ISU Journal of Law (ISSN: 3079-7586 & E-ISSN: 3079-7594)

Volume: 01, Issue: 01, 2026 Web: www.isu.ac.bd/journal

RESEARCH ARTICLE

The DHS Intelligence Dilemma: Reforming the DHS Intelligence Sharing and Judicial Oversight under FISA

Md Harun Or Rashid[1]

[1] Additional District and Sessions Judge, Judiciary of Bangladesh; Ph.D. Candidate in International Crime and Justice program, Florida International University (FIU), USA

ABSTRACT

The Department of Homeland Security (DHS) was created to protect the U.S. homeland, yet it cannot conduct electronic surveillance or seek authorization from the Foreign Intelligence Surveillance Court (FISC). Scholarship on the Foreign Intelligence Surveillance Act (FISA) has examined the balance between surveillance and civil liberties but has overlooked DHS's dependence on the Department of Justice and the National Security Agency, and its exclusion from FISC proceedings. Using qualitative doctrinal and policy analysis guided by five theoretical lenses, this study examines how the FISA framework shapes DHS's access to intelligence. It finds that interagency dependence delays actionable intelligence, *ex parte* procedures weaken judicial scrutiny, and intelligence-sharing agreements are outdated. The study proposes expanded amici curiae participation, limited adversarial review, reformed judicial appointments, and a DHS-led One-stop Center for Intelligence Gathering and Sharing (OCIGS). It concludes that institutional redesign can strengthen intelligence effectiveness and judicial oversight together.

ARTICLE HISTORY

Received: October, 2025

1st Revision: November, 2025

Accepted: August, 2026

Online Publication: September, 2026

KEYWORDS

DHS Intelligence, FISA, FISC, Surveillance, Privacy Rights

1. Introduction

Balancing the constitutional right to privacy with the imperatives of national security remains one of the most enduring and complex challenges for modern democratic states. As the leading global power, the United States continues to face persistent threats from transnational terrorist networks, cyber adversaries, and covert foreign intelligence agents operating both domestically and abroad. In response to the September 11, 2001, terrorist attacks, the U.S. government established the Department of Homeland Security (DHS) as the principal federal agency responsible for safeguarding the nation from future threats. Through its Office of Intelligence and Analysis (I&A), DHS contributes to the broader

[1] Corresponding Author: Additional District and Sessions Judge, Judiciary of Bangladesh; Ph.D. Candidate in International Crime and Justice program, Florida International University (FIU), USA. email: mrash021@fiu.edu

Intelligence Community (IC) by assessing threats, producing analytical reports, and disseminating intelligence to federal, state, and local partners[2].

Unlike intelligence agencies such as the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI)[3], DHS does not independently conduct surveillance. Instead, it relies on intelligence shared by other agencies that operate under statutory surveillance authorities. The Foreign Intelligence Surveillance Act (FISA)[4] of 1978 authorizes federal agencies to conduct foreign intelligence surveillance with judicial approval from the Foreign Intelligence Surveillance Court (FISC) [5]. The FISC reviews classified applications and authorizes electronic surveillance, physical searches, and data collection in national security investigations. Although FISA[6] was intended to create judicial oversight and ensure a balance between surveillance authority and civil liberties, scholars and civil rights advocates argue that the court's ex parte proceedings, secrecy, and historically high approval rate raise concerns about transparency, accountability, and privacy protections (Mondale et al., 2016)[7]. Others contend that the framework is necessary to counter evolving forms of terrorism and espionage, but acknowledge that operational and legal reforms are required to enhance surveillance accountability.

This study examines the DHS intelligence dilemma within this legal and operational framework by tracing the historical evolution of U.S. surveillance from early initiatives such as COINTELPRO and ECHELON to post-9/11 expansions under the USA PATRIOT Act, the Protect America Act of 2007, and Section 702 of the FISA Amendments Act of 2008. It investigates DHS's dependence on external surveillance outputs, limitations in intelligence access, and structural barriers to timely information sharing within the IC. The study also evaluates the oversight roles of the FISC and the Foreign Intelligence Surveillance Court of Review (FISCR), particularly in balancing privacy rights and national security.

Although the difficulties of intelligence sharing after 9/11 are well documented in government reports and homeland security studies, the scholarly literature leaves three gaps that this paper addresses. First, most legal scholarship on FISA concentrates on the balance between surveillance powers and civil liberties (e.g.,

[2] U.S. Department of Homeland Security. (n.d.). Creation of the Department of Homeland Security. https://www.dhs.gov/creation-department-homeland-security

[3] Federal Bureau of Investigation & Department of Homeland Security. (2023). Strategic intelligence assessment and data on domestic terrorism. https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report-2022.pdf/view

[4] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978)

[5] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008).

[6] Congressional Research Service. (2020, March 10). Foreign Intelligence Surveillance Act (FISA): An overview. https://crsreports.congress.gov/product/pdf/IF/IF11451/2

[7] Mondale, W. F., Stein, R. A., & Fisher, C. (2016). No longer neutral magistrate: The Foreign Intelligence Surveillance Court in the wake of the War on Terror. Minnesota Law Review, 100(6), 2251–2312.

