LETTERS TO AMERICA #96

May 27, 2024 13:13:45 EST

Q !!120613817 ID: 177645 No. 6156-7254-8118-052724 🔗

#96 Unveiling the Deep State: How The Deep State Utilizes the NSA, FBI, DOJ, and The IRS to Maintain Power Through Bureaucratic Surveillance and Control

At this pivotal moment in time, America finds itself entrenched within a crisis of unprecedented magnitude, one surpassing the gravity of even the tumultuous period of 1776. This isn't merely a crisis; it's a confluence of conflicts. At its core lies an exhaustive information war, but paramount to that, a spiritual battle for the essence of America and the very souls of its people, reminiscent of biblical proportions. The annals of the last fifteen decades bear witness to an insidious proliferation of corruption, tyranny, and moral decay within the fabric of America. The magnitude of malevolence, treachery, sedition, and blatant disregard for the sanctity of human rights, freedom, and liberty, orchestrated by a cabal of global elites driven by insatiable greed and thirst for power, is nothing short of abhorrent. We find ourselves navigating through a juncture in time where the imperative for every American, every patriot, to rise in defiance, to safeguard our liberties and resist the encroaching tyranny lest they slip through our fingers forever. Letters To America serves as a beacon of truth amidst the pervasive fog of deception, illuminating the shadows of deceit that have enveloped our government for generations, empowering you to discern the truth amidst the pervasive darkness of corruption and manipulation, offering insights into the entrenched evils and pervasive corruption that have ensnared our government and compromised the very essence of America, all for the pursuit of personal gain.

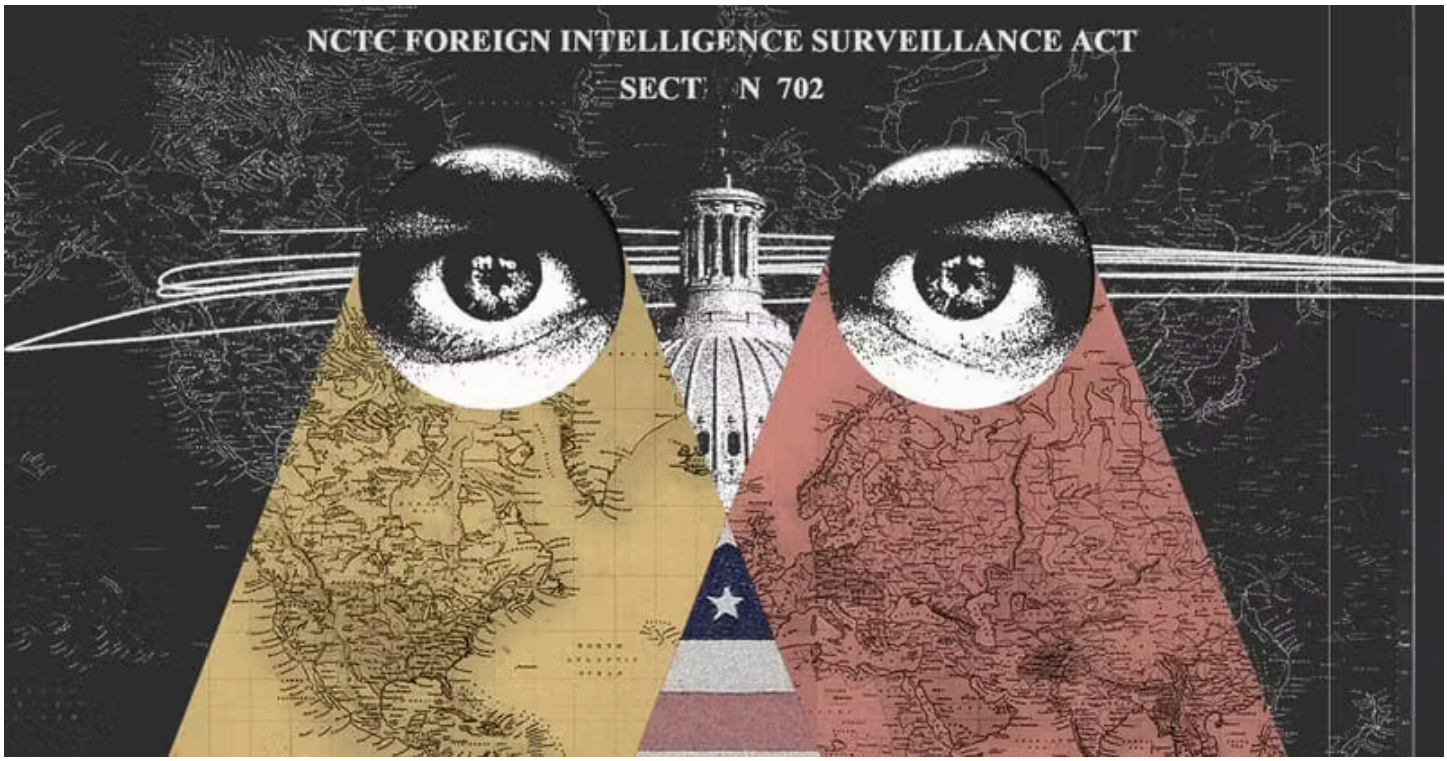
Letters to America is a very detailed collection of intel and information based on the truth that the American people need to know about that has been hidden in the shadows and suppressed for far too long. Letters to America is not just a compilation of facts and data; it embodies a profound commitment to unveiling the concealed realities that the American public deserves to be aware of, truths obscured in the obscure corners and silenced by the mainstream media [FAKE NEWS] outlets. It is a repository of

