d

Collection without Coordination:

The Bureaucratic Failures of 9/11 and the American Surveillance Dilemma

Aidan Free

Advanced United States History

Dr. Laura Moore

23 May 2025

As President George W. Bush read a book aloud to Florida elementary school students on September 11th, 2001, the largest loss of life from a foreign attack on American soil occurred. Nearly 3000 people died as a result of the crash of four airplanes; two into the World Trade Center, one into the Pentagon, and one into an open field. The world stood alongside the United States in the grief, mourning, and shock that ensued. When the country caught a glimpse of the president, not hiding in Air Force One, "he seemed unready. He looked like he was the hunted, not the hunter," said his own speechwriter, David Frum.[1] As the Commander-in-Chief and the person responsible for protecting the American people, Bush was tormented by ideas of what he could have done to prevent the attacks. Yet, the immediate and prolonged response to 9/11 overcompensated for the government's shortcomings. The September 11th terrorist plots could have been foiled had the very agencies designed to connect intelligence dots not been handicapped by legal firewalls, risk-averse leadership, and a Cold War mindset that prioritized secrecy over sharing. Riding the wave of nationwide solidarity, Congress passed legislation permitting the expansion of intelligence agencies' surveillance capabilities on U.S. citizens, an emotional overreaction that, while addressing the initial intelligence gap, also reshaped how America wields power, compromises liberty for security, and projects digital influence abroad.[2]

The four terrorist attacks were perpetrated by the radical Islamic group named Al-Qaeda. The militant organization comprised mainly Sunni jihadists, one of the two major factions that battled for control of Afghanistan in the 1990s. Resulting from the collapse of the Soviet Union and the end of the Cold War, power vacuums appeared globally, especially in the former Soviet-controlled Afghanistan.[3] Meanwhile, the United States emerged as the global superpower

---

[1] *America After 9/11*, directed by Michael Kirk (PBS Frontline, 2021), 07:00-9:00.
[2] Ibid., 07:00-9:00.
[3] Ibid., 07:00-9:00.

and victor of the Cold War, further elevated by the swift military success in the Gulf War. As a result, Americans held high confidence in their government's ability to protect them. In the late 90s, people were satisfied with the growing economy and ".com" boom, and the general positive state of the United States at the time.[4] Almost 80% of adults held steadfast optimism for the nation at the turn of the century.[5] In a similar vein, top security officials regarded terrorism as a secondary concern to rogue nations developing weapons of mass destruction. From the time of the Oklahoma City bombing in 1995 until 2025, citizens' worry was at its lowest just before 9/11 in May of 2000, even after the Al-Qaeda-coordinated attacks on the USS Cole and the Kenyan embassy.[6] For many, 9/11 was an inconceivable event. The psychological distance of foreign United States-targeted attacks allowed the American public to be in a state of immense shock following 9/11, even though the acts of terrorism in the 1990s and early 2000s should've served as a harbinger of a threat on American soil.

Further, the government was made aware of the increasing threat of terrorist attacks on US soil, yet chose not to take action. Stemming from the U.S. military occupation of sacred muslim land in Saudi Arabia during the early '90s and other perceived anti-muslim American foreign policy, Osama Bin Laden utilized his pro-Islam organization that tried to protect from Soviet invasion in the Cold War to one that tried to protect his people from American encroachment in the Middle East.[7] However, this mindset justified ever more militant actions, focusing Al Qaeda's efforts on attacks on United States interests. In some ways, Bin Laden filled

---

[4] Ibid., 07:00-9:00.
[5] Pew Research Center, "Optimism Reigns, Technology Plays Key Role," October 24, 1999, https://www.pewresearch.org/politics/1999/10/24/optimism-reigns-technology-plays-key-role/.
[6] Hess, Ryan C.K., "Al-Qaeda's Keys to Success," Journal of Indo-Pacific Affairs, Summer 2021, https://media.defense.gov/2021/Jun/03/2002733839/-1/-1/0/HESS2.PDF/HESS2.PDF.
[7] Ibid.

