grounds [10]. The IG called the exigent-letter practice so "casual, routine, and unsupervised" that phone-company employees sometimes drafted the letters for FBI agents to sign — and a 2010 follow-up found senior officials had issued eleven after-the-fact "blanket NSLs" to retroactively paper over the illegal requests [10][101]. A federal court struck down the NSL statute's gag regime as an unconstitutional prior restraint in 2004 [11].

Sneak-and-peek told the same story in mission-creep form. From September 2001 to April 2003 there were 47 delayed-notice warrant requests. By FY2013 there were 11,129 — of which 51, about 0.5%, involved terrorism; the overwhelming majority were drug cases [8]. By FY2020 courts were issuing nearly 20,000 a year, still more than 70% narcotics [7].

THE RATCHET IN STATUTE FORM

- **2006:** Of sixteen sunsetted provisions, fourteen made permanent; only §215 and §206 kept expiration dates [12]. (§213 and §505 — the most abused — were permanent from day one.)
- **2011:** Obama signed a clean four-year extension by autopen from France, hours before expiration [13].
- **2015:** The USA FREEDOM Act — the only genuine post-Snowden contraction — ended NSA bulk collection but preserved the authorities and created a carrier-held call-detail-records regime [14]. That regime promptly failed: in 2018 the NSA collected 434 million call records from just 11 targets, then had to delete ~685 million records it was never authorized to receive; it quietly suspended the program in 2019 [15].
- **2020:** Section 215 finally lapsed — not by choice, but because the House and Senate passed irreconcilable renewal bills. Grandfather clauses kept existing investigations running [16].
- **2008–2024:** The FISA Amendments Act created Section 702 and killed some 40 telecom lawsuits with retroactive immunity [17][18]. It was renewed without reform in 2012 [19], renewed again in 2018 [20], and renewed again in 2024 as RISAA — which *expanded* the definition of "electronic communication service provider" so broadly that critics warned it could conscript data centers, landlords, and IT contractors into NSA assistance; the FISA Court has kept the provision's actual scope classified [21][22].

Emergency powers, in other words, were converted into permanent ones at every decision point where reversal was possible.

---

2. THE DREAM OF TOTAL INFORMATION: TIA AND ITS AFTERLIVES

POINDEXTER'S MACHINE

In January 2002, DARPA stood up the Information Awareness Office under retired Rear Admiral John Poindexter — Reagan's national security adviser, convicted in 1990 on five felony counts in Iran-Contra (overturned on appeal because his immunized testimony had tainted the witnesses) [23][24]. Poindexter had called his old DARPA partner Brian Sharkey — an executive at Hicks & Associates, a wholly owned SAIC subsidiary — on the morning of September 12, 2001, to pitch the system [25].

His DARPAtech speech laid out the thesis with unusual candor: terrorists "must engage in transactions and they will leave signatures in this information space," and the goal was to treat "the world-wide, distributed, legacy data bases as if they were one centralized data base" [26]. The office's logo was the all-seeing eye atop the pyramid, gazing at the globe, over the motto *scientia est potentia* — knowledge is power. It was quietly scrubbed from the website in December 2002 after public ridicule [23][29].

The components read today like a product roadmap for the modern surveillance stack: Genisys (a "virtual, centralized grand database" of transactions), EELD (link analysis), HumanID (face and gait recognition at a distance), TIDES (mass translation and text mining), Genoa II (analyst collaboration tools), Bio-Surveillance, and Wargaming the Asymmetric Environment — roughly $317 million across FY2001–2003 [23][27]. A related DARPA program, LifeLog, aimed to record a person's entire existence; it was canceled February 4, 2004 — the same week Facebook launched [38].

THE PUBLIC DEATH

William Safire's November 14, 2002 column "You Are a Suspect" detonated the program: "Every purchase you make with a credit card, every magazine subscription... every Web site you visit and e-mail you send or receive... will go into what the Defense Department describes as 'a virtual, centralized grand database'" [28]. Congress restricted funding in February 2003 [30]; DARPA renamed the program "Terrorism Information Awareness" in May — a change EFF compared to the FBI renaming Carnivore "DCS-1000" [31]. In July, Wyden and Dorgan exposed FutureMAP, an IAO prediction market that would have let traders bet on assassinations and terror attacks; the Pentagon killed it within a day, and Poindexter resigned weeks later [32][33]. In September 2003, the FY2004 Defense Appropriations Act directed "that the Office be terminated immediately" [34].

THE CLASSIFIED AFTERLIFE

The same law contained the escape hatch: TIA-style "processing, analysis, and collaboration tools" described in the *classified annex* could continue, funded through the National Foreign Intelligence Program [34]. Shane Harris's reporting in *National Journal* documented what happened next: the core projects moved to ARDA — the intelligence community's research arm housed at NSA headquarters, Fort Meade. Genoa II became "Topsail." The Information Awareness Prototype System became "Basketball." Funding "remained intact, sometimes under the same contracts"; Sharkey told TIA contractors, "A new sponsor has come forward that will enable us to continue much of our previous work" [35][36]. When Wyden asked in a 2006 hearing whether TIA components had moved to other agencies, Michael Hayden asked to answer in closed session [35]. ARDA became the Disruptive Technology Office, which was folded into IARPA in 2007 — where the research lineage continues today [37].

The kill was cosmetic in a second sense: the approach had already metastasized. A May 2004 GAO survey found 199 federal data-mining efforts operational or planned, 122 using personal information [40]. The states got MATRIX — data broker Seisint's "High Terrorist Factor" scoring of millions of Americans, which handed a list of 120,000 top-scoring names to federal agents before privacy backlash shut it down in 2005 (LexisNexis bought Seisint for $775 million) [39]. DHS got ADVISE, killed in 2007 after it was caught testing on live personal data without privacy assessments [41]. Rumsfeld's own advisory committee concluded in 2004 that killing TIA had simply left the underlying activities running *without* oversight [42].

The through-line matters: TIA is the only moment the American public was asked, explicitly, whether it wanted a total-information architecture. It said no. The architecture was built anyway — at NSA, in the classified budget, on statutory authorities passed in October 2001. Snowden's documents are the proof of completion.

---

3. STELLAR WIND TO SNOWDEN: THE NSA'S DOMESTIC TURN

THE SECRET ORDER

On October 4, 2001 — three weeks before the PATRIOT Act — Bush signed the first authorization of the President's Surveillance Program, codenamed STELLARWIND, reauthorized every 30–45 days on his sole authority, bypassing the FISA Court entirely [43]. The NSA Inspector General's leaked

draft history describes its four baskets: content of international phone calls, content of international emails, bulk telephony metadata, and bulk internet metadata [44].

The program's illegality was severe enough to nearly decapitate the Justice Department. On March 10, 2004, with Ashcroft hospitalized and DOJ refusing to recertify the internet-metadata basket, White House Counsel Alberto Gonzales and Chief of Staff Andrew Card went to Ashcroft's hospital room to extract his signature; Ashcroft, "summoning the strength to lift his head," refused. Bush reauthorized the program the next day without DOJ certification, and only modified it after Comey, Mueller, Goldsmith, and some thirty officials threatened to resign en masse [45]. Over the following years the program's pieces were laundered into legal process: internet metadata onto a FISC pen-register order (2004), phone metadata onto Section 215 (first order May 24, 2006), and content collection into the Protect America Act and then Section 702 (2008) [43][61].

The public learned fragments early. James Risen and Eric Lichtblau's NYT story — "Bush Lets U.S. Spy on Callers Without Courts," held by the paper for roughly thirteen months under White House pressure — ran December 16, 2005 and won the Pulitzer [46]. USA Today revealed the call-records database in May 2006, noting that Qwest alone had refused [47].