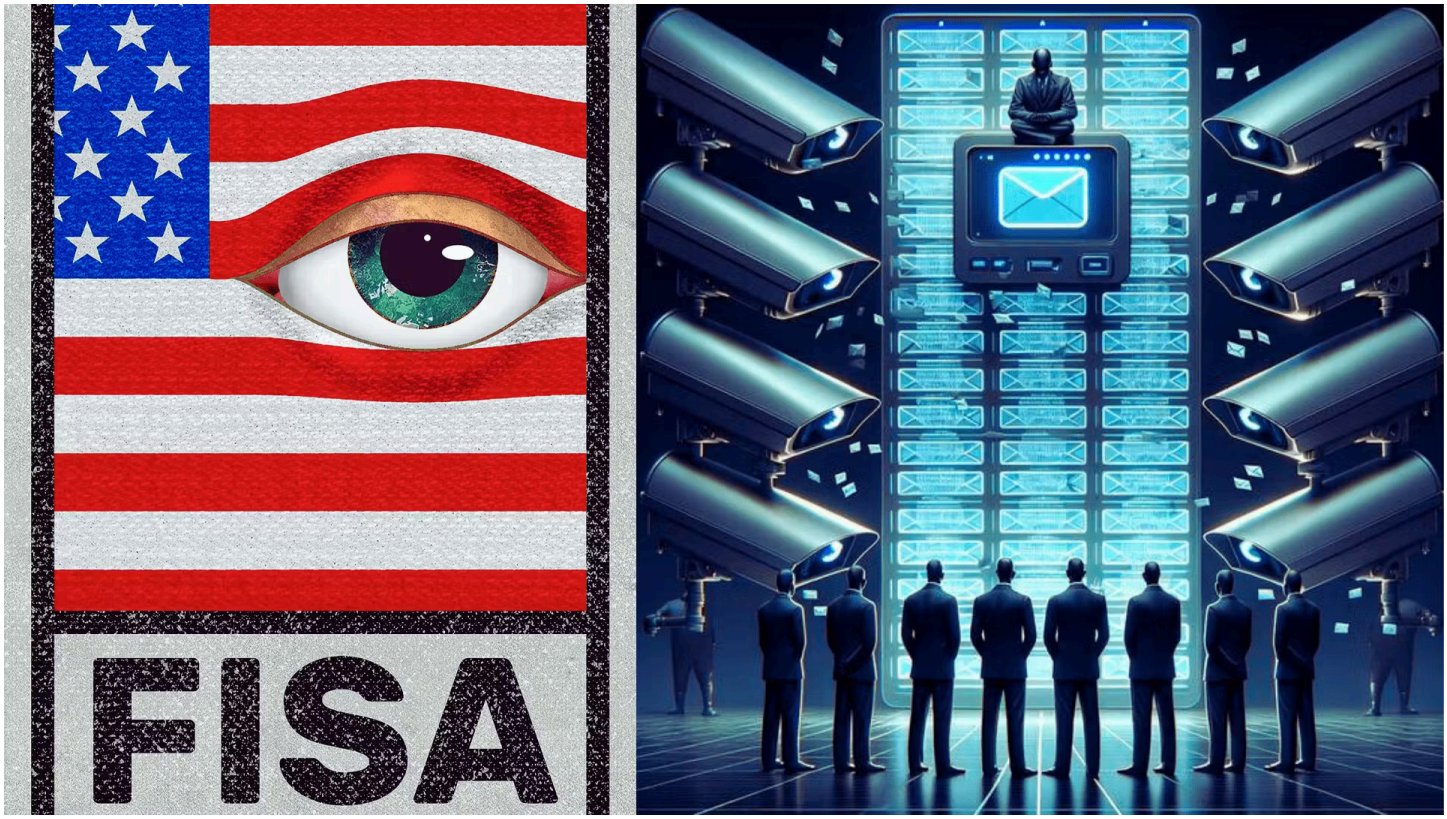
untold stories and hidden narratives and agendas, shunned and suppressed by the behemoth of big tech platforms, including the likes of Facebook. The driving force behind Letters to America is singular and unwavering: the dissemination of unfiltered, unvarnished truth to the people of this great nation. Its mission is to empower individuals to awaken to the veracity that surrounds them, to be informed people, capable of making choices and decisions rooted in the bedrock of truth rather than the quicksand of misinformation, lies and deceit. With depth, integrity, character, and purpose, Letters to America aspires to be the torchbearer of honesty in an era where the clarity of truth is often overshadowed by obscurity.