Mondale et al., 2016; Vladeck, 2015), while largely ignoring DHS's institutional reliance on the DOJ and the NSA for surveillance outputs. Second, previous analyses have not examined the constitutional and governance consequences of DHS's exclusion from FISC proceedings, even though DHS carries the statutory duty to protect the homeland (6 U.S.C. § 121) [8]. Third, reform debates are often framed as a trade-off between intelligence effectiveness and judicial oversight, when the two can in fact be pursued together. Accordingly, this study aims to examine how the evolution of FISA and the FISC has shaped DHS's access to foreign intelligence. It also evaluates the institutional and legal barriers that limit DHS's intelligence-sharing capacity within the Intelligence Community; and finally, it develops structural and legislative reforms that can improve intelligence effectiveness and judicial oversight together. By answering these questions, the paper offers an institutional account of the DHS intelligence dilemma and a theory-informed reform model that treats effectiveness and oversight as complementary rather than competing goals.

This study applies a qualitative doctrinal and policy analysis, drawing from both primary and secondary sources. The analysis is guided by five theoretical lenses: the Security–Liberty Dilemma (Waldron, 2003; Zedner, 2005)[9][10], Social Contract Theory (Locke, 1689/1988; Rousseau, 1762/1973)[11][12], Security Governance (Krahmann, 2003)[13], Accountability Theory (Bovens, 2007)[14], and Surveillance Theory (Foucault, 1977)[15]. This approach enables a structured understanding of DHS's surveillance limitations, oversight gaps, and ethical concerns related to privacy, transparency, and institutional power.

In addition to diagnosing the problems, this paper evaluates proposals for structural and procedural reforms to improve intelligence efficiency while upholding constitutional safeguards. These include establishing a DHS-led One-Stop Center for Intelligence Sharing, embedding second-in-command (2IC) intelligence liaisons from core agencies, modernizing interagency agreements, and enhancing FISC transparency through amici curiae participation and limited

[8] U.S. Code § 121, 6 U.S.C. § 121 (n.d.). https://www.law.cornell.edu/uscode/text/6/121
[9] Waldron, J. (2003). Security and liberty: The image of balance. Journal of Political Philosophy, 11(2), 191–210. https://doi.org/10.1111/1467-9760.00174
[10] Zedner, L. (2005). Securing liberty in the face of terror: Reflections from criminal justice. Journal of Law and Society, 32(4), 507–533. https://doi.org/10.1111/j.1467-6478.2005.00338.x
[11] Locke, J. (1988). Two treatises of government (P. Laslett, Ed.). Cambridge University Press. (Original work published 1689)
[12] Rousseau, J.-J. (1973). The social contract and discourses (G. Cole, Trans.). J.M. Dent & Sons. (Original work published 1762)
[13] Krahmann, E. (2003). Conceptualizing security governance. Cooperation and Conflict, 38(1), 5–26. https://doi.org/10.1177/0010836703038001001
[14] Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x
[15] Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. European Law Journal, 13(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

adversarial review. It also considers legislative reforms to modernize FISA and the need to apply privacy-enhancing technologies in intelligence practices.
Ultimately, this study seeks to determine whether the United States can maintain effective intelligence operations while preserving individuals' privacy rights. It argues that meaningful reform, rather than expansion or restriction alone, is essential to recalibrating the balance between national security and privacy in the evolving surveillance landscape and to keep the nation safe. In short, the paper reimagines DHS intelligence sharing and judicial oversight as two parts of a single governance design, rather than as separate problems.

2. Background of the Study

2.1. Early Surveillance Practices in the United States

Surveillance practices in the United States evolved gradually as part of national security efforts rather than emerging suddenly. Secret surveillance and the gathering and analysis of information are not new to the United States; these practices expanded sharply during and after the Second World War and continue to this day, with certain modifications under the veil of legislative frameworks and court scrutiny. Before the creation of DHS, federal entities, such as the FBI, CIA, and NSA, played key roles in conducting surveillance, ranging from domestic to foreign citizens, targeting both citizens and political opponents in the name of safeguarding the nation's security. The COINTELPRO program was one of them, targeting to suppress those groups and individuals, or civil rights activists who raised their voice against the government[16]. Ruby et al. (2017)[17] stated that it extended into the international arena, particularly through the UK-USA Surveillance Agreement in 1946 and the ECHELON alliance of the USA, Canada, UK, Australia, and New Zealand, known as FIVE EYES[18]. Morrison (2008)[19] stated that since the NSA started its journey in 1952, presidents believed they could spy on people without warrants, even within the USA. This idea grew stronger when President Roosevelt authorized warrantless spying on those suspected of opposing the government in 1940[20]. Before 1967, they thought this spying did not violate the basic principle of the Fourth Amendment's "unreasonable search and seizure" as long as they did not physically break in[21]. In fact, before the enactment of FISA in 1978, there were no clear rules governing

[16] Boykin, S. A. (2015). The Foreign Intelligence Surveillance Act and the separation of powers. University of Arkansas at Little Rock Law Review, 38(1), 33–62. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827313
[17] Ruby, F., Goggin, G., & Keane, J. (2017). "Comparative silence" still? Digital Journalism, 5(3), 353–367. https://doi.org/10.1080/21670811.2016.1254568
[18] Ruby, F., Goggin, G., & Keane, J. (2017). "Comparative silence" still? Digital Journalism, 5(3), 353–367. https://doi.org/10.1080/21670811.2016.1254568
[19] Morrison, T. W. (2008). The story of United States v. United States District Court (Keith): The surveillance power. In C. H. Schroeder & C. A. Bradley (Eds.), Presidential power stories (pp. 189–224). Foundation Press.
[20] Morrison, T. W. (2008). The story of United States v. United States District Court (Keith): The surveillance power. In C. H. Schroeder & C. A. Bradley (Eds.), Presidential power stories (pp. 189–224). Foundation Press.
[21] Liu, E. C. (2013, April 8). Reauthorization of the FISA Amendments Act. Congressional Research Service.