THE WHISTLEBLOWERS BEFORE SNOWDEN

Inside NSA, the dissent predated all of it. Bill Binney, Kirk Wiebe, and Ed Loomis had built ThinThread — a collection-and-analysis system costing about $3.2 million that *encrypted and anonymized U.S.-person data by design*. NSA director Michael Hayden rejected it in favor of Trailblazer, a contractor program led by SAIC that consumed roughly $1.2 billion and never produced a deployable system; when ThinThread components were later used, the privacy protections were stripped out [48]. The group's 2002 DoD Inspector General complaint was vindicated by a scathing 2004 audit [49]. The government's response was to raid their homes and prosecute Thomas Drake — who had given *unclassified* evidence of Trailblazer waste to the Baltimore Sun — under the Espionage Act. The case collapsed days before trial to a single misdemeanor; the sentencing judge called the government's four-year pursuit of Drake "unconscionable" [50].

Meanwhile in San Francisco, AT&T technician Mark Klein revealed Room 641A at 611 Folsom Street: a secret NSA room fed by fiber-optic splitters that copied backbone internet traffic into a Narus STA 6400 deep-packet-inspection appliance [51]. EFF's resulting class action, *Hepting v. AT&T*, survived a state-secrets challenge — and was then killed by Congress itself via the 2008 retroactive-immunity provision [52]. The successor suit against the government, *Jewel v. NSA*, was

dismissed on standing and state-secrets grounds without any court ever reaching the merits; the Supreme Court declined to hear it in 2022 [53].

JUNE 2013

The Snowden disclosures turned allegation into record:

- **THE VERIZON ORDER** (June 5, 2013): a FISC order compelling production, "on an ongoing daily basis," of all call detail records "wholly within the United States, including local telephone calls" — the bulk 215 program, renewed every 90 days since May 2006, 41 times by early 2014 [54][61].
- **PRISM** (June 6): Section 702 downstream collection from nine companies, with slide-documented onboarding dates — Microsoft 2007, Yahoo 2008, Google 2009, Facebook 2009, YouTube 2010, Skype 2011, AOL 2011, Apple 2012 [55].
- **BOUNDLESS INFORMANT** (June 8): NSA's own heat map, showing 97 billion intelligence records collected in a single month [56].
- **XKEYSCORE** (July 31): the analyst front-end — searchable emails, chats, and browsing histories across 700+ servers, no prior authorization required [57].
- **MUSCULAR** (October 30): NSA and GCHQ tapping the private fiber between Google and Yahoo data centers *overseas* — outside FISA entirely, under Executive Order 12333 — 181 million records in 30 days, memorialized in the hand-drawn slide reading "SSL added and removed here! :)" [58].
- **CO-TRAVELER** (December 4): roughly five billion cellphone-location records per day, worldwide, used to find associates by co-movement [59]. **DISHFIRE** (January 2014): nearly 200 million text messages a day [60].

The scale had a doctrine behind it. As one former official summarized Keith Alexander's approach: "Rather than look for a single needle in the haystack, his approach was, 'Let's collect the whole haystack'" [68]. The FY2013 black budget Snowden leaked: $52.6 billion, $10.8 billion of it NSA's [67]. The storage went to the $1.5 billion, million-square-foot Utah Data Center at Bluffdale [69].

WHAT OVERSIGHT FOUND WHEN IT FINALLY LOOKED

- The FISA Court itself, in Judge John Bates's declassified October 2011 opinion, found upstream collection was acquiring some 250 million internet communications a year including tens of thousands of wholly domestic ones, held the procedures unconstitutional

in part, and noted this was "the third instance in less than three years" of the government substantially misrepresenting a major program to the court [63].

- The Privacy and Civil Liberties Oversight Board concluded in January 2014 that the bulk 215 program lacked statutory authorization and could identify "no instance" in which it "made a concrete difference in the outcome of a counterterrorism investigation" [61]. Its July 2014 report on 702 found that program lawful "at its core" but recommended ten reforms [62].
- Judge Richard Leon called the metadata program "almost Orwellian": "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion'" [64]. The Second Circuit held in *ACLU v. Clapper* (2015) that the program "exceeds the scope of what Congress has authorized" [65]. The Ninth Circuit in *United States v. Moalin* (2020) held it violated FISA and noted the government's claims about the program's value were "inconsistent with the contents of the classified record" [66].

ILLEGAL, MISREPRESENTED TO ITS OWN COURT, AND USELESS BY ITS OVERSEERS' ACCOUNT — AND YET THE ONLY STRUCTURAL CONSEQUENCE WAS THE USA FREEDOM ACT'S HALF-REFORM, WHOSE REPLACEMENT REGIME FAILED OF ITS OWN OVERCOLLECTION AND WAS QUIETLY ABANDONED [15].

---

4. THE SURVEILLANCE-INDUSTRIAL COMPLEX

PALANTIR: THE CIA'S STARTUP

Palantir was incorporated in 2003–04 by Peter Thiel with Alex Karp, Joe Lonsdale, Stephen Cohen, and PayPal engineer Nathan Gettings, on the premise of adapting PayPal's fraud-detection pattern analysis to counterterrorism [70]. The CIA's venture arm In-Q-Tel invested roughly $2 million in 2005, and from 2005 to 2008 the CIA was Palantir's *only* customer — agency analysts iterated directly on what became the Gotham platform [70]. From that seed: ICE contracts totaling roughly $435 million (FALCON, the Investigative Case Management system, and 2025's "ImmigrationOS") [73]; a secret 2012–2018 predictive-policing deployment in New Orleans routed through a philanthropic arrangement that even city council members didn't know about [72]; LAPD's Operation LASER,

arranged via the police foundation to bypass council approval [71]; and a JPMorgan insider-threat program that spiraled into monitoring employees' emails, GPS trails, and browser histories [71]. Palantir went public in 2020; by late 2025 its *quarterly* U.S. government revenue was $486 million [70].

In-Q-Tel's broader portfolio shows the model at scale: Keyhole (bought by Google in 2004, becoming Google Earth) [74]; and a 2016 Intercept analysis of 38 undisclosed investments heavy in social-media mining — Dataminr, Geofeedia, PATHAR, TransVoyant [75]. Geofeedia was caught marketing protest surveillance to police — helping Baltimore "stay one step ahead of rioters" during the Freddie Gray protests — before the platforms cut its access [76].

BOOZ ALLEN AND THE REVOLVING DOOR

The Carlyle Group bought Booz Allen's government business for $2.54 billion in 2008; ~97–99% of its revenue comes from the U.S. government [77]. Mike McConnell's career is the system in one résumé: NSA director → Booz Allen senior VP → Director of National Intelligence → Booz Allen vice chairman [78]. James Clapper also passed through Booz Allen on his way to DNI [78]. And it was a Booz Allen infrastructure analyst on an NSA contract in Hawaii — Edward Snowden — who walked out with the archive [70]. Tim Shorrock's reporting established the headline number, from a DIA industry-conference slide: intelligence outsourcing is "a $50 billion-a-year business that consumes up to 70 percent of the U.S. intelligence budget" [79].

The Washington Post's *Top Secret America* investigation (2010) mapped the result: 1,931 private companies working top-secret programs at some 10,000 locations, 854,000 people holding top-secret clearances — "a hidden world, growing beyond control... so large, so unwieldy and so secretive that no one knows how much money it costs, how many people it employs, how many programs exist within it" [83]. SAIC's Trailblazer — supervised at NSA by a deputy director rehired from SAIC itself — is the complex's type specimen: a billion dollars, nothing delivered, whistleblowers prosecuted [49][50].