In today's Letter to America, like always, we embark on a profound journey into the depths of our collective consciousness, where uncomfortable truths reside that are waiting to be acknowledged and confronted. As we navigate the tumultuous waters of our world, it becomes clearly evident that our awareness, or lack thereof, profoundly shapes our understanding of the narratives that unfold before us. The revelations that are chronicled within this letter unveil hidden truths that will challenge preconceived notions, test the boundaries of our beliefs, and ultimately, illuminate the path towards a more enlightened existence. It is in our capacity and our willingness to explore these unsettling truths, to engage with them authentically, and to foster a deeper sense of integrity that will pave the way for a nation that transcends division and seeks the profound unity that binds us all as Americans.

Your level of awakening and consciousness serves as a lens through which the intricate layers of meaning within today's letter unfold, revealing the profound wisdom and insight chronicled within its words. As you delve deeper into the text, your heightened awareness allows you to grasp the subtle nuances and hidden truths hidden between the lines, enriching your understanding of the message and the world around you.

-





The real Russia scandal? [The] Clinton campaign paid for the fake Russia dossier, then lied about it and covered it up. –Sarah Huckabee Sanders, October 2017

The attempts of the deep state to infuse politics into the bureaucracy of the US government mean that organizations like the FBI, the DOJ, and the IRS all agree on the so-called “enemies of the state” who are primed for

harassment, tax audits, criminal prosecutions, and investigations (both civil and criminal). These agencies, which should ideally operate independently and impartially, instead function in a coordinated manner to target individuals and groups deemed a threat to the prevailing power structures. The intertwining of their operations signifies a deliberate effort to centralize control and enforce a uniform narrative across multiple facets of governance and law enforcement. Of course, the Deep State would first need a sophisticated system to gather intelligence, a system that surpasses the capabilities of the CIA and other organizations traditionally tasked with covert information gathering. This well-oiled machine is the National Security Agency, or the NSA. The NSA's vast surveillance infrastructure, coupled with its advanced data analysis capabilities, allows for the comprehensive monitoring of communications and activities, ensuring that the deep state maintains its grip on power by preemptively identifying and neutralizing any potential dissent.

The NSA operates on a global scale, collecting data from millions of sources, which it then processes and analyzes to extract valuable insights. This enables the deep state to anticipate and counteract any threats to its authority, both domestically and internationally. By leveraging cutting-edge technology and sophisticated algorithms, the NSA can sift through enormous volumes of information, identifying patterns and connections that would be invisible to less capable organizations. This pervasive surveillance network effectively creates a state of omnipresence, where the deep state can exert influence and control over virtually every aspect of public and private life. In essence, the deep state's integration of political motives into the bureaucratic machinery, bolstered by the formidable capabilities of the NSA, represents a significant shift in the balance of power within the US government. This alignment of interests and resources underscores a concerted effort to fortify the deep state's position, ensuring its continued dominance and the suppression of any opposition that might challenge its agenda.

With the careful eye of the national intelligence director, the NSA has grown and morphed into a huge surveillance entity. Rather than focusing solely on screening for threats to national security, the NSA has adopted a secondary purpose of monitoring Americans to identify any potential threats to the Deep State and its objectives concerning global governance. Alongside the warrantless surveillance authorized under FISA Section 702, which refers to Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, this expanded role has raised significant concerns about privacy and civil liberties. Critics argue that these measures, initially intended to protect against foreign threats, have been

repurposed to keep tabs on domestic activities, blurring the lines between national security and individual rights. This shift has sparked ongoing debates about the balance between ensuring safety and preserving the freedoms that define American liberty. The increasing capabilities of the NSA to collect and analyze vast amounts of data have led to fears of an Orwellian state where government overreach infringes upon personal freedoms. Moreover, the lack of transparency and accountability in the NSA's operations has further fueled public distrust and calls for reform. Advocates for privacy rights emphasize the need for stringent oversight and legal safeguards to prevent abuses of power and to ensure that surveillance practices do not undermine the fundamental values of America.

(FISA) AMENDMENTS ACT - SECTION 702

The Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, commonly referred to by its specific provision, Section 702, represents a pivotal component in the legal framework governing the United States' foreign intelligence operations. Enacted amidst the evolving landscape of global terrorism and technological advancements, Section 702 is a testament to the nation's ongoing efforts to balance national security imperatives with the protection of civil liberties. To understand Section 702, it is essential to first explore its legislative roots. The original Foreign Intelligence Surveillance Act (FISA) of 1978 was a response to revelations about domestic spying abuses during the 1960s and 1970s. FISA established a legal procedure for surveillance activities targeting foreign powers and their agents within the United States, creating a specialized court—the Foreign Intelligence Surveillance Court (FISC)—to oversee these activities.

However, the rapid technological advancements and the increasing complexity of global communications in the early 21st century exposed limitations in FISA's original framework. Particularly, the pre-9/11 legal structures were seen as insufficient to address the real-time intelligence needs posed by international terrorism and cyber threats. This led to the introduction of the FISA Amendments Act of 2008, with Section 702 being one of its most significant provisions. Section 702 authorizes the U.S. government to conduct targeted surveillance of foreign persons reasonably believed to be located outside the United States, for the purpose of acquiring foreign intelligence information. Unlike traditional FISA processes, Section 702 does not require individual court orders for each target. Instead, it allows the Attorney General and the Director of National Intelligence to jointly authorize annual certifications, which are then approved by the FISC. These certifications define the categories of foreign intelligence information sought and the procedures for targeting and minimizing data.