government spying for foreign intelligence[22]. The Keith case (*United States v. United States District Court for the Eastern District of Michigan, Southern Division*, 407 U.S. 297, 1972) held that the government needs a warrant before spying within the country. However, it did not clarify everything, making lower courts unsure when spying needed a warrant. These early developments eventually brought public attention to the unchecked power of federal agencies, setting the stage for greater scrutiny.

2.2. Church Committee Investigations and Public Outcry

As surveillance operations expanded secretly, concerns about government overreach intensified, particularly when political opponents and civil rights leaders became targets. This rising concern ultimately led to congressional investigations that exposed widespread abuse of authority within U.S. intelligence agencies. The scandals like Watergate showed that President Nixon abused this power for political purposes[23]. In December 1974, Seymour Hersh's revelations in The New York Times uncovered illegal covert activities conducted by both the FBI in the USA and the CIA at both home and abroad through extensive hearings and investigations. People grew concerned about warrantless espionage and demanded a greater balance between their right to privacy and national security. Church committees were formed to investigate the activities concerning. After almost two years of investigation, they found an astonishing scenario. They revealed that the FBI's Counterintelligence Program (COINTELPRO), which began in 1956 under President Eisenhower, granted the FBI authority to engage in covert domestic operations, including disinformation operations, mail interception, and electronic surveillance, targets ranging from U.S. anti-Vietnam War activists and African American organizations named as the Southern Christian Leadership Conference, which was founded by Martin Luther King Jr.[24]. According to Goitein and Patel (2015)[25][26], from 1953 to 1973, the CIA searched over 28 million letters, primarily those exchanged with the Soviet Union, and opened around 2 million. In addition, President Lyndon B. Johnson initiated a program in 1967, aiming to investigate the potential involvement of foreign Communist agents in anti-war protests and urban unrest. Moreover, the NSA conducted "Project Shamrock" from the mid-1940s to the mid-1970s, intercepting and analyzing international telegrams sent by American citizens. It is estimated

[22] Sommer, J. (2014). FISA authority and blanket surveillance: Gatekeeper without opposition. Litigation, 40(4), 40–46.
[23] James, A. (2018). Government mass surveillance and law in the Five Eyes countries (Doctoral dissertation). University of Melbourne Law School.
[24] Goitein, E., & Patel, F. (2015, March 18). What went wrong with the FISA Court. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court
[25] Goitein, E., & Patel, F. (2015, March 18). What went wrong with the FISA Court. Brennan Center for Justice. https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court
[26] Patel, F., & Koreh, R. (2021). The impact of amici curiae in the FISA Courts on civil liberties. New York University Annual Survey of American Law, 76(2), 499–598.

that the NSA processed nearly 150,000 messages monthly. These findings revealed an alarming pattern of secret surveillance against U.S. citizens, forcing lawmakers to act and paving the way for legal reforms intended to restore constitutional safeguards.

2.3. Enactment of FISA and Judicial Oversight

The exposure of intelligence abuse demonstrated the urgent need for formal legal oversight to protect civil liberties. The Church Committee expressed grave concerns about the abuse of electronic surveillance capabilities that infringe the rights of privacy of the individual and proposed significant reforms in the existing mechanism of unwarranted surveillance and that eventually persuaded the Congress to legislate the Foreign Intelligence Surveillance Act (FISA)[27] of 1978 aiming to create a check by the Judiciary to the intelligence gathering executive agencies and to establish a legal framework for conducting monitoring of foreign agents and entities within the USA.

FISA's key components included the establishment of the FISC to scrutinize agencies' surveillance requests and criteria for demonstrating probable cause by constraining the duration and breadth of surveillance operations. FISA and the creation of FISC were designed to introduce judicial oversight and safeguard citizens' privacy amidst heightened surveillance[28]. Following the September 2001 attacks, the USA Patriot Act broadened FISA's jurisdiction[29]. This statute extended agencies' surveillance capabilities by extending the validity of surveillance warrants from 45 to 120 days (about 4 months), authorizing wiretapping, and facilitating intelligence exchange between domestic and foreign agencies. It also relaxed and altered the surveillance requirement from a primary to a significant purpose. Previously, applicants were required to certify that surveillance's sole purpose was foreign intelligence acquisition, whereas now they only need to attest that collecting foreign intelligence serves a significant purpose. This adjustment represented a broader initiative to respond to evolving threats and bolster the agency's capacity to counter terrorism. Additionally, the ruling in *In re Sealed* Case (310 F.3d 717, FISCR 2002)[30] affirmed the agency's authority to conduct warrantless surveillance of foreign agents within the USA, providing greater freedom for intelligence-gathering endeavors aimed at thwarting threats. Although FISA introduced judicial oversight mechanisms, critics argue that its post-9/11 expansions granted even broader surveillance powers, raising new concerns about privacy and government accountability.

[27] ibid

[28] Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court: An empirical perspective. Northwestern University Law Review, 101(1), 239–258.