THE TELECOMS: PARTNERS, NOT CONSCRIPTS

NSA documents published by the NYT and ProPublica in 2015 describe AT&T's relationship with the agency — codename FAIRVIEW, dating to 1985 — with the phrase "extreme willingness to help": surveillance equipment in at least 17 U.S. internet hubs, billions of emails and call records, assistance wiretapping the United Nations. "This is a partnership, not a contractual relationship," one document notes [80]. Verizon/MCI was the smaller STORMBREW partner [80].

The countercase proves the rule. Qwest CEO Joseph Nacchio met with NSA on **FEBRUARY 27, 2001 – MORE THAN SIX MONTHS BEFORE 9/11** — and refused a surveillance request his lawyers deemed illegal. He was subsequently prosecuted for insider trading, and his defense that the prosecution was retaliation was excluded from trial on state-secrets grounds [81]. The telecoms that did cooperate faced some 40+ lawsuits — all extinguished by the retroactive immunity Congress granted in 2008 [82][52].

THE POST-SNOWDEN GENERATION

The model — venture-backed companies performing state surveillance functions — is now the default:

- **AMAZON** won the CIA's $600 million cloud contract in 2013, putting intelligence-community data on commercial infrastructure [84].
- **ANDURIL** (2017, Palmer Luckey plus ex-Palantir executives, Thiel-backed) built CBP's AI surveillance-tower "virtual wall"; $30.5 billion valuation by 2025 [85].
- **CLEARVIEW AI** scraped 30+ billion face images from social media and sold search access to police — nearly a million searches by 2023 [86].
- **FLOCK SAFETY** has ~90,000 license-plate-reader cameras across thousands of communities — a de facto national vehicle-tracking network searchable by police without warrants [87].
- **L3HARRIS** (Stingrays) sold cell-site simulators under FBI-mandated NDAs; **DATA BROKERS** — Venntel, Babel Street, Fog Data Science — sell phone-location data to DHS, IRS, FBI, and local police for as little as $7,500 a year [88].

The ODNI's own declassified 2022 report on "commercially available information" concedes the point: the intelligence community buys large amounts of Americans' data, doesn't fully know how much, and acknowledges the data "can reveal sensitive and intimate information" and could "be used to identify every person who attended a protest or rally" [89]. The FBI even bought and tested NSO Group's Pegasus — including "Phantom," a version built to target U.S. phones — at a secret New Jersey facility [90].

One caveat belongs on the record here. The 2001 Fox News reporting on Israeli-founded intercept vendors (Comverse/Verint, Amdocs) documented genuine counterintelligence *concerns* about foreign-built equipment inside U.S. wiretap and billing infrastructure — Narus, also Israeli-founded, built the Room 641A appliance — but the espionage allegations were never prosecuted and remain unproven; the verifiable core is the deep placement of these vendors in U.S. infrastructure, not confirmed spying [51].

---

5. THE INSTITUTIONAL BUILD-OUT

NEW AGENCIES, NEW DATABASES

The Homeland Security Act (November 25, 2002) merged 22 agencies and ~180,000 employees — the largest federal reorganization since 1947; DHS is now the third-largest cabinet department [91]. TSA was stood up in ten weeks flat [92]. The watchlists that came with it grew without brakes: the No Fly List held **16 NAMES ON 9/11** and roughly **47,000 BY 2013**; the consolidated Terrorist Screening Database held 680,000 people, of whom more than 40% were flagged by the government's own documents as having "no recognized terrorist group affiliation" [93]. The upstream TIDE database passed 1 million identities by 2013 and 2.5 million by 2020 [94]. The leaked 166-page Watchlisting Guidance allowed nomination without "concrete facts" or "irrefutable evidence" [95]. A federal judge found the redress process "wholly ineffective" and unconstitutional in 2014 [96].

FUSION CENTERS: THE DOMESTIC INTELLIGENCE NETWORK THAT DOESN'T WORK

DHS built ~77 state and local fusion centers with FEMA grant money. The bipartisan Senate investigation (Coburn/Levin, 2012) found their reporting "oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties... and more often than not unrelated to terrorism," and "could identify no reporting which uncovered a terrorist threat, nor... a contribution such fusion center reporting made to disrupt an active terrorist plot" [97]. DHS could not say whether it had spent $289 million or $1.4 billion on them [97][98]. Documented outputs included intelligence reports on a Muslim parenting lecture and a motorcycle club's know-your-rights leaflets [97]. What fusion centers demonstrably did do is monitor domestic dissent: Occupy Wall Street, Black Lives Matter, Standing Rock [99].

THE FBI UNBOUND

Beyond the NSL explosion (§1), the Attorney General's own guidelines were serially loosened — Ashcroft's 2002 revision let agents attend mosques and meetings without evidence of a crime, and Mukasey's 2008 guidelines created "assessments" permitting physical surveillance, database searches, and informant tasking with *no factual predicate at all* [102]. Joint Terrorism Task Forces tripled to 100+, embedding local police in federal intelligence work [103]. The CIA seconded officer Lawrence Sanchez to the NYPD, where he built the Demographics Unit that mapped Muslim

neighborhoods across New York and New Jersey; in a 2012 deposition, the chief of the NYPD Intelligence Division admitted the unit had never generated a single lead in six years [100][104].

THE REST OF THE ICEBERG

- **LOCAL POLICE** got $35+ billion in DHS grants over the first decade — cameras, license-plate readers, drones — with no system for measuring whether any of it improved security [105], alongside $7.4 billion in military equipment via the 1033 program [106].
- **THE CIA** ran its own bulk collection sweeping in Americans' data under Executive Order 12333 — "entirely outside the statutory framework that Congress and the public believe govern this collection," as Senators Wyden and Heinrich put it when the program was declassified in 2022 [107][108].
- **NCTC** in 2012 quietly got authority to copy entire federal databases and hold data on innocent Americans for **FIVE YEARS**, up from 180 days [109].
- **BIOMETRICS** scaled from US-VISIT fingerprinting to the FBI's ~$1.2 billion Next Generation Identification system — the world's largest biometric database, mixing criminal and civil records [110] — while the REAL ID Act (2005) standardized state licenses into de facto national ID infrastructure [111].

---

6. THE PROGRAMS NOBODY TALKS ABOUT

These are the mechanisms engineered specifically to stay invisible — the strongest evidence that the surveillance state understands its own legal vulnerability.

HEMISPHERE: THE DATABASE BIGGER THAN THE NSA'S

Since at least 2007, the White House drug-policy office has paid AT&T to embed employees with DEA and local police units, giving them query access to AT&T's own switch data: call records going back to **1987**, roughly four billion records added daily — trillions of records, dwarfing the NSA's 215 database, which held only five years [112]. The leaked training deck instructs users to conceal the program's existence: results must be "walled off" and re-attributed to a routine "AT&T subpoena," and "all requestors are instructed to never refer to Hemisphere in any official document" [113]. Funding flows as federal grants to local agencies rather than a federal contract — which kept it out of federal contracting disclosure and privacy review [112]. Exposed by the NYT in 2013, it was

suspended, renamed **DATA ANALYTICAL SERVICES**, and resumed. Senator Wyden's November 2023 letter confirmed it still operates, warrantless in most uses, with "chain analysis" reaching people two hops from any suspect [114][115].

PARALLEL CONSTRUCTION: LAUNDERING THE EVIDENCE TRAIL

Reuters revealed in 2013 that the DEA's Special Operations Division — partnered with NSA, CIA, FBI, and IRS — funnels intelligence tips to field agents who are *trained to "recreate" the investigative trail* to conceal the tip's origin from defense lawyers, prosecutors, and judges, e.g., by staging a pretextual traffic stop [116]. An IRS manual carried the same instructions [116]. Human Rights Watch's 2018 report concluded the practice is likely "frequent" and systematically hides potential constitutional violations from courts. Internally the SOD was nicknamed "the dark side"; departing agents got Darth Vader keychains [117].