Minimization procedures are crucial as they dictate how the government handles, retains, and disseminates information about U.S. persons incidentally collected during the surveillance of foreign targets.

A notable and controversial aspect of Section 702 is its warrantless surveillance component. Under Section 702, the U.S. government can collect communications from foreign targets without obtaining a warrant for each individual case. This means that, as long as the surveillance is directed at foreign individuals reasonably believed to be outside the United States, specific warrants are not required, even if the communication is routed through U.S. infrastructure or involves a U.S. person incidentally. This warrantless approach is justified by proponents on the grounds of efficiency and necessity, arguing that the fast-paced nature of intelligence operations, particularly in counterterrorism and counterespionage, cannot afford the delays associated with obtaining individual warrants. They assert that the broad authority granted by Section 702 has been crucial in uncovering and thwarting numerous threats to national security.

Recent legislative and interpretative developments have expanded the scope of Section 702's warrantless surveillance to include certain domestic targets under specific circumstances. These changes have further fueled the debate over the balance between national security and civil liberties. Under the new interpretations, the government can conduct warrantless surveillance on domestic targets if they are communicating with foreign targets under surveillance. This extension means that if a U.S. person is in contact with a foreign individual who is under surveillance, their communications can be collected without a warrant. This expansion aims to address the challenge of identifying and thwarting domestic threats that are linked to foreign entities.

The implementation of Section 702 involves several key agencies, including the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Central Intelligence Agency (CIA). These agencies work in concert to identify, target, and collect foreign intelligence under the parameters set by the FISC-approved certifications. Oversight of Section 702 operations is multifaceted, involving internal compliance officers, the FISC, and external oversight bodies such as the Privacy and Civil Liberties Oversight Board (PCLOB) and Congressional committees. Regular audits and compliance reviews are conducted to ensure adherence to legal requirements and to address any incidents of non-compliance.

Since its inception, Section 702 has been the subject of significant controversy and debate, particularly concerning its impact on privacy and civil liberties. Critics argue that the incidental collection of U.S. persons' communications, coupled with the broad scope of surveillance, poses risks to individual privacy and freedom. The revelations by Edward Snowden in 2013 further intensified these concerns by exposing the extent of data collection practices under Section 702. Proponents, on the other hand, emphasize the critical role of Section 702 in national security. They argue that the provision has been instrumental in thwarting terrorist plots, uncovering espionage activities, and providing actionable intelligence on global threats. The safeguards and oversight mechanisms in place are cited as robust measures designed to prevent abuse and protect civil liberties.

Over the years, Section 702 has undergone several reauthorizations and reforms aimed at enhancing transparency and accountability. Notably, the USA FREEDOM Act of 2015 and subsequent legislative actions introduced measures to increase oversight and limit the scope of incidental collection. The periodic reauthorization process also provides a platform for robust public and legislative debate, ensuring that Section 702 evolves in response to changing technological, legal, and geopolitical landscapes. Each reauthorization has seen attempts to fine-tune the balance between effective intelligence gathering and the protection of individual rights.

Section 702 of the FISA Amendments Act of 2008 remains a cornerstone of U.S. foreign intelligence operations. It embodies the complexities and challenges of maintaining national security in an era characterized by rapid technological change and sophisticated global threats. As debates over privacy and civil liberties continue to shape public discourse, the ongoing evolution of Section 702 will be a critical indicator of how societies navigate the intersection of security and freedom.

In 1976, the Church Committee, a U.S. Senate select committee, conducted a thorough investigation into the activities of the U.S. intelligence agencies. Their findings were alarming: by that time, the FBI had amassed over half a million files on domestic intelligence activities. This extensive surveillance operation included the opening of nearly a quarter of a million first-class letters between 1953 and 1973. Additionally, the CIA had created and maintained a digital index that cataloged the names of approximately 1.5 million Americans, highlighting the pervasive nature of intelligence gathering during this period. Moreover, the NSA, not to be outdone, significantly expanded its surveillance operations in 1967. They compiled a comprehensive "watch list" that targeted peace groups, Black

Power movements, and any individual or organization suspected of engaging in activities that could incite civil disturbances or pose a threat to national security. This widespread monitoring by the NSA exemplified the lengths to which intelligence agencies would go to track and scrutinize Americans, raising serious concerns about privacy and civil liberties in the United States.

ABOUT THE CHURCH COMMITTEE

The Church Committee, officially known as the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, was established in 1975. Named after its chairman, Senator Frank Church of Idaho, the committee was a pivotal force in uncovering and examining the abuses and overreach of U.S. intelligence agencies during the Cold War era.

The establishment of the Church Committee was prompted by a series of revelations about misconduct within U.S. intelligence agencies, particularly the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). In the wake of the Watergate scandal, public trust in government institutions was at an all-time low. Investigative journalists and whistleblowers had begun to expose illegal activities, including domestic surveillance, assassination plots, and other covert operations that violated constitutional rights and international laws.