[29] Dinh, V. D., & Keefer, W. J. (2006). FISA and the Patriot Act: Look back and look forward. Annual Review of Criminal Procedure, 35, iii–xxxiv.

[30] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008).

2.4. Expansion Through the PA Act and the FISA Amendments

As terrorism threats evolved in the 21st century, the U.S. government continued expanding its surveillance authorities beyond what was originally envisioned in FISA. These expansions significantly increased executive power while raising debates over privacy rights and constitutional limits. Subsequent legislation, such as the Protect America (PA) Act, 2007 as well as the FISA Amendments Act, 2008 (50 U.S.C. § 1881a), further expanded FISA's scope and powers, allowing for increased surveillance of electronic communications, and sets rules for gathering foreign intelligence on people outside the USA including American and non-American, adding Section 702, which lets the government collect foreign intelligence from communications passing via US networks[31], asking network operators to help for up to a year in targeting non-American people outside the USA, with the Attorney General and DNI needing approval. The FISC needs to approve, before any action, and if there is no time for approval, they must get it within a week after starting the surveillance[32]. However, after Edward Snowden's public disclosure in 2013 as a whistleblower, the Freedom Act of 2015 sought to strike a balance by adding a new amicus curiae provision and allowing the FISC to seek legal advice from amici curiae when necessary[33]. Now, FISA and the FISC serve as the leading judicial authorities for reviewing applications for surveillance activities or for issuing warrants against such applications by the agencies, particularly the NSA. These reforms aimed to address transparency concerns, yet they also highlighted the growing concentration of surveillance power in federal agencies.

Most recently, Congress reauthorized Section 702 through the Reforming Intelligence and Securing America Act (RISAA)[34] of 2024 (Pub. L. No. 118-49). RISAA[35] extended Section 702 until April 20, 2026, tightened the FBI's rules for querying U.S.-person information, expanded the use of *amici curiae* and designated counsel in FISC proceedings, and strengthened reporting requirements and criminal penalties for FISA violations[36]. These continuing amendments show that Congress is still adjusting the balance between surveillance authority and privacy, which makes the institutional questions raised in this paper timely. Table 1 traces this statutory evolution (from 1978–2024*)* and shows what each amendment meant for oversight and for DHS.

[31] Patel, F., & Koreh, R. (2021). The impact of amici curiae in the FISA Courts on civil liberties. New York University Annual Survey of American Law, 76(2), 499–598.
[32] Congressional Research Service. (2025). FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act (CRS Report No. R48592). https://www.congress.gov/crs-product/R48592
[33] USA Freedom Act, Pub. L. No. 114-23, H.R. 2048 (2015).
[34] Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, 138 Stat. 862 (2024).
[35] Chauvin, N. (2025). Increasing congressional oversight of FISA Section 702 after RISAA [Working paper]. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391
[36] Congressional Research Service. (2025). FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act (CRS Report No. R48592). https://www.congress.gov/crs-product/R48592

Table 1. *Evolution of the U.S. Foreign-Intelligence Surveillance Framework*

Legal instrument (year)	Key change introduced	Implication for oversight and for DHS
Foreign Intelligence Surveillance Act (1978)	Created the FISC and FISCR; required probable cause that the target is a foreign power or agent; set duration limits and minimization rules	Established judicial review of foreign-intelligence surveillance for the first time
USA PATRIOT Act (2001)	Changed the certification test from "sole purpose" to "significant purpose"; extended warrant validity; eased intelligence exchange	Broadened surveillance powers and increased the volume of shared intelligence
Protect America Act (2007)	Temporarily authorized programmatic collection targeting persons outside the United States	Shifted part of the process from individualized warrants to programmatic approval
FISA Amendments Act (2008)	Added Section 702 (50 U.S.C. § 1881a): court-approved procedures and annual certifications instead of individual warrants for foreign targets	Concentrated collection capacity in the NSA and FBI, on which DHS depends
USA FREEDOM Act (2015)	Ended bulk metadata collection; created the amici curiae mechanism (50 U.S.C. § 1803(i)); added transparency reporting	Introduced limited independent voices into FISC proceedings
RISAA (2024), Pub. L. No. 118-49	Reauthorized Section 702 to April 20, 2026; tightened FBI U.S.-person query rules; expanded amici and designated counsel; strengthened reporting and penalties	Confirms that Congress keeps adjusting the balance, opening a window for the reforms proposed in this paper

Table 1, compiled from the statutes and analyses cited in Sections 2 and 4 of this paper, shows that each amendment expanded collection capacity or adjusted oversight procedures, but none of them addressed DHS's position within the system. The next subsection turns to that institutional story.

2.5. Post 9/11 Expansion: DHS, External Intelligence, and Dependency

The creation of the Department of Homeland Security (DHS) marked a major restructuring of U.S. national security after 9/11. However, until the inception of DHS, it was still relying on intelligence gathering and sharing from the other intelligence communities, particularly the CIA, FBI, and NSA. Mr. Bush, then President of the USA, acknowledging the challenges, addressed the nation on June 6, 2002, emphasizing the importance of comprehensive engagement to enhance national security. Nonetheless, since its establishment, DHS has left major intelligence agencies such as the FBI, CIA, NSA, and DOD largely independent[37]. Consequently, the DHS lacks an internal intelligence-gathering and analysis department, although it has an Intelligence and Analysis division that relies heavily on external entities such as the CIA and FBI for crucial intelligence, including surveillance reports. Even with the establishment of the ODNI to oversee the entire Intelligence Community, as authorized by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, the DHS and its I&A continue to face challenges in effectively collecting and analyzing intelligence. DHS still relies on the will and wishes of other agencies' reports, even though it is mandated by a heavy duty to protect the nation from all kinds of direct and

[37] National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. https://www.9-11commission.gov/report/911Report.pdf

indirect threats, including terrorism. This dependence on other agencies highlights the lack of independent intelligence capacity within DHS and exposes vulnerabilities in national security coordination.