the Soviet Union's shoes as America's ideological nemesis. Al Qaeda, protected in their home of Afghanistan (at the time), mainly recruited people into training camps from the neighboring geographical region of the Arabian peninsula and North Africa who held or adopted similar radical Islamic values to the leaders in the group. While the important officials coordinated a system of centralized leadership and logistics, Al Qaeda also relied on decentralized cells and networks to carry out attacks.[8] These aspects, along with the elusive nature of the group and physical isolation from the United States, further obscured counter-intelligence efforts. Though tedious, the Central Intelligence Agency (CIA) and Counter Terrorism Center (CTC) gathered significant information on suspected terrorists and their plots, and produced forewarning analyses of Bin Laden's danger.[9] With an increase in terrorism worldwide and government awareness of it, these insightful analyses still did not convince the senior security officials in the U.S. government, who chose to remain stagnant and not disrupt the nation's positive economic and psychological state at the time. For example, the analysis of Bin Laden as an imminent threat was not taken seriously by senior officials who, "beneath the acknowledgment that Bin Ladin and al Qaeda presented serious dangers … [were uncertain] about whether this was just a new and especially venomous version of the ordinary terrorist threat America had lived with for decades, or was radically new, posing a threat beyond any yet experienced."[10] Even after sending warnings to the Taliban of retaliation in 1998, 1999, 2000, and 2001 for Bin Laden's attacks on the Kenyan embassy and the USS Cole, "delivering it repeatedly did not make it more effective."[11] Although officials were very well aware of the imminent danger that Bin Laden

---

[8] Ibid.
[9] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (Washington, DC: Government Printing Office, 2004), 341, https://www.9-11commission.gov/report/911Report.pdf.
[10] Ibid., pp. 119.
[11] Ibid., pp. 350.

posed, they chose not to quell the threat. As one CIA officer wrote to his supervisor in 1997, "All we're doing is holding the ring until the cavalry gets here."[12] The agent's lament captures the cycle of bureaucratic stagnation, where analysts submitted detailed briefings to their superiors, anticipating the green light to take action. On the other hand, policymakers waited for conclusive evidence that no analyst could provide and took no action. Despite having access to the information detailing Bin Laden's danger to America, top security officials remained stagnant and indecisive, choosing not to address the growing threat. In turn, the lack of response from the United States government further encouraged Bin Laden to ambitiously attack without fear of consequences.

The other major shortcoming of the U.S. government that could've prevented 9/11 was the poor communication. Many useful counterterrorism analyses throughout the Intelligence Community provided insight into the methods of carrying out an aviation-mediated terrorist attack, the potential targets, and the suspected perpetrators. For example, an FBI analyst anonymously named "Jane" was assigned to the *USS Cole* case and worked with CIA analyst "Dave".[13] Jane's supervisor provided her with three photographs, including one of a suspected terrorist and eventual hijacker of the plane flown into the Pentagon named Khalid al-Mihdhar, to show to FBI agents who had interviewed someone close to Mihdhar. On June 11, 2001, she met with them in New York with no other information, except from NSA reports she discovered on Intelink (a secure intranet for the Intelligence Community). Some of the information in these reports was restricted from being shared with criminal investigators without the Justice Department's Office of Intelligence Policy and Review, and "Jane" therefore did not share it. However, "this decision was potentially significant, because the signals intelligence she did not

[12] Ibid., pp. 349.
[13] Ibid., pp. 268.

share linked Mihdhar to a suspected terrorist facility in the Middle East."[14] The agents would have established a connection to the facility from their work on the embassy bombings case, which would have led them to investigate Mihdhar further. Not only this, but a second opportunity arose when an FBI criminal agent working on the *Cole* case expressed interest in the lead and contacted "Jane." She responded, claiming that he did not have the jurisdiction to open an intelligence case on Mihdhar.[15] Her misunderstanding, along with that of the others involved, of the rules governing the sharing of information gathered in intelligence channels excluded knowledgeable and experienced criminal agents from the search. The unclear and overly exclusive regulations preventing the dissemination of information between relevant intelligence agencies allowed terrorists like Khalid al-Mihdhar to bypass the U.S. government's supervision. The 9/11 attacks were successful not because of a lack of counterterrorist intelligence, but due to a lack of interagency communication in the Intelligence Community. That is to say, surveillance was not the issue; communication was. And yet, the government still chose to expand the Intelligence Community's oversight to one without limits, even on American citizens. Instead of taking accountability for their indecisiveness, disregard of the harbingers, and failing bureaucratic systems, policymakers deflected the blame on a lack of information.