The Church Committee was tasked with a comprehensive investigation into the actions and operations of U.S. intelligence agencies. The committee held numerous hearings, both public and closed, and interviewed a wide range of witnesses, including government officials, intelligence officers, and victims of surveillance. These hearings were marked by a rigorous examination of evidence and often revealed shocking details about the extent of intelligence operations.

One of the committee’s most notable hearings involved the testimony of CIA Director William Colby, who provided a “Family Jewels” report detailing the agency's most controversial activities. These included plots to assassinate foreign leaders such as Fidel Castro, covert operations to destabilize foreign governments, and extensive surveillance of Americans, including civil rights leaders like Martin Luther King Jr.

The Church Committee's findings were groundbreaking and deeply troubling. It revealed that the CIA had engaged in assassination attempts against foreign leaders, operated secret prisons, and conducted mind-control

experiments under projects like MKUltra. The FBI was found to have engaged in COINTELPRO, a series of covert and often illegal activities aimed at surveilling, infiltrating, and discrediting domestic political organizations.

Moreover, the NSA was discovered to have been involved in extensive warrantless wiretapping and monitoring of Americans' communications. The committee's investigation highlighted a pervasive culture of secrecy and unaccountability within the intelligence community, where operations were often conducted without proper oversight or regard for legal and ethical standards.

The revelations of the Church Committee led to significant reforms in U.S. intelligence operations. One of the most critical outcomes was the establishment of the Foreign Intelligence Surveillance Act (FISA) in 1978, which created a legal framework for surveillance activities and established the FISA court to oversee requests for surveillance warrants against foreign spies inside the United States.

Additionally, the Intelligence Oversight Act of 1980 mandated that intelligence activities be conducted in accordance with the Constitution and subjected them to increased congressional oversight. The committee's work also led to the creation of permanent intelligence oversight committees in both the Senate and the House of Representatives.

The Church Committee's findings had a lasting impact on the public perception of intelligence agencies. It underscored the need for transparency and accountability and established a precedent for congressional oversight of intelligence operations. While some argued that the committee's work hampered intelligence capabilities during the Cold War, others contended that it was essential for safeguarding American principles and preventing abuses of power.

THE WATERGATE COMMITTEE

During the Watergate Committee hearings in June 1973, John Dean released startling information that President Nixon maintained a list of “enemies,” or political adversaries. This revelation exposed a deliberate and systemic effort by the Nixon administration to target and harass individuals on this list. The consequences for those listed were severe and multifaceted. They faced denial of grants and federal contracts, harassment by the IRS and FBI, and potential legal prosecutions. Essentially, any federal action that could be conceived and implemented to complicate or undermine their personal and professional lives was employed. This strategy represented an

unprecedented abuse of executive power aimed at suppressing political dissent and punishing perceived opposition. The exposure of this list highlighted the extent to which the administration would go to maintain its grip on power and silence critics. It revealed a disturbing willingness to use the machinery of the federal government for personal vendettas, undermining the principles of fair governance and rule of law. The revelation of this enemies list not only shocked the nation but also contributed significantly to the growing distrust in the Nixon administration, ultimately playing a crucial role in the unraveling of the Watergate scandal. The deliberate targeting of Americans by their own government underscored the dangers of unchecked executive power and the importance of accountability and transparency in America.

ABOUT THE WATERGATE COMMITTEE

The Watergate scandal remains one of the most significant political events in American history. At the heart of this scandal was the Watergate Committee, formally known as the Senate Watergate Committee, which played a pivotal role in uncovering the depths of corruption within the Nixon administration. Established in 1973, this committee's investigation brought to light abuses of power that ultimately led to the resignation of President Richard Nixon, reshaping the landscape of American politics.

The Watergate Committee was formed in response to the break-in at the Democratic National Committee headquarters at the Watergate complex in Washington, D.C., on June 17, 1972. Initially dismissed as a minor incident, it soon became clear that the break-in was part of a much broader campaign of political espionage and sabotage orchestrated by members of the Nixon administration and his re-election committee. As suspicions grew, so did the demand for a thorough investigation.

In February 1973, the United States Senate voted unanimously to establish a special committee to investigate the Watergate scandal. The committee was chaired by Senator Sam Ervin, a Democrat from North Carolina, known for his deep respect for the Constitution and legal principles. Ervin's reputation for integrity and his background in constitutional law made him an ideal choice to lead the investigation.

The committee's televised hearings began on May 17, 1973, captivating the nation. Millions of Americans tuned in to watch as the committee interrogated key figures involved in the scandal. The hearings revealed a complex web of illegal activities, including burglary, wiretapping, and a cover-up orchestrated at the highest levels of government.

One of the most significant moments in the investigation came when former White House counsel John Dean testified before the committee. Dean provided a detailed account of the cover-up, implicating President Nixon and other top officials. His testimony was a turning point, painting a damning picture of the administration's involvement in the scandal.

Another crucial development was the revelation of the existence of tape recordings of conversations in the Oval Office. These tapes, recorded by a system installed at Nixon's behest, were seen as potential evidence of the president's knowledge and involvement in the Watergate cover-up. The committee's battle to obtain these tapes became a focal point of the investigation.