2.6. Scholarly Debates and the Research Gap

The literature reviewed above can be grouped into three streams that do not fully agree with one another. The first stream debates whether the FISC provides real judicial scrutiny. Critics describe the court as a "rubber stamp" or a "lapdog" because of its secrecy and near-total approval rate[38], while Clarke (2013–2014) responds that high approval rates are common in *ex parte* warrant practice and do not, by themselves, prove weak review. The second stream concerns constitutional structure. Vladeck (2015)[39] and Chin (2021)[40] question whether the FISC's one-sided proceedings fit comfortably within Article III, and Boykin (2015)[41] frames FISA as a separation-of-powers problem, whereas Dinh and Keefer (2006) defend the post-9/11 expansions as a lawful and necessary response to evolving threats. On balance, this study finds the structural critique more convincing, because the defenders of the current framework address the need for surveillance but not the institutional design through which it is authorized and shared. The third stream, found mostly in homeland security studies and official reports, documents DHS's coordination and dependency problems[42][43][44]. Scholarship published since the 2024 reauthorization continues these debates: Chauvin (2025), for example, argues that RISAA delivered only modest reforms and left the Section 702 oversight regime largely intact, which supports this study's position that procedural adjustment alone has not resolved the underlying questions of institutional design.[45]

What is missing is a bridge between these streams: the constitutional literature rarely considers DHS's institutional position, and the institutional literature rarely engages the constitutional questions. The unresolved question, therefore, is what DHS's exclusion from the FISA process means for both intelligence effectiveness and accountable oversight, and whether the two can be improved together. This

[38] Mayer, J. D. (2002). 9-11 and the secret FISA Court: From watchdog to lapdog. Case Western Reserve Journal of International Law, 34(2), 249–252.
[39] Vladeck, S. I. (2015). The FISA Court and Article III. Washington and Lee Law Review, 72(3), 1161–1180.
[40] Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. Yale Law Journal, 131(2), 655–725.
[41] Boykin, S. A. (2015). The Foreign Intelligence Surveillance Act and the separation of powers. University of Arkansas at Little Rock Law Review, 38(1), 33–62. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827313
[42] Brown, M. (2017). The reality of the DHS enterprise field intelligence information sharing environment. Homeland Security Affairs.
[43] Burch, J. (2008). The domestic intelligence gap: Progress since 9/11? Homeland Security Affairs. https://www.hsaj.org/articles/129
[44] U.S. Department of Justice Office of Inspector General [U.S. DOJ OIG]. (2017, March 30). Review of domestic sharing of counterterrorism information (Report No. OIG-17-49).
[45] Chauvin, N. (2025). Increasing congressional oversight of FISA Section 702 after RISAA [Working paper]. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5084391

paper addresses that question directly, and the remainder of the analysis is organized around it.

3. Research Design

This study uses a qualitative doctrinal and policy analysis approach to examine the Department of Homeland Security (DHS)'s intelligence-sharing limitations within the United States' surveillance framework. This approach is appropriate because the subject matter involves legal authorities, institutional procedures, and national security policies that operate in classified environments and are not accessible through empirical field research. Accordingly, this study relies on the interpretation and analysis of legal texts, policy documents, institutional reports, and scholarly literature to evaluate how surveillance is authorized, implemented, and overseen under the Foreign Intelligence Surveillance Act (FISA)[46] and the Foreign Intelligence Surveillance Court (FISC)[47]. This method enables a structured investigation of the legal and institutional arrangements governing national security surveillance without requiring direct access to classified operational data.

The analysis is guided by five theoretical perspectives that, together, provide a coherent framework for understanding the interaction among state security powers, institutional practice, and constitutional safeguards. First, the security–liberty dilemma theory explains the tension between the government's responsibility to maintain national security and its duty to protect individual rights[48]. This theoretical lens is relevant for analyzing how surveillance powers expand during periods of heightened security threats and how FISC's classified, non-adversarial process raises concerns over due process and privacy. Second, the study draws on social contract theory, which holds that citizens permit the exercise of state power in exchange for security but expect that such power will remain accountable and within constitutional limits (Locke, 1689/1988; Rousseau, 1762/1973)[49]. This framework supports the role of judicial authorization, congressional oversight, and legislative safeguards in preserving public trust in surveillance practices.