THE BLUEPRINT PREDATES 9/11 — AND THE MODEL GOT EXPORTED TO IT

The DEA ran a bulk phone-records program (USTO) from **1992** to 2013, logging virtually every call from the U.S. to up to 116 countries via administrative subpoenas — no court at all. DOJ lawyers cited it as precedent when blessing the NSA's program. It was shut down in September 2013 only because Snowden's disclosures made exposure likely [121]. The DOJ Inspector General later found the DEA had never conducted a comprehensive legal analysis of any of its bulk programs — and had used parallel construction to shield them [122]. 9/11 didn't invent the dragnet; it nationalized it.

STINGRAYS AND ENFORCED SECRECY

Cell-site simulators — fake cell towers that force every phone in an area to connect — were sold to 75+ agencies under FBI non-disclosure agreements that instructed prosecutors to *drop cases rather than disclose the device* and to call the FBI if judges asked questions [118][119]. Baltimore police alone admitted ~4,300 uses [119]. The 2015 DOJ warrant policy is internal guidance only, with a national-security exemption, and doesn't bind local police [120].

YOUR MAIL, YOUR SEARCHES, YOUR LOCATION

- **USPS** photographs the exterior of every piece of mail — ~160 billion a year — under the post-anthrax Mail Isolation Control and Tracking program; its inspector general found ~20% of mail covers approved without adequate justification [123][124]. Its Internet Covert

Operations Program monitored protest organizers on social media until an IG review found it had exceeded the Postal Service's legal authority [125].

- **GEOFENCE WARRANTS** to Google grew from 982 (2018) to 11,554 (2020) — a quarter of all legal demands Google received — until Google re-architected location storage in 2023 to kill its own ability to answer them [126]. Reverse *keyword* warrants (everyone who searched a term) reached a state supreme court in 2023 [127].
- **SECTION 702 "BACKDOOR SEARCHES"**: the FBI ran up to **3.4 MILLION** warrantless U.S.-person queries of 702 data in 2021 [128]. A declassified FISA Court opinion found 278,000+ improper queries, including searches on January 6 suspects, George Floyd protest arrestees, and 19,000 donors to a congressional campaign — violations the court called "persistent and widespread" [129]. FISC rebukes had already forced NSA to abandon "about" collection — interception of communications merely *mentioning* a target — in 2017 [130], and a federal court finally held in 2025 that backdoor searches require a warrant [131].
- **EXECUTIVE ORDER 12333** remains the deepest loophole — overseas collection with no court and no meaningful congressional oversight, sweeping in Americans' data wherever it is routed or stored abroad. Whistleblower John Napier Tye: Americans "should be even more concerned" about 12333 than about Section 215 [132]. Under it, MYSTIC/SOMALGET recorded the *full audio* of virtually every cell call in the Bahamas — access obtained through a DEA "lawful intercept" backdoor [133].
- **THE POST-*CARPENTER* END-RUN**: after the Supreme Court held in 2018 that cell-location history requires a warrant, agencies simply bought equivalent data from brokers — ICE and CBP from Venntel, the Secret Service via Babel Street's Locate X, dozens of local departments from Fog Data Science — on the theory that purchased data needs no warrant [137][138]. The FTC began banning these location-broker practices only in 2024 [139].
- **WATCHING THE WATCHERS' CRITICS**: DHS kept a secret database of journalists, an attorney, and activists tied to the 2018–19 migrant caravan, flagging them for secondary inspection [134]; the FBI contracted Dataminr and later ZeroFox for social-media monitoring that swept in BLM organizers [135]; warrantless border device searches grew from 8,503 (FY2015) to over 55,000 (FY2025) [136].

---

7. THE RATCHET: WHAT 9/11 ACTUALLY BUILT

Setting the six threads side by side, the mechanics of the post-9/11 surveillance state reduce to five repeating moves:

1. EMERGENCY BECOMES PERMANENT. Sixteen PATRIOT provisions got sunsets; fourteen became permanent at the first renewal. Section 702 — "temporary" in 2008 — is on its third renewal, each one broader or more entrenched than the last. In twenty-five years, exactly one authority was deliberately narrowed (bulk 215 collection, in 2015) — and only after a global scandal, a hostile appellate ruling, and an oversight board finding the program had never mattered. Its replacement failed and the underlying authority lapsed in 2020 through congressional gridlock, not choice — the ratchet's single slip, and an accidental one [12][16][22].

2. PUBLIC DEATH, CLASSIFIED RESURRECTION. TIA is the clean experiment: the one time the public voted on total information awareness, the program was killed by name — and continued at Fort Meade under new codenames, with the same contractors, authorized by a classified annex in the very law that "terminated" it [34][35]. Stellar Wind ran the same play in reverse: born secret, then laundered piece by piece into statute (215, pen-register, 702) once exposure loomed [43]. The lesson institutionalized: names are mortal; capabilities are not.

3. SECRECY ENGINEERED AGAINST THE COURTS. The FISA Court operated for years on government representations that were, in its own judge's words, substantially misrepresentative — three times in three years [63]. Below the federal level, the machinery was purpose-built to avoid adjudication entirely: Hemisphere's "never refer to Hemisphere in any official document" rule [113], the DEA's parallel-construction training [116], FBI stingray NDAs instructing prosecutors to drop cases rather than disclose the device [119], and state-secrets dismissals of every civil challenge that got close (*Hepting*, *Jewel*) [52][53]. A surveillance regime that systematically prevents courts from ruling on it is not merely under-overseen — it is designed to be unadjudicable.

4. THE PRIVATE SECTOR AS CONSTITUTIONAL WORKAROUND. The government seeded (In-Q-Tel), enriched (contracts to Booz Allen, SAIC, Palantir), and deputized (AT&T's FAIRVIEW "partnership") an industry that now performs collection the state could not lawfully perform itself — culminating in the post-*Carpenter* practice of simply *buying* the location data a warrant would otherwise be required for [70][80][137]. Seventy percent of the intelligence budget flows through this industry, and its alumni run the agencies that fund it [79][78]. Eisenhower's warning got an upgrade: the military-industrial complex built weapons pointed outward; this one builds sensors pointed inward.

5. TERRORISM AS THE ENTRY, EVERYTHING ELSE AS THE USE. Every authority justified by counterterrorism migrated to ordinary enforcement: sneak-and-peek warrants (0.5% terrorism, ~75% drugs) [8], Hemisphere (drug cases) [112], fusion centers (Occupy, BLM, a Muslim parenting lecture) [97][99], 702 queries (January 6 defendants, George Floyd protesters, campaign donors) [129], stingrays and geofence warrants (routine local crime) [119][126]. The pattern is old — the DEA's 1992 dragnet was the NSA program's actual blueprint [121] — but 9/11 supplied the political permission to scale it to the whole population.

THE SCOREBOARD, TWENTY-FIVE YEARS ON

What did the machine catch? Its own overseers' answers are on the record: the bulk metadata program made "no concrete difference in the outcome of a counterterrorism investigation" [61]; fusion centers "could identify no reporting which uncovered a terrorist threat" [97]; the NYPD Demographics Unit generated zero leads in six years [104]; Trailblazer produced nothing for its billion dollars [49]. The programs that survive today — Hemisphere/DAS, 702 backdoor searches, EO 12333 collection, data-broker purchases, Flock's 90,000 cameras — survive not because they demonstrably stop terrorism but because the ratchet has no reverse gear: each element now has a constituency, a budget line, a contractor, and a classification stamp.