The Watergate Committee's findings had profound legal and political consequences. The investigation led to the indictment and conviction of several high-ranking officials, including Nixon's top aides, H.R. Haldeman and John Ehrlichman, as well as Attorney General John Mitchell. These convictions underscored the pervasive nature of the corruption within the Nixon administration.

The committee's efforts also set in motion a series of events that ultimately led to President Nixon's resignation. The tapes, once obtained and reviewed, provided undeniable evidence of Nixon's involvement in the cover-up. Facing almost certain impeachment and removal from office, Nixon chose to resign on August 8, 1974, becoming the first and only U.S. president to do so.

The impact of the Watergate Committee's work extended far beyond the immediate consequences for those involved. The scandal and the committee's investigation led to a significant erosion of public trust in government. The American people were shocked by the extent of the abuses of power and the lengths to which officials had gone to conceal their actions.

In response to the Watergate scandal, Congress enacted several reforms aimed at increasing transparency and accountability in government. The Federal Election Campaign Act amendments of 1974, for example, imposed stricter regulations on campaign finance, while the Ethics in Government Act of 1978 established mandatory financial disclosure requirements for federal officials.

The Watergate Committee's investigation also had a lasting impact on journalism. The relentless reporting by journalists Bob Woodward and Carl Bernstein of The Washington Post played a crucial role in uncovering the

scandal and highlighted the importance of investigative journalism in holding those in power accountable.

THE PATRIOT ACT

When the Patriot Act was passed following the terrorist attacks of 9/11, surveillance agencies gained surprising authority for the gathering of domestic intelligence. This legislation enabled agencies such as the NSA to expand their reach and capabilities significantly, allowing for unprecedented levels of surveillance. Whistleblowers like Edward Snowden and William Binney have revealed that the process of gathering domestic intelligence to surveil Americans has reached astonishing new levels, with widespread data collection and monitoring practices that many believe infringe on privacy rights and civil liberties. These revelations have sparked intense debate about the balance between national security and individual privacy in the digital age. Critics argue that the mass surveillance tactics employed domestically have led to a pervasive state of monitoring where individuals' phone calls, emails, and online activities are subject to scrutiny without their knowledge or consent. Proponents, on the other hand, claim that such measures are essential for preventing future terrorist attacks and ensuring the safety of the nation. The controversy continues to evoke strong reactions from the public, policymakers, and legal experts, highlighting the ongoing struggle to define the appropriate limits of government surveillance in a rapidly evolving technological landscape.

Additionally, the impact of these surveillance practices extends beyond just privacy concerns. There are significant implications for freedom of expression and the press, as journalists and activists may feel inhibited in their communications due to the fear of being monitored. This chilling effect can undermine the role of the media as a watchdog and discourage individuals from speaking out against government actions or participating in political discourse. The legal framework surrounding surveillance has also come under scrutiny, with numerous court cases challenging the constitutionality of various provisions of the Patriot Act and related legislation. These legal battles have highlighted the need for clearer guidelines and oversight to prevent abuse of surveillance powers.

Internationally, the revelations have strained relations with allies and raised questions about the global reach of American surveillance operations. Countries that once collaborated closely with the United States on intelligence matters have expressed concerns about the extent of data collection on their people and government officials. This has led to

diplomatic tensions and calls for greater transparency and accountability in intelligence-sharing agreements.

As technology continues to advance, the debate over surveillance and privacy is likely to intensify. Emerging technologies such as artificial intelligence, facial recognition, and big data analytics have the potential to enhance surveillance capabilities even further, raising new ethical and legal questions. This evolving landscape necessitates ongoing discussions about the need for reforms and stronger safeguards to protect civil liberties in an interconnected world. Policymakers, technologists, and civil society organizations must work together to strike a balance that ensures security while respecting individual rights and freedoms. The future of surveillance will depend on finding this equilibrium and establishing robust mechanisms to prevent overreach and protect our American values.

ABOUT THE PATRIOT ACT

The USA PATRIOT Act, enacted in the aftermath of the September 11, 2001 World Trade Center attacks, stands as a significant and contentious piece of legislation in American history. Its primary aim was to enhance national security by broadening the surveillance and investigative powers of federal agencies. However, the act has sparked widespread concerns among Americans regarding mass surveillance and the potential overreach into personal privacy by the National Security Agency (NSA) and other government entities.

The Patriot Act, officially titled "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism," was signed into law by President George W. Bush on October 26, 2001. This act aimed to improve the ability of law enforcement agencies to detect and prevent terrorism. It facilitated information sharing between agencies, expanded the scope of surveillance and wiretapping, and allowed for the detention and deportation of suspected terrorists. While these measures were intended to bolster national security, they also raised significant issues related to civil liberties and privacy.

One of the most contentious aspects of the Patriot Act is its provisions for mass surveillance. The act's Section 215, also known as the "library records" provision, allows the FBI to order any tangible thing, including books, records, papers, documents, and other items, for investigations related to international terrorism or clandestine intelligence activities. This provision has been criticized for its broad scope and potential for

abuse, as it can be used to collect vast amounts of data on innocent individuals without their knowledge.