Third, security governance theory acknowledges that modern security is dispersed across multiple actors rather than centralized in a single institution[50]. This perspective is essential for explaining DHS's structural dependency on agencies such as the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) for

[46] ibid
[47] ibid
[48] Zedner, L. (2005). Securing liberty in the face of terror: Reflections from criminal justice. Journal of Law and Society, 32(4), 507–533. https://doi.org/10.1111/j.1467-6478.2005.00338.x
[49] ibid
[50] Krahmann, E. (2003). Conceptualizing security governance. Cooperation and Conflict, 38(1), 5–26. https://doi.org/10.1177/0010836703038001001

intelligence collected under FISA authority. Fourth, accountability theory emphasizes the need for institutional oversight to prevent the misuse of governmental power (Bovens, 2007)[51]. This framework is used to assess the effectiveness of FISA-related oversight mechanisms, including FISC judicial review, Inspector General evaluations, congressional reporting under 50 U.S.C. § 1871, and reforms introduced by the USA FREEDOM Act of 2015. Finally, Foucault's surveillance theory provides a broader socio-institutional interpretation of surveillance as a mechanism of control carried out through the regulation of information (Foucault, 1977)[52]. This theory informs the critique of FISC secrecy and the concentration of surveillance authority within the executive branch.

This study relies on documentary analysis of both primary and secondary sources. Primary sources include statutory texts such as FISA (1978)[53], the USA PATRIOT Act (2001)[54], the Protect America Act (2007)[55], the FISA Amendments Act (2008), Section 702 of the U.S. Code, and the USA FREEDOM Act (2015)[56]. Judicial decisions, including *United States v. United States District Court for the Eastern District of Michigan, Southern Division*, 407 U.S. 297, 1972 and *In re Sealed* Case, 310 F.3d 717 (FISCR 2002)[57], provide legal interpretation of surveillance authority. Secondary sources include reports from the Congressional Research Service (CRS), ODNI transparency reports, DHS Office of Intelligence and Analysis publications, Office of Inspector General (OIG) assessments, and peer-reviewed academic studies on surveillance law, counterterrorism policy, and intelligence oversight.

Sources were selected using three criteria: (1) legal authority, giving priority to statutes, codified provisions, and judicial decisions as primary sources; (2) institutional relevance, focusing on official oversight materials that directly address DHS, the FISC, or interagency intelligence sharing; and (3) scholarly quality, favoring peer-reviewed law review articles and academic monographs over secondary commentary. Where authorities conflict—for example, on whether the FISC's high approval rate shows weak scrutiny (Mayer, 2002; Mondale et al., 2016)[58] or ordinary *ex parte* practice (Clarke, 2013–2014) [59]—the

[51] ibid
[52] ibid
[53] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008).
[54] The USA PATRIOT Act: Preserving life and liberty. (2001). U.S. Department of Justice. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf
[55] Purnell, E. (2022). The American right to privacy: Legacies of the 1975 Church Committee in U.S. public memory (1976–2021) (Doctoral dissertation, Carnegie Mellon University).
[56] USA Freedom Act, Pub. L. No. 114-23, H.R. 2048 (2015).
[57] ibid
[58] Mayer, J. D. (2002). 9-11 and the secret FISA Court: From watchdog to lapdog. Case Western Reserve Journal of International Law, 34(2), 249–252.
[59] Clarke, C. (2013–2014). Is the Foreign Intelligence Surveillance Court really a rubber stamp? Ex parte proceedings and the FISC win rate. Stanford Law Review Online, 66, 125–134.

study weighs the empirical basis of each claim, the interpretive method used, and its consistency with the statutory text before adopting a position. Doctrinal analysis is appropriate for this study because the study's objectives concern what the law authorizes, how institutions are structured by that law, and whether the resulting arrangements satisfy constitutional principles; such questions cannot be answered through empirical field research in a classified environment.

A thematic analysis approach is used to organize and interpret findings across three core areas: (1) the historical evolution of U.S. surveillance authority and oversight mechanisms; (2) institutional limitations affecting DHS intelligence access and operational dependency; and (3) accountability challenges related to secrecy, transparency, and compliance within the FISA framework. This methodology aligns with the study's qualitative design and ensures that the analysis remains grounded in verifiable legal evidence, institutional records, and theoretical reasoning, while addressing the broader policy implications of surveillance reform in the United States.

Finally, the study distinguishes among its descriptive, analytical, and normative components. Sections 2, 4, and 5 are mainly descriptive and doctrinal: they set out what the law provides and how the institutions operate. Section 6.1 is analytical: it applies the five theoretical lenses to evaluate those arrangements. Section 6.2 is normative: it derives reform proposals from that analysis. Each recommendation is developed in the same sequence—an institutional or legal weakness is identified in the doctrinal analysis, the relevant theory explains why the weakness matters, and the proposal is then checked against constitutional constraints such as Article III limits, the Fourth Amendment, and separation-of-powers principles. This explicit chain from evidence to theory to proposal is intended to make the study's normative reasoning transparent and reproducible rather than intuitive.