Feingold's floor warning in October 2001 — that the war would be lost "without firing a shot if we sacrifice the liberties of the American people" [4] — and Poindexter's DARPAtech promise that terrorists "will leave signatures in this information space" [26] turn out to be the two poles of the whole story. Poindexter's vision was built. Feingold's price was paid. The attacks took one morning; the architecture they justified is now old enough to have a generation of Americans who have never lived outside it.

LIMITATIONS & CAVEATS

- **CONTESTED CLAIMS ARE FLAGGED IN PLACE.** The Comverse/Amdocs espionage allegations (§4) were never prosecuted and remain unproven; Able Danger's claimed pre-9/11 identification of Mohamed Atta was not corroborated by the DoD IG. Neither is load-bearing for this report's thesis.
- **VOTE COUNTS** for the 2011 PATRIOT extension (Senate 72–23) and the 2008 FISA Amendments Act House vote (293–129) are single-sourced from contemporaneous reporting [MOD].

- The oft-cited claim that the 2011 Bates FISC opinion found "79%" over-collection could not be verified against the opinion; this report uses the opinion's actual figures (≈250M communications/year, tens of thousands wholly domestic) [63]. Similarly, by 2013 the 215 program likely covered well under all U.S. call records due to cellphone gaps — "virtually all" describes the program's orders, not necessarily its coverage.
- Several classified programs (PCLOB "Deep Dive I," the actual scope of RISAA's expanded provider definition) remain unknowable from public sources; where the report describes them, it describes only what has been declassified or credibly leaked.

REFERENCES

1. U.S. Senate Roll Call Vote #313, 107th Congress — USA PATRIOT Act (Oct. 25, 2001). United States Senate. https://www.senate.gov/legislative/LIS/roll_call_votes/vote1071/vote_107_1_00313.htm
2. "Congress Had No Time to Read the USA PATRIOT Act." Sunlight Foundation, Mar. 2, 2009. https://sunlightfoundation.com/2009/03/02/congress-had-no-time-to-read-the-usa-patriot-act/
3. "USA PATRIOT Act." Electronic Privacy Information Center (EPIC). https://epic.org/issues/surveillance-oversight/patriot-act/
4. Sen. Russ Feingold, Senate floor statement on the USA PATRIOT Act, Oct. 25, 2001. EPIC archive. https://archive.epic.org/privacy/terrorism/usapatriot/feingold.html
5. CRS Report R40138 (PATRIOT Act/FISA sunset provisions). Congressional Research Service. https://www.congress.gov/crs-product/R40138
6. "Section 206: Roving Surveillance Authority." ABA Patriot Debates, American Bar Association. http://apps.americanbar.org/natsecurity/patriotdebates/section-206
7. CRS Report LSB10652, "The USA PATRIOT Act at 20: Sneak and Peek Searches." Congressional Research Service. https://www.congress.gov/crs_external_products/LSB/PDF/LSB10652/LSB10652.3.pdf
8. "Peekaboo, I See You: Government Authority Intended for Terrorism Is Used for Other Purposes." Electronic Frontier Foundation, Oct. 2014. https://www.eff.org/deeplinks/2014/10/peekaboo-i-see-you-government-uses-authority-meant-terrorism-other-uses
9. CRS Report RL33320, "National Security Letters in Foreign Intelligence Investigations." Congressional Research Service. https://www.congress.gov/crs-product/RL33320

10. DOJ Office of the Inspector General, "A Review of the FBI's Use of National Security Letters," Mar. 2007. https://oig.justice.gov/sites/default/files/legacy/special/s0703b/final.pdf
11. Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004). Civil Rights Litigation Clearinghouse. https://clearinghouse.net/case/12966/
12. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177. GovInfo. https://www.govinfo.gov/content/pkg/PLAW-109publ177/pdf/PLAW-109publ177.pdf
13. "Obama Wields His Autopen." NPR, May 27, 2011. https://www.npr.org/2011/05/27/136717719/obama-wields-his-autopen
14. "Senate Clears USA Freedom Act After Ending Rand Paul Filibuster." Roll Call, June 2, 2015. https://rollcall.com/2015/06/02/senate-clears-usa-freedom-act-after-ending-rand-paul-filibuster-updated/
15. PCLOB, "Report on the Government's Use of the Call Detail Records Program Under the USA FREEDOM Act," 2020. https://documents.pclob.gov/prod/Documents/OversightReport/87c7e900-6162-4274-8f3a-d15e3ab9c2e4/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf
16. "Yes, Section 215 Expired. Now What?" Electronic Frontier Foundation, Apr. 2020. https://www.eff.org/deeplinks/2020/04/yes-section-215-expired-now-what
17. FISA Amendments Act of 2008, Pub. L. 110-261. GovInfo. https://www.govinfo.gov/content/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf
18. "Senate Passes Unconstitutional Spying Bill and Grants Sweeping Immunity to Phone Companies." ACLU, July 9, 2008. https://www.aclu.org/press-releases/senate-passes-unconstitutional-spying-bill-and-grants-sweeping-immunity-phone
19. FISA Amendments Act Reauthorization Act of 2012, Pub. L. 112-238. GovInfo. https://www.govinfo.gov/content/pkg/PLAW-112publ238/pdf/PLAW-112publ238.pdf
20. FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118. GovInfo. https://www.govinfo.gov/content/pkg/PLAW-115publ118/pdf/PLAW-115publ118.pdf
21. "House Approves Surveillance Authority Reauthorization Bill." Roll Call, Apr. 12, 2024. https://rollcall.com/2024/04/12/house-approves-surveillance-authority-reauthorization-bill/
22. CRS Report R48592, "FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act." Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R48592/R48592.1.pdf
23. CRS Report RL31786, "Total Information Awareness Programs: Funding, Composition, and Oversight Issues," Mar. 2003. https://www.everycrsreport.com/reports/RL31786.html

24. Lawrence Walsh, Final Report of the Independent Counsel for Iran/Contra Matters, Ch. 3 (John Poindexter). Federation of American Scientists. https://irp.fas.org/offdocs/walsh/chap_03.htm
25. "Lightning Rod." Government Executive, July 2004. https://www.govexec.com/magazine/features/2004/07/lightning-rod/17199/
26. John Poindexter, "Overview of the Information Awareness Office," DARPAtech speech, Aug. 2, 2002. Federation of American Scientists. https://irp.fas.org/agency/dod/poindexter.html
27. DARPA, "Report to Congress Regarding the Terrorism Information Awareness Program," May 20, 2003. EPIC archive. https://archive.epic.org/privacy/profiling/tia/may03_report.pdf
28. William Safire, "You Are a Suspect." The New York Times, Nov. 14, 2002. https://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html
29. "Total 'Terrorism' Information Awareness (TIA)" archive. Electronic Privacy Information Center. https://archive.epic.org/privacy/profiling/tia/
30. Consolidated Appropriations Resolution 2003, Pub. L. 108-7 (Wyden amendment restricting TIA). EPIC archive. https://archive.epic.org/privacy/profiling/tia/pub_law_108-7.html
31. "EFF Review of May 20 Report to Congress on Total Information Awareness." Electronic Frontier Foundation, May 2003. https://www.eff.org/deeplinks/2003/05/eff-review-may-20-report-total-informatin-awareness
32. "Pentagon Kills 'Terror Futures Market.'" NBC News, July 29, 2003. https://www.nbcnews.com/id/wbna3072985
33. "Poindexter Resigns." CNN, July 31, 2003. https://www.cnn.com/2003/ALLPOLITICS/07/31/poindexter.resigns/
34. Section 8131, Department of Defense Appropriations Act 2004, Pub. L. 108-87 (TIA termination and classified annex). Federation of American Scientists. https://sgp.fas.org/congress/2003/tia.html
35. Shane Harris, "TIA Lives On." National Journal, Feb. 23, 2006 (full-text reprint). https://911truth.org/total-information-awareness-lives-on/
36. "The Total Information Awareness Project Lives On." MIT Technology Review, Apr. 26, 2006. https://www.technologyreview.com/2006/04/26/229286/the-total-information-awareness-project-lives-on/
37. "History." IARPA. https://www.iarpa.gov/who-we-are/history