The revelations by former NSA contractor Edward Snowden in 2013 brought the issue of mass surveillance to the forefront of public consciousness. Snowden disclosed that the NSA was collecting and storing metadata from millions of phone calls, emails, and other forms of communication. This metadata included information such as the time and duration of calls, phone numbers involved, and email addresses. The scale of this data collection was unprecedented and raised serious concerns about the erosion of privacy and civil liberties.

Americans expressed widespread outrage over the NSA's surveillance practices. Critics argued that mass surveillance violated the Fourth Amendment, which protects against unreasonable searches and seizures. The notion that the government could monitor the communications of millions of Americans without individualized suspicion or warrants was deeply unsettling to many. The lack of transparency and oversight in these surveillance programs further fueled concerns about potential abuses of power.

The controversy surrounding the Patriot Act and NSA surveillance led to significant legal and political challenges. In 2015, the USA FREEDOM Act was passed, which aimed to address some of the concerns related to mass surveillance. The FREEDOM Act ended the bulk collection of phone metadata by the NSA and introduced more stringent requirements for obtaining records. However, many privacy advocates argued that these reforms did not go far enough in curbing the government's surveillance powers.

The debate over the balance between national security and individual privacy continues to be a contentious issue in America. Proponents of the Patriot Act argue that the enhanced surveillance capabilities are necessary to protect the nation from terrorism and other security threats. They contend that the measures are justified given the evolving nature of global threats and the need for robust intelligence-gathering capabilities.

On the other hand, critics argue that the erosion of privacy and civil liberties is too high a price to pay for security. They emphasize the importance of maintaining constitutional protections and the potential for government overreach and abuse. The surveillance programs, they argue, create a chilling effect on free speech and dissent, undermining the very principles they are purportedly designed to protect.

A DEEP DIVE ON THE PATRIOT ACT

The September 11, 2001, terrorist attack on the United States led President George W. Bush to declare a War on Terror and Congress to hastily pass the USA PATRIOT Act 45 days later. Supporters said the law would make America safer. Critics argued it gave the government too much power to pry into the private lives of Americans and violated constitutional liberties. Almost two decades after its initial passage, the law, including its most controversial provisions, is still in effect, having been renewed repeatedly by successive administrations and Congresses controlled by both parties. In the background remains the question whether Americans should trade some of their freedom and privacy for more safety and security.

The USA PATRIOT Act's name is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism". The act contained 10 titles, or sections, that covered hundreds of pages of text and amended at least 15 existing statutes. Many of its provisions were relatively noncontroversial, including increasing communication among different federal agencies in foreign intelligence gathering and granting greater regulatory powers to combat foreign money laundering and terrorism and shore up border security. However, a handful of changes to government surveillance powers in Titles II and V of the Act were widely debated. These gave the federal government greater authority to track, intercept, and gather communications and intelligence regarding suspected terrorists at home and abroad.

Under existing criminal law at the time Congress passed the act, the government had the ability to obtain "roving wiretaps" or surveillance on multiple phones for ordinary crimes. These court orders omitted the identification of specific devices or places where the surveillance was to occur when the target was likely to change locations or cell phones rapidly. The only way the government could conduct surveillance on multiple devices used by a foreign target of interest was to obtain separate court authorizations for each device. Section 206 of the USA PATRIOT Act allowed for roving wiretaps, which covered multiple devices without the need for individual authorizations, thus permitting the government to surveil targets of terrorist investigations who rapidly changed locations or devices. Section 207 of the Act expanded the government's authority to conduct surveillance of agents of foreign powers and non-U.S. citizens who are members of international groups. Critics charged that these provisions could lead to the targeting of innocent Americans and the intentional or unintentional intercept of their communications. Supporters argued that

roving wiretaps were a reasonable response to changing technology not tied to a certain location or device.

Section 213 of the USA PATRIOT Act covered "sneak and peek" search warrants, which allowed law enforcement officers to search a home or business and seize material without the knowledge or consent of the owner or occupant. The law did not specify when the FBI had to notify the target, and critics charged that delays in notification were unconstitutional under the protections against unreasonable search and seizure in the Fourth Amendment. Section 215, nicknamed "the library provision," allowed the FBI to ask the Foreign Intelligence Surveillance Act (FISA) court – a special court of federal judges selected by the U.S. chief justice who may issue warrants in foreign intelligence investigations – to compel the sharing of "any tangible thing" related to a terrorism investigation, including books, business documents, tax records, and library check-out lists.

Before the USA PATRIOT Act, the government was required to identify the place or the particular instrument it wished to search. The Act lowered that standard so the government needed only to show the court that a "significant purpose" of the surveillance was to obtain foreign intelligence information. The American Civil Liberties Union (ACLU), as well as other groups, expressed fears that the government would use this new power to circumvent the stricter probable-cause standard for criminal investigations by citing a foreign intelligence interest. In response, the government stressed that the Act explicitly prohibited the government from targeting suspects who solely exercise their freedom of speech to criticize the government or its leaders. Thus, according to the Act's defenders, the government, in fact, would need to establish probable cause by showing the target had performed suspicious actions or had participated in activities that would lead others to believe the target was acting as an agent of a foreign power.