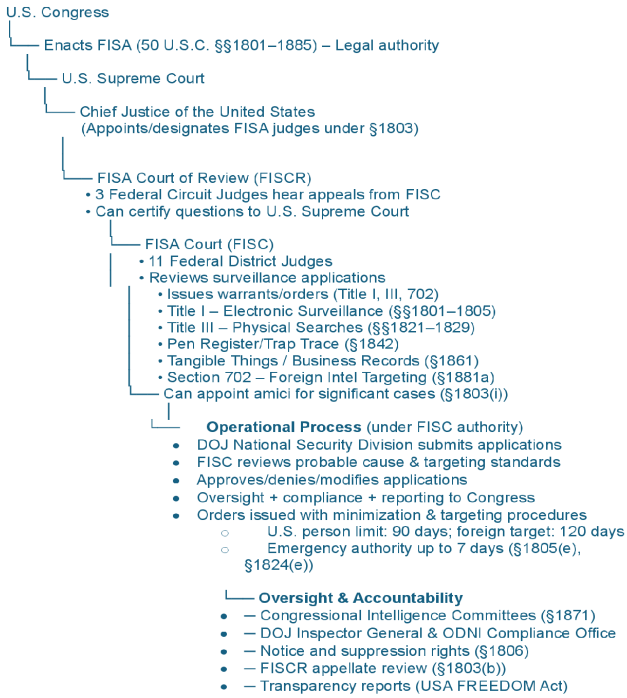
4. Discussion and Analysis

4.1. Structure and Operation of FISC and FISCR

Understanding the surveillance accountability and judicial oversight that is, the functioning of the Foreign Intelligence Surveillance Court (FISC)[60] and the Foreign Intelligence Surveillance Court of Review (FISCR)[61] is essential to grasping how secret surveillance is authorized and reviewed in the United States. The flow chart visually outlines the institutional structure, legal authority, and operational process of the Foreign Intelligence Surveillance Court (FISC)[62] and the Foreign Intelligence Surveillance Court of Review (FISCR) under the Foreign Intelligence Surveillance Act (FISA), demonstrating how surveillance applications are authorized, reviewed, and overseen within the United States national security framework (**Figure 1**).

[60] ibid
[61] ibid
[62] ibid

Figure 1: *FISA Court Operation and Surveillance Framework*



As illustrated in the flow chart, the statutory, judicial, and operational architecture of foreign intelligence surveillance is established under the Foreign Intelligence Surveillance Act (FISA), codified at 50 U.S.C. §§ 1801–1885c [63]. Enacted by Congress to regulate national security surveillance while safeguarding constitutional rights, FISA created a specialized judicial system to oversee classified intelligence operations. Under 50 U.S.C. § 1803, the Chief Justice of the U.S. Supreme Court appoints federal judges to serve on the FISA courts, which include the FISC, composed of 11 federal district judges, and the FISCR, a three-judge appellate body[64].

Applications for surveillance warrants are submitted to FISC by the Department of Justice's National Security Division (DOJ-NSD). These applications must satisfy statutory requirements for probable cause, minimization procedures, and targeting limitations for foreign intelligence purposes (Patel & Koreh, 2021)[65]. The legal authorities under which FISC issues orders include Title I electronic

[63] ibid
[64] U.S. Code § 121, 6 U.S.C. § 121 (n.d.). https://www.law.cornell.edu/uscode/text/6/121
U.S. Code § 1805, 50 U.S.C. § 1805. https://www.law.cornell.edu/uscode/text/50/1805
[65] ibid

surveillance, physical searches, business records, pen registers, and Section 702 foreign intelligence collection. As Dinh and Keefer (2006)[66] explain, FISA applications must include detailed information identifying the federal officer submitting the request, the authority granted by the President and certified by the Attorney General, a description of the surveillance target, justification that the target is a foreign power or agent, the type of information sought, proposed minimization procedures, and the method of surveillance. Additional disclosures must include the history of prior applications, the duration of the requested surveillance, the nature of surveillance devices, and accompanying executive certifications (Dinh & Keefer, 2006)[67].

FISC proceedings are conducted *ex parte* and in secrecy, meaning only the government participates in the process (Vladeck, 2015)[68]. The court scrutinizes each application to determine whether there is probable cause to believe that the target of surveillance is a foreign power or an agent using facilities or locations inside the United States, as required by 50 U.S.C. § 1805. If satisfied, FISC may issue an order authorizing surveillance for a limited duration—90 days for U.S. persons for electronic surveillance, 45 days for physical searches, and up to 120 days for foreign targets, with emergency authorization of up to 7 days permitted under §§ 1805(e) and 1824(e). In cases involving novel or complex legal issues, FISC may appoint amici curiae to provide independent legal perspectives, as authorized under 50 U.S.C. § 1803(i) (Patel & Koreh, 2021)[69].

Appeals from FISC decisions are heard by the FISCR, which serves as the exclusive appellate body for FISA-related matters and may certify questions of law to the U.S. Supreme Court[70]. Although rare, individuals subjected to FISA surveillance may, under limited circumstances, petition for a writ of certiorari to seek review of such orders[71]. In addition to judicial oversight, FISA incorporates multiple accountability mechanisms, including mandatory reporting to Congressional Intelligence Committees (§ 1871), compliance audits conducted by the DOJ Office of Inspector General and the Office of the Director of National Intelligence (ODNI), and transparency reporting obligations introduced under the USA FREEDOM Act of 2015, which also eliminated bulk metadata collection (Vladeck, 2015)[72].

Despite these procedural safeguards, scholars frequently argue that FISC's classified, non-adversarial proceedings raise constitutional concerns about due

[66] Dinh, V. D., & Keefer, W. J. (2006). FISA and the Patriot Act: Look back and look forward. Annual Review of Criminal Procedure, 35, iii–xxxiv.
[67] ibid
[68] Vladeck, S. I. (2015). The FISA Court and Article III. Washington and Lee Law Review, 72(3), 1161–1180.
[69] ibid
[70] ibid
[71] ibid
[72] ibid

process, transparency, and the separation of powers (Vladeck, 2015)[73]. Nonetheless, the structure of FISC and FISCR illustrates an institutional attempt to balance national security imperatives with judicial review and democratic accountability within the framework of American constitutional governance.