38. "15 Years Ago, the Military Tried to Record Whole Human Lives. It Ended Badly." Vice. https://www.vice.com/en/article/15-years-ago-the-military-tried-to-record-whole-human-lives-it-ended-badly/
39. "ACLU Unveils Disturbing New Revelations About the MATRIX Surveillance Program." ACLU. https://www.aclu.org/press-releases/aclu-unveils-disturbing-new-revelations-about-matrix-surveillance-program
40. GAO-04-548, "Data Mining: Federal Efforts Cover a Wide Range of Uses." Government Accountability Office, May 2004. https://www.gao.gov/assets/gao-04-548.pdf
41. "DHS Discontinues Anti-Terror Data-Mining Project (ADVISE)." NPR, Sept. 5, 2007. https://www.npr.org/2007/09/05/14181932/dhs-discontinues-anti-terror-data-mining-project
42. Technology and Privacy Advisory Committee, "Safeguarding Privacy in the Fight Against Terrorism," Mar. 2004. EPIC archive. https://archive.epic.org/privacy/profiling/tia/tapac_report.pdf
43. Unclassified Joint Report of the Inspectors General on the President's Surveillance Program, July 10, 2009. Federation of American Scientists. https://irp.fas.org/eprint/psp.pdf
44. NSA Office of the Inspector General, Draft Working Report ST-09-0002 on STELLARWIND, Mar. 24, 2009 (Snowden leak). ACLU. https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf
45. "Gonzales Hospital Episode Detailed" (James Comey testimony). The Washington Post, May 15, 2007. https://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500864.html
46. James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," The New York Times, Dec. 16, 2005 (2006 Pulitzer Prize, National Reporting). https://www.pulitzer.org/winners/james-risen-and-eric-lichtblau
47. Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," USA Today, May 11, 2006 (via NPR). https://www.npr.org/2006/05/11/5398629/report-nsa-collecting-domestic-phone-records
48. "System Error." The Baltimore Sun, Jan. 29, 2006. https://www.baltimoresun.com/2006/01/29/system-error/
49. DoD Inspector General, "Requirements for the TRAILBLAZER and THINTHREAD Systems," Report 05-INTEL-03, Dec. 15, 2004. Federation of American Scientists. https://irp.fas.org/agency/dod/ig-thinthread.pdf

50. "Justice Department Agrees to Plea Deal in Drake Case." NPR, June 10, 2011. https://www.npr.org/2011/06/10/137112903/justice-department-agrees-to-plea-in-drake-case
51. Mark Klein, unredacted declaration with exhibits, Hepting v. AT&T, 2006. Electronic Frontier Foundation. https://www.eff.org/files/filenode/att/mark_klein_unredacted_decl-including_exhibits.pdf
52. "Hepting v. AT&T" case page. Electronic Frontier Foundation. https://www.eff.org/cases/hepting
53. "Jewel v. NSA" case page. Electronic Frontier Foundation. https://www.eff.org/cases/jewel
54. FISC Secondary Order to Verizon Business Network Services, Docket BR 13-80, Apr. 25, 2013. EPIC. https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf
55. "NSA Slides Explain the PRISM Data-Collection Program." The Washington Post, June 6, 2013. https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/
56. Boundless Informant slides (The Guardian, June 8, 2013). Internet Archive. https://archive.org/details/NSA-Boundless-Informant-Slides
57. "NSA Project XKeyscore Collects Nearly Everything You Do on the Internet." TechCrunch (on The Guardian's July 31, 2013 disclosure). https://techcrunch.com/2013/07/31/nsa-project-x-keyscore-collects-nearly-everything-you-do-on-the-internet/
58. Barton Gellman & Ashkan Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say." The Washington Post, Oct. 30, 2013. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
59. Barton Gellman & Ashkan Soltani, "NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show." The Washington Post, Dec. 4, 2013. https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
60. "NSA Collected Nearly 200 Million Text Messages Daily" (Dishfire). NBC News, Jan. 16, 2014. https://www.nbcnews.com/news/world/nsa-collected-nearly-200-million-text-messages-daily-report-flna2d11944640
61. PCLOB, "Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act," Jan. 23, 2014. https://documents.pclob.gov/prod/Documents/

OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf

62. PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of FISA," July 2, 2014. https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf
63. FISC, Memorandum Opinion of Judge John Bates on NSA upstream collection, Oct. 3, 2011 (declassified Aug. 2013). ODNI. https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf
64. Klayman v. Obama, Memorandum Opinion of Judge Richard Leon, D.D.C., Dec. 16, 2013. CourtListener. https://www.courtlistener.com/opinion/2659672/klayman-v-obama/
65. ACLU v. Clapper, No. 14-42 (2d Cir. May 7, 2015). ACLU. https://www.aclu.org/wp-content/uploads/legal-documents/clapper-ca2-opinion.pdf
66. United States v. Moalin, 973 F.3d 977 (9th Cir. Sept. 2, 2020). https://cdn.ca9.uscourts.gov/datastore/opinions/2020/09/02/13-50572.pdf
67. Barton Gellman & Greg Miller, "'Black Budget' Summary Details U.S. Spy Network's Successes, Failures and Objectives." The Washington Post, Aug. 29, 2013. https://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html
68. "NSA Boss's Mantra: Collect It All." Techdirt (summarizing Washington Post profile of Gen. Keith Alexander), July 15, 2013. https://www.techdirt.com/2013/07/15/nsa-bosses-mantra-who-cares-what-law-says-collect-it-all/
69. James Bamford, "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)." Wired, Mar. 2012. https://www.wired.com/2012/03/ff_nsadatacenter/
70. Andy Greenberg, "How a 'Deviant' Philosopher Built Palantir, a CIA-Funded Data-Mining Juggernaut." Forbes, Aug. 14, 2013. https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/
71. Peter Waldman, Lizette Chapman & Jordan Robertson, "Palantir Knows Everything About You." Bloomberg Businessweek, Apr. 2018. https://www.bloomberg.com/features/2018-palantir-peter-thiel/
72. Ali Winston, "Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology." Type Investigations/The Verge, Feb. 27, 2018. https://typeinvestigations.org/investigation/2018/02/27/palantir-secretly-use-new-orleans-test-predictive-policing/