After Portland attorney Brandon Mayfield was wrongly jailed on the basis of these newly eased government procedures, they were struck down in 2007 by Judge Ann Aiken of the U.S. District Court for the District of Oregon as a violation of the Fourth Amendment. The provisions were reinstated, however, when the Ninth Circuit Court of Appeals overturned Aiken's decision in 2009, and they were extended by Congress and President Obama in 2011.

However, in 2013, the media published documents obtained by former National Security Agency contractor Edward Snowden revealed that the U.S. government had allowed the bulk collection of data from Americans under Section 215. Snowden's released documents demonstrated that a FISA Court order forced

Verizon to turn over customer metadata. In 2015, the Second Circuit Court of Appeals ruled that Section 215 did not authorize the bulk collection of phone metadata. Later that year, Congress renewed Section 215 but amended the law to make plain that instead of the government collecting bulk records, the government could obtain information about individuals from phone companies with the permission of a federal court.

One of the Act's most controversial provisions bolstered existing law that enabled the FBI to use National Security Letters (NSLs), a type of administrative subpoena or order to appear in court, to demand various records and data without probable cause or judicial oversight. Although many federal agencies routinely used administrative subpoenas for information gathering, NSLs can be used only in terrorism and espionage investigations. Typically, the FBI made a request to a third party such as a bank, communication provider, or consumer credit agency for subscriber and transactional information like a suspect's name, address, and employment and other records. NSLs did not allow inspection of the content of communications or financial transactions but instead focused on information needed to find out who was in contact with whom. This initial step allowed the FBI to determine whether additional investigation was necessary.

The Act authorized law enforcement to obtain this information through pen register (an electronic device that records phone numbers of outgoing calls from a phone line) and trap-and-trace device (which records phone numbers of calls incoming to a phone line) orders for e-mail as well as telephone conversations. This allowed internet provider (IP) addresses and phone numbers to be disclosed. The pen register and trap-and-trace provision was meant to update existing law that had allowed detectives to examine U.S. postal mail envelopes (but not their contents) for sender and receiver information. Before the USA PATRIOT Act, NSLs could only be issued if the information was "relevant to an authorized foreign counterintelligence investigation" and there were "specific and articulable acts that the person or entity to whom the information sought pertained was a foreign power." The USA PATRIOT Act loosened the standard to allow NSLs to be issued if the information sought from the recipient was "relevant to an investigation to protect against international terrorism or clandestine intelligence activities" (Section 505). In addition, NSLs could be issued by FBI field offices, as opposed to the previous practice whereby only high-level FBI officials such as the director or deputy assistant director could issue them. Finally, the Act placed a gag order on NSLs, meaning the targets whose information was sought were never notified that their information was being turned over to the FBI.

Despite the relative ease with which NSLs could be issued, it was important to note how NSLs differed from search warrants. A person or entity could refuse an NSL request if compliance would be burdensome. Accordingly, the FBI could not simply take the information it wanted. Search warrants, in contrast, required the government to go before a judge and establish probable cause before conducting a search for information. But refusing to comply with a search warrant was not an option, and the government could simply seize the information. Judges also set the scope of search warrants as broad or narrow depending on the information sought, whereas the scope of NSLs has been strictly defined by Congress.

In the years after the USA PATRIOT Act's passage, internal Justice Department audits showed that 40,000 to 50,000 NSLs were issued each year, most of them against people in the United States. Before the Act's passage, only 8,500 NSLs had been issued. Critics charged that this increased level of surveillance of Americans was a direct result of the USA PATRIOT Act's changes to the standards under which NSLs could be issued. Initial audits also showed that, in some cases, information about innocent people was mistakenly obtained and uploaded to FBI databases. Later audits found that the problems had been corrected. But the ACLU challenged NSLs in court, arguing that they violated the First Amendment's freedom of speech guarantee and the Fourth Amendment's prohibition against unreasonable searches and seizures. Specifically, the ACLU said it was impossible for a target to legally oppose a government action he or she did not know about, and that the gag order prohibited the third parties that hold the information from even consulting with their attorneys.

The ACLU prevailed in court. When the controversial sunset provisions of the USA PATRIOT Act, including the NSL provision, were set to expire at the end of 2005, Congress amended the law to allow third parties who receive NSLs to consult their attorneys. Despite this additional safeguard, additional court challenges led to a 2007 ruling striking down the amended NSL provision because, according the court, meaningful judicial review was still not possible under the gag rule.

In all, the controversies surrounding the USA PATRIOT Act prompted a dialogue among Americans and government about the proper balance between security and privacy. Despite the controversy and court challenges, the law has been repeatedly renewed by Congress and succeeding presidents, and the government has exercised greater investigatory powers in areas that were previously private. Although there has not been a major terrorist attack in America since 9/11, the USA PATRIOT Act continues to be a source of

controversy and is routinely cited by critics as an example of excessive government power.

Qx

Listen: https://americanpatriotsocial.com/Qx/LTA/audio/LTA-96.mp3