In turn, the government expanded its surveillance programs to remedy the tragedy of 9/11, despite it not being the problem, and instead infringing on citizens' civil liberties. During the Cold War, the National Security Agency (NSA) was mandated to collect foreign signals, working under a warrant system set by the 1978 Foreign Intelligence Surveillance Act (FISA) and later technologies such as the 1986 Electronic Communications Privacy Act Extended and 1994 CALEA, extending wiretaps from telephones to computer traffic and forcing cell carriers to

[14] Ibid., pp. 269.
[15] Ibid., pp. 269.

keep their digital switches wire-tap-ready.[16] These statutes assumed that sensible warrants and discrete intercepts would suffice. The September 11th attacks disrupted that framework. Though vital leads never reached the right desks in time, Washington treated the catastrophe as a deficit of collection, not coordination. Within six weeks, the USA PATRIOT Act let the FBI seize "any tangible things" and lowered the bar for nationwide wiretaps, while Section 215 dismantled the old probable-cause standard for library, banking, and internet service provider (ISP) records. The 2008 FISA Amendments then authorized warrant-free interception whenever one party of a conversation was "reasonably believed" to be overseas.[17] These legal footholds laid the foundation for mass internet surveillance under the collection of any domestic or foreign traffic through AT&T's Room 641A and PRISM. [18] [19]Policymakers portrayed the increase in legislation as the missing antidote to 9/11: if the hijackers' calls and visas had been visible in one unified database, the plot could have been stopped. Yet, the 9/11 Commission found the actual failure lay in that "information was not shared, analysis was not pooled" across CIA, FBI, and NSA, rather than in any shortage of raw signals intelligence.[20] Policymakers rebuilt the intelligence apparatus around maximal intelligence collection on the premise that more information would translate to more safety, even though the tragedy itself had demonstrated that the issue was within the legal

---

[16] University of Michigan, "History of Surveillance Timeline," Safe Computing, https://safecomputing.umich.edu/protect-privacy/history-of-surveillance-timeline.
[17] U.S. Department of Justice, Bureau of Justice Assistance, "The Foreign Intelligence Surveillance Act of 1978 (FISA)," https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286.
[18] Room 641A is a secret NSA interception facility built into an AT&T switching center in San Francisco and beginning in 2003, where a splitter copied all domestic and international internet traffic that flowed through there. See Ryan Singel, "Whistle-Blower Outs NSA Spy Room," Wired, May 22 2006.
[19] PRISM, launched in 2007, requires US technology companies such as Google to provide the NSA with store data such as e-mails and chat logs for targets "reasonably believed" to be abroad. See Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad, Secret Program," Washington Post, June 7 2013.
[20] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: Government Printing Office, 2004), 353.

and institutional framework of the government. The solution mirrors the common American problem-solving of using brute force and technological scale to resolve an issue. In this case, however, that meant funneling data on hundreds of millions of citizens to be unjustly collected and potentially searched through without their knowledge. The proposed need behind the mass surveillance programs was unjustified, and the constitutionality, or lack thereof, undermined citizens' civil liberties and the Fourth Amendment, setting a precedent for the government's expanding oversight of its citizens.