73. "Palantir's Growing Role in Trump Deportations." Axios Denver, May 1, 2025. https://www.axios.com/local/denver/2025/05/01/palantir-deportations-ice-immigration-trump
74. "The Genesis of Google Earth." Trajectory Magazine (USGIF). https://medium.com/trajectory-magazine/the-genesis-of-google-earth-7357204ecfb5
75. Lee Fang, "The CIA Is Investing in Firms That Mine Your Tweets and Instagram Photos." The Intercept, Apr. 14, 2016. https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/
76. "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color." ACLU of Northern California, Oct. 2016. https://www.aclu.org/news/privacy-technology/facebook-instagram-and-twitter-provided-data-access
77. Nathan Vardi, "The Carlyle Group Has Made $2 Billion Off of Booz Allen." Forbes, June 10, 2013. https://www.forbes.com/sites/nathanvardi/2013/06/10/the-carlyle-group-has-made-2-billion-off-of-booz-allen/
78. Pratap Chatterjee, "How Booz Allen Made the Revolving Door Redundant." Antiwar.com, June 17, 2013. https://original.antiwar.com/pratap-chatterjee/2013/06/17/how-booz-allen-made-the-revolving-door-redundant/
79. Tim Shorrock, "The Corporate Takeover of U.S. Intelligence." Salon, June 1, 2007. (See also Shorrock, *Spies for Hire*, Simon & Schuster, 2008.) https://www.salon.com/2007/06/01/intel_contractors/
80. Julia Angwin, Charlie Savage, Jeff Larson, et al., "NSA Spying Relies on AT&T's 'Extreme Willingness to Help.'" ProPublica/The New York Times, Aug. 15, 2015. https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help
81. "Qwest CEO: NSA Punished Qwest for Refusing to Participate in Illegal Surveillance — Pre-9/11." EFF, Oct. 2007; United States v. Nacchio, 555 F.3d 1234 (10th Cir. en banc 2009). https://www.eff.org/deeplinks/2007/10/qwest-ceo-nsa-punished-qwest-refusing-participate-illegal-surveillance-pre-9-11
82. CRS Report RL34600, "Retroactive Immunity Provided by the FISA Amendments Act of 2008." Congressional Research Service. https://www.everycrsreport.com/reports/RL34600.html
83. Dana Priest & William Arkin, "Top Secret America: A Hidden World, Growing Beyond Control." The Washington Post, July 19, 2010. https://www.washingtonpost.com/investigations/top-secret-america/2010/07/19/hidden-world-growing-beyond-control-2/

84. "Amazon Win Restarts CIA Cloud Contract." Washington Technology, Oct. 2013. https://www.washingtontechnology.com/2013/10/amazon-win-restarts-cia-cloud-contract/338279/

85. "Anduril Industries" (founding, CBP Lattice towers, valuation). Wikipedia/TechCrunch reporting. https://en.wikipedia.org/wiki/Anduril_Industries

86. "Clearview AI Scraped 30 Billion Images from Facebook and Gave Them to Police." The Register, Mar. 28, 2023. https://www.theregister.com/2023/03/28/us_police_clearview/

87. "The Fight Against Flock's Surveillance Cameras." The Nation; Campaign Zero, "The Private Companies Quietly Building a Police State." https://www.thenation.com/article/activism/flock-camera-surveillance-activism/

88. "Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police." Electronic Frontier Foundation, Aug. 2022. https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police

89. ODNI Senior Advisory Group, Declassified Report on Commercially Available Information, Jan. 2022. https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

90. "The FBI Tested NSO Group's Pegasus." The Washington Post, Feb. 2, 2022 (on NYT reporting); House Judiciary Committee letter re: "Phantom," Mar. 3, 2022. https://www.washingtonpost.com/technology/2022/02/02/pegasus-fbi-nso-test/

91. Homeland Security Act of 2002, Pub. L. 107-296. GovInfo. https://www.govinfo.gov/content/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf

92. TSA, "20 Years After 9/11: The State of the Transportation Security Administration," testimony, Sept. 29, 2021. https://www.tsa.gov/news/press/testimony/2021/09/29/20-years-after-911-state-transportation-security-administration-0

93. Jeremy Scahill & Ryan Devereaux, "Barack Obama's Secret Terrorist-Tracking System, by the Numbers." The Intercept, Aug. 5, 2014. https://theintercept.com/2014/08/05/watch-commander/

94. ODNI/NCTC, TIDE Fact Sheet. https://www.dni.gov/files/Tide_Fact_Sheet.pdf

95. Jeremy Scahill & Ryan Devereaux, "Blacklisted: The Secret Government Rulebook for Labeling You a Terrorist." The Intercept, July 23, 2014. https://theintercept.com/2014/07/23/blacklisted/

96. Latif v. Holder, Opinion of Judge Anna Brown (D. Or. June 24, 2014). ACLU. https://www.aclu.org/sites/default/files/assets/no_fly_list_ruling__-*latif_v._holder*-_6-24-14.pdf

97. Senate Permanent Subcommittee on Investigations, "Federal Support for and Involvement in State and Local Fusion Centers," Oct. 3, 2012. https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf
98. "New Senate Report Confirms Government 'Counterterrorism' Centers Don't Stop Terrorism." Electronic Frontier Foundation, Oct. 2012. https://www.eff.org/deeplinks/2012/10/new-senate-report-confirms-government-counterterrorism-centers-dont-stop
99. "Where's the Suspicion? The Government's Suspicious Activity Reports." ACLU. https://www.aclu.org/news/national-security/wheres-suspicion-governments-suspicious-activity
100. "NYPD: Muslim Spying Led to No Leads, Terror Cases." CNN, Aug. 21, 2012. https://www.cnn.com/2012/08/21/justice/new-york-nypd-surveillance-no-leads
101. DOJ Office of the Inspector General, "A Review of the FBI's Use of Exigent Letters and Other Informal Requests for Telephone Records," Jan. 2010. https://oig.justice.gov/sites/default/files/legacy/special/s1001r.pdf
102. "Fact Sheet: New Attorney General Guidelines" (Mukasey 2008 'assessments'). ACLU. https://www.aclu.org/documents/fact-sheet-new-attorney-general-guidelines
103. "Celebrating 45 Years of FBI Joint Terrorism Task Forces." FBI. https://www.fbi.gov/news/stories/celebrating-45-years-of-fbi-joint-terrorism-task-forces
104. Declaration of NYPD Assistant Chief Thomas Galati, Handschu litigation, June 28, 2012; AP NYPD surveillance series (2012 Pulitzer Prize). https://www.nyc.gov/assets/nypd/downloads/pdf/legal/declaration_of_thomas_galati_with_exhibit_a.pdf
105. Sen. Tom Coburn, "Safety at Any Price: Assessing the Impact of Homeland Security Spending in U.S. Cities," Dec. 2012. https://info.publicintelligence.net/SenatorCoburn-UASI.pdf
106. "War Comes Home: The Excessive Militarization of American Policing." ACLU, 2014. https://www.aclu.org/news/criminal-law-reform/federal-militarization-of-law-enforcement-must-end
107. Sens. Ron Wyden & Martin Heinrich, letter to DNI Haines and CIA Director Burns on CIA bulk collection, Apr. 13, 2021 (declassified Feb. 10, 2022). https://www.heinrich.senate.gov/newsroom/press-releases/heinrich-and-wyden-newly-declassified-documents-reveal-previously-secret-cia-bulk-collection-problems-with-cia-handling-of-americans-information-
108. PCLOB, Report on CIA Financial Data Activities ("Deep Dive II," redacted), Mar. 2022. https://documents.pclob.gov/prod/Documents/OversightReport/

f01950e2-75ff-4fb4-9b2e-9e7d6937ae3a/PCLOB%20Report%20on%20CIA%20Activities%20-%20508,%20Mar%2022,%202022%201305.pdf

109. "The National Counterterrorism Center's Massive New Surveillance Program" (on Julia Angwin, WSJ, Dec. 2012). Slate; NCTC 2012 Guidelines. https://slate.com/technology/2012/12/national-counterterrorism-center-s-massive-new-surveillance-program-uncovered-by-wall-street-journal.html
110. "FBI's Next Generation Identification Biometrics Database." Electronic Frontier Foundation. https://www.eff.org/cases/fbis-next-generation-identification-biometrics-database
111. REAL ID Act of 2005 (H.R. 418, 109th Congress). Congress.gov. https://www.congress.gov/bill/109th-congress/house-bill/418
112. Scott Shane & Colin Moynihan, "Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s." The New York Times, Sept. 1, 2013. https://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html
113. "Los Angeles Hemisphere" training slide deck (Law Enforcement Sensitive). DocumentCloud/NYT. https://www.documentcloud.org/documents/782287-database/
114. Sen. Ron Wyden, letter to Attorney General Garland on Hemisphere/Data Analytical Services, Nov. 20, 2023. https://www.wyden.senate.gov/imo/media/doc/wyden_hemisphere_surveillance_letter_112023.pdf
115. Dell Cameron & Dhruv Mehrotra, "Secretive White House Surveillance Program Gives Cops Access to Trillions of US Phone Records." Wired, Nov. 20, 2023. https://www.wired.com/story/hemisphere-das-white-house-surveillance-trillions-us-call-records/
116. John Shiffman & Kristina Cooke, "Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans." Reuters, Aug. 5, 2013. https://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805
117. "Dark Side: Secret Origins of Evidence in US Criminal Cases." Human Rights Watch, Jan. 9, 2018. https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases
118. "Cell-Site Simulators / IMSI Catchers." EFF Street-Level Surveillance. https://www.eff.org/pages/cell-site-simulatorsimsi-catchers
119. "Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases." The Baltimore Sun, Apr. 9, 2015. https://www.baltimoresun.com/2015/04/09/baltimore-police-used-secret-technology-to-track-cellphones-in-thousands-of-cases/

120. "Finally! DOJ Reverses Course and Will Get Warrants for Stingrays." Electronic Frontier Foundation, Sept. 2015. https://www.eff.org/deeplinks/2015/09/finally-doj-reverses-course-and-will-get-warrants-stingrays

121. Brad Heath, "U.S. Secretly Tracked Billions of Calls for Decades." USA Today, Apr. 7, 2015. https://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

122. DOJ Office of the Inspector General, "Review of the DEA's Use of Administrative Subpoenas to Collect or Exploit Bulk Data," Mar. 2019. https://oig.justice.gov/reports/review-drug-enforcement-administrations-use-administrative-subpoenas-collect-or-exploit

123. Ron Nixon, "U.S. Postal Service Logging All Mail for Law Enforcement." The New York Times, July 3, 2013 (via IRE). https://www.ire.org/2013/07/08/u-s-postal-service-logging-all-mail-for-law-enforcement/

124. USPS Office of Inspector General, "Postal Inspection Service Mail Covers Program," Audit HR-AR-14-001, May 2014. https://www.uspsoig.gov/sites/default/files/reports/2023-01/HR-AR-14-001.pdf

125. Jana Winter, "The Postal Service Is Running a Covert Operations Program That Monitors Americans' Social Media Posts." Yahoo News, Apr. 21, 2021. https://www.yahoo.com/news/the-postal-service-is-running-a-running-a-covert-operations-program-that-monitors-americans-social-media-posts-160022919.html

126. Google, "Supplemental Information on Geofence Warrants in the United States." https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf

127. "Colorado Court Upholds Google Keyword Search Warrant" (People v. Seymour). Colorado Public Radio, Oct. 16, 2023. https://www.cpr.org/2023/10/16/colorado-court-upholds-google-keyword-search-warrant-which-led-to-arrests-in-fatal-arson/

128. ODNI, Annual Statistical Transparency Report Regarding National Security Authorities, CY2021 (Apr. 2022). https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2021.pdf

129. FISC Memorandum Opinion and Order, Apr. 21, 2022 (unsealed May 19, 2023) on FBI Section 702 U.S.-person queries. ODNI/intelligence.gov. https://www.intelligence.gov/assets/documents/702-documents/declassified/21/2021_FISC_Certification_Opinion.pdf

130. "NSA Backs Down on Major Surveillance Program That Captured Americans' Communications Without a Warrant" ('about' collection). The Intercept, Apr. 28, 2017.

https://theintercept.com/2017/04/28/nsa-backs-down-on-major-surveillance-program-that-captured-americans-communications-without-a-warrant/

131. "Victory: Federal Court (Finally) Rules Backdoor Searches of 702 Data Unconstitutional." Electronic Frontier Foundation, Jan. 2025. https://www.eff.org/deeplinks/2025/01/victory-federal-court-finally-rules-backdoor-searches-702-data-unconstitutional
132. John Napier Tye, "Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans." The Washington Post, July 18, 2014. https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html
133. Ryan Devereaux, Glenn Greenwald & Laura Poitras, "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas." The Intercept, May 19, 2014. https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/
134. "Leaked Documents Show the U.S. Government Tracking Journalists and Immigration Advocates Through a Secret Database." NBC 7 San Diego, Mar. 2019. https://www.nbcsandiego.com/news/local/source-leaked-documents-show-the-us-government-tracking-journalists-and-advocates-through-a-secret-database/3438/
135. "FBI Hired Social Media Surveillance Firm That Labeled Black Lives Matter Organizers 'Threat Actors.'" The Intercept, July 6, 2023 (see also The Intercept, June 24, 2020, on Dataminr). https://theintercept.com/2023/07/06/fbi-social-media-surveillance-zerofox/
136. "Device Searches Hit Record Numbers at US Border." Freedom of the Press Foundation. https://freedom.press/digisec/blog/device-searches-hit-record-numbers-at-us-border/
137. "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data." ACLU. https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data
138. "Secret Service Bought Access to Americans' Location Data" (Babel Street "Locate X"). Vice/Motherboard, Aug. 2020. https://www.vice.com/en/article/secret-service-phone-location-data-babel-street/
139. "Federal Regulators Limit Location Brokers from Selling Your Whereabouts: 2024 in Review." Electronic Frontier Foundation, Dec. 2024. https://www.eff.org/deeplinks/2024/12/federal-regulators-limit-location-brokers-selling-your-whereabouts-2024-review

APPENDIX: THE DOCUMENT LIBRARY

The `documents/` folder alongside this report contains the primary sources, organized to mirror the report's sections:

FOLDER	CONTENTS
01-PATRIOT-ACT-AND-LAWS	Full statute texts (PATRIOT Act, all reauthorizations, FISA Amendments Act, USA FREEDOM, RISAA), DOJ IG reports on Section 215, PCLOB call-detail-records report, CRS analyses, Feingold's floor statement
02-TOTAL-INFORMATION-AWARENESS	DARPA's May 2003 report to Congress, the TIA System Description Document, Poindexter's DARPAtech speech and resignation letter, the TAPAC report, GAO data-mining surveys, Safire's column, Shane Harris's "TIA Lives On"
03-NSA-PROGRAMS	The joint IG report on the President's Surveillance Program, the leaked NSA IG Stellar Wind history, both PCLOB reports, the Verizon FISC order, the Bates FISC opinions, Mark Klein's declaration, the ThinThread/Trailblazer IG report, ACLU v. Clapper and U.S. v. Moalin opinions
04-SURVEILLANCE-INDUSTRY	ODNI's commercially-available-information report, the Nacchio appellate opinion, Top Secret America, the CSIS data-broker report, ProPublica's AT&T piece, the Forbes Palantir profile, In-Q-Tel reporting
05-INSTITUTIONAL-BUILDOUT	Homeland Security Act, the Senate fusion-center report, all three DOJ IG reports on NSLs and exigent letters, the Wyden–Heinrich CIA letter, PCLOB's CIA "Deep Dive II" report, NCTC 2012 guidelines, the Coburn grant-spending report, Latif v. Holder, the Galati deposition, watchlist documents
06-LESSER-KNOWN-PROGRAMS	The Hemisphere slide deck, Wyden's DAS letter, the HRW parallel-construction report, the USPS mail-covers audit, Google's geofence-warrant data, ODNI transparency reports, the declassified FISC opinion on FBI query abuse, Reuters/USA Today/Intercept investigative pieces

Report compiled September 11, 2026 — twenty-five years to the day. Built from six parallel research passes across government documents, court records, inspector general reports, declassified FISA court opinions, and original investigative reporting.