Additionally, a decade of audits demonstrates that the post-9/11 surveillance systems offer far less security than advertised. The nation, though, became dependent on the existence and perpetuity of the new mass surveillance framework. After reviewing classified case files, Congress's Privacy and Civil Liberties Oversight Board concluded in 2014 that the NSA's collection of bulk phone records had provided only "minimal value" in disrupting terrorist plots.[21] By 2019, Pew Research found that 79 percent of Americans were worried about government data collection, and 62 percent felt it was impossible to escape such tracking—evidence that public frustration had become mainstream.[22] Then why do these programs continue? Former NSA counsel Timothy Edgar pinpoints the structural reason: vast sensor grids are expensive to build but cheap to run, sustaining a "surveillance-industrial complex" of agencies, contractors, and oversight committees whose budgets and careers now depend on data collection.[23] Rolling them back would mean "unwinding an entire operational

---

[21] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (Washington, DC: Privacy and Civil Liberties Oversight Board, January 23, 2014), 146.
[22] Pew Research Center, "Americans and Privacy: Concerned, Confused and Feeling a Lack of Control over Their Personal Information," November 15, 2019.
[23]Timothy H. Edgar, Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA (Washington, DC: Brookings Institution Press, 2017), 11.

culture."[24] The result is an ecosystem of jobs, contractor revenue, and political reputations dependent on the continuance of widespread data collection as an economic cornerstone and security tool. Although the mass surveillance programs were unjustifiably created and provided minimal benefit, the foundation had already been laid, and it was the path of least resistance for legislators to continue them.

In 2013, the Snowden leaks lit a diplomatic flame that forced governments to confront the sweeping global surveillance efforts of the United States. Brazil and Germany—both betrayed by evidence that the NSA had tapped their President Dilma Rousseff and Chancellor Angela Merkel—pushed for the first United Nations resolution on "the right to privacy in the digital age," which called on states to review all mass-surveillance practices and uphold international law.[25] The European Parliament went further, condemning U.S. programs like PRISM as "vast, systemic, blanket" violations of fundamental rights and threatening to suspend financial-data sharing and pause a transatlantic trade pact unless protections improved.[26] Yet Washington did not retreat. President Obama doubled down, defending Section 702 and bulk metadata collection as "critical to our counterterrorism efforts," but promised further oversight.[27] By exporting its data-oriented mindset, the U.S. government inadvertently taught allies and adversaries that strategic advantage lies in digital dominance, laying the blueprint for increased cyberdefense involvement worldwide. A Pew survey helps explain why the security narrative resonated at home: nine in ten American adults described the internet as essential or important to

---

[24] Ibid., pp. 11.
[25] United Nations General Assembly, *Third Committee Approves Text Titled "Right to Privacy in the Digital Age,"* press release GA/SHC/4094, November 26 2013.
[26] European Parliament, *Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights* (2013/2188(INI)), March 12 2014.
[27] Barack Obama, "Remarks by the President on Reviews of United States Surveillance," White House press conference, Washington, DC, August 9 2013.

daily life, even as 64 percent conceded they could not avoid government data tracking.[28] With Americans' increasing reliance on the internet, Congress has repeatedly renewed Section 702 of FISA as especially vital to counterterrorism intelligence and protecting the nation's safety. The same ethos migrated from defensive to offensive, surveillance to sabotage. Determined to slow Iran's nuclear program and quell the nightmare of terrorists acquiring weapons of mass destruction, U.S. and Israeli engineers deployed the Stuxnet worm against the Natanz centrifuges in 2010—the first cyber operation to inflict physical destruction on critical infrastructure.[29] Stuxnet illustrated how code could silently breach sovereign borders and wreak havoc on hardware without a single soldier crossing a line: an example that Russia, China, Iran, and North Korea have since incorporated into their doctrines. Therefore, the diplomatic backlash to the reveal of mass surveillance programs did not curb American ambition: instead, it initiated a global turn toward cyber warfare, where prevention of terror and projection of power now interact in lines of code, making cyberspace the new front line of deterrence and attack.

Two decades after 9/11, the United States still lives with the security architecture built to solve the wrong problem. What the 9/11 Commission identified as a failure of coordination became, through political fear and institutional inertia, an expanding charge for collection. That pivot delivered only marginal strategic gains, but locked surveillance into the backbone of government, commerce, and international conflict. Thus, the mass surveillance programs served as more of an emotional remedy than a reasoned cure. However, the effects had already rippled

---

[28] Pew Research Center, "Digital Privacy: Survey From Pew Research Finds Americans Are 'Concerned, Confused and Feeling Lack of Control Over Their Personal Information'," November 15, 2019, https://www.infodocket.com/2019/11/15/new-report-from-pew-research-finds-americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[29] Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington, DC: Congressional Research Service, 9 December 2010), 1–3.

throughout the world, illuminating data as the key to national security. Every government wanted a piece of it for themselves, with the nations that once criticized PRISM modeling off of it. The idea soon became weaponized in counterterrorism efforts, using lines of code to disrupt uranium enrichment and nuclear armament without sending a single soldier into foreign territory. Alongside this development, terrorists and state-sponsored attackers are turning to the internet as an attack vector, cracking into critical yet vulnerable systems across the world, and allowing the United States government to justify sustaining Section 702 and other signal intelligence programs. Surveillance was never the missing ingredient, yet its reckless expansion by American policymakers has made personal data the strategic high ground of the 21st century, further integrating the misinformed mass surveillance systems and unjust collection of private data into the modern world. A lack of proper communication protocols and response from policymakers to win the War on Terror, a facade of necessary surveillance, and citizens' loss of civil liberties all led to Trump's electoral victory, where he used pathos to appeal to those angered and disillusioned with the American government.

Bibliography:

Edgar, Timothy H. *Beyond Snowden: Privacy, Mass Surveillance, and the Struggle to Reform the NSA*. Washington, DC: Brookings Institution Press. 2017. https://www.jstor.org/stable/10.7864/j.ctt1hfr0zp.

European Parliament. *Resolution on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights* (P7_TA-2014-0230). Strasbourg, 12 March 2014. https://www.europarl.europa.eu/doceo/document/TA-7-2014-0230_EN.html.

Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad, Secret Program." *Washington Post*, 7 June 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Hess, Ryan C. K. "Al-Qaeda's Keys to Success." *Journal of Indo-Pacific Affairs* (Summer 2021): 15-29. https://media.defense.gov/2021/Jun/03/2002733839/-1/-1/0/HESS2.PDF/HESS2.PDF.

Kerr, Paul K., John Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger*

of an Emerging Warfare Capability. CRS Report R41524. Washington, DC: Congressional Research Service, 9 December 2010. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-040.pdf.

Kirk, Michael, director. *America After 9/11*. PBS. Frontline, 2021. 1 hour 56 minutes. https://www.pbs.org/wgbh/frontline/documentary/america-after-9-11/.

Mueller, John, and Mark G. Stewart. *Trends in Public Opinion on Terrorism*. Columbus, OH: Ohio State University, 2020. https://politicalscience.osu.edu/faculty/jmueller/terrorpolls.pdf.

National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. Washington, DC: Government Printing Office, 2004. https://www.9-11commission.gov/report/911Report.pdf.

Obama, Barack. "Remarks by the President on Reviews of United States Surveillance." Press conference, 9 August 2013. White House Archives. https://obamawhitehouse.archives.gov/the-press-office/2013/08/09/remarks-president-press-conference.

Pew Research Center. "Optimism Reigns, Technology Plays Key Role." 24 October 1999. https://www.pewresearch.org/politics/1999/10/24/optimism-reigns-technology-plays-key-role/.

Pew Research Center. "Digital Privacy: Survey From Pew Research Finds Americans Are

'Concerned, Confused and Feeling Lack of Control Over Their Personal Information'." 15 November 2019. https://www.infodocket.com/2019/11/15/new-report-from-pew-research-finds-americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Privacy and Civil Liberties Oversight Board. *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court.* Washington, DC, 23 January 2014. https://irp.fas.org/offdocs/pclob-215.pdf.

Public Law 110-261. *FISA Amendments Act of 2008.* 122 Stat. 2436 (10 July 2008).

Singel, Ryan. "Whistle-Blower Outs NSA Spy Room." *Wired*, 22 May 2006. https://www.wired.com/2006/04/whistle-blower-outs-nsa-spy-room-2/.

United Nations General Assembly. "The Right to Privacy in the Digital Age." A/RES/68/167, 18 December 2013. https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

University of Michigan, "History of Surveillance Timeline," Safe Computing. https://safecomputing.umich.edu/protect-privacy/history-of-surveillance-timeline.