4.2. Approval Rates and Criticism of FISC

Although FISA and FISC were created to introduce judicial checks on surveillance, critics argue that the system functions more as a formality than as true oversight. The primary purpose of the FISC court is to oversee agency surveillance activities while protecting individuals' privacy rights. However, debates persist regarding its effectiveness, particularly considering its nearly 99% approval rate. During the first 33 years of its existence, from 1979 to 2012, the FISC received 33,900 ex parte requests from federal agencies, with a remarkable approval rate of 99.97%, as only 11 requests were denied (Clarke, 2013)[74]. The NSA and FBI, upon receiving approval from the FISC, are conducting surveillance activities and trying to protect the nation from all external and internal threats and future terrorist attacks. The DHS was created under the Homeland Security Act of 2002 for the same protective purpose after the September 11, 2001, attacks (Bullock et al., 2018)[75]. The department combined all or part of 22 federal agencies and roughly 180,000 employees when it opened its doors in March 2003, and it has since grown into the third-largest cabinet department (U.S. Department of Homeland Security, n.d.)[76]. These developments shifted part of the national security focus toward homeland protection, but they also introduced new challenges in intelligence coordination across agencies. Section 5 examines those coordination challenges in detail.

4.3. DHS in the intelligence sharing mechanism in the USA

The US national security depends on the ability to share accurate information in a timely manner with the proper person (U.S. DOJ OIG, 2017). Meaningful coordination and communication among federal, state, local, and tribal entities, along with engagement with the private sector and international partners, are imperative (U.S. DOJ OIG, 2017; White House, June 27, 2023)[77]. In the wake of September 11, 2001, the United States faces persistent threats from various terrorist organizations, both domestically and internationally. Recent attacks in New Zealand, Paris, Brussels, and Orlando underscore the ongoing challenges in safeguarding national security (U.S. DOJ OIG, 2017; Crothers & O'Brien,

[73] ibid
[74] ibid
[75] Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2018). Homeland security: The essentials (2nd ed.). Elsevier.
[76] U.S. Department of Homeland Security. (n.d.). Creation of the Department of Homeland Security. https://www.dhs.gov/creation-department-homeland-security
[77] ibid

2020)[78]. In response to these threats, the U.S. government has implemented comprehensive intelligence-sharing mechanisms involving all national entities and international partners (White House, June 27, 2023)[79]. As a major partner of the IC, the DHS plays a vital role in protecting the nation from all forms of terrorist and security threats through intelligence analysis, information gathering, and sharing with other agencies.

Following the attacks of September 11, the DHS's goal is to prevent any terrorist incidents within the nation and bolster national security by gathering and disseminating intelligence from other members of the intelligence community (6 U.S. Code § 121). Through its Office of Intelligence and Analysis (I&A), the DHS collects, evaluates, and shares intelligence vital for detecting and countering potential threats from adversaries. Moreover, DHS enterprises such as Immigration and Customs Enforcement, Customs and Border Protection, the US Coast Guard, and the Transportation Security Administration play pivotal roles in protecting the nation's borders, transportation systems, and critical infrastructure, and in enforcing immigration laws (U.S. DOJ OIG, 2017). The intelligence-sharing framework in the United States operates through collaboration among federal, state, local, tribal, and private-sector entities (6 U.S. Code § 121). The IRTPA of 2004 laid the foundation for establishing the Information Sharing Environment (ISE), aimed at facilitating the exchange of terrorism-related information among diverse stakeholders. As a crucial participant in this environment, the DHS utilizes its intelligence capabilities to contribute to the broader national security landscape.

At the federal level, the ODNI serves as the central coordinator of intelligence activities across the 16 members of the IC and as an advisor to the DHS (ODNI, 2007). A crucial component of the ODNI is the NCTC, which plays a pivotal role in analyzing and integrating terrorism-related intelligence (Pigato, 1989)[80]. Additionally, oversight of the dissemination of terrorism-related information among federal, state, local, tribal, and private sector partners is managed by the Program Manager for the Information Sharing Environment, ensuring a cohesive approach to intelligence sharing (U.S. DOJ OIG, 2017)[81].

Within the DHS, the I &A department leads the collection and analysis of intelligence in a prompt and actionable manner (U.S. Department of Homeland Security, 2020)[82]. Through its nationwide Field Operations, I&A deploys intelligence officers and regional directors to engage with state and local partners,

[78] Crothers, C., & O'Brien, T. (2020). The contexts of the Christchurch terror attacks: Social science perspectives. Kōtuitui: New Zealand Journal of Social Sciences Online, 15(2), 247–259. https://doi.org/10.1080/1177083X.2020.1746364
[79] ibid
[80] Pigato, G. (1989). The turn of the role of intelligence after September 11 [Master's thesis]. Ca' Foscari University of Venice.
[81] ibid
[82] ibid

facilitating intelligence gathering and sharing. Moreover, components such as the US Coast Guard, CBP, ICE, and TSA integrate intelligence into their operations to detect and mitigate potential threats at various points of entry and critical infrastructure (U.S. DOJ OIG, 2017)[83].

Close cooperation between the DHS and the DOJ, particularly with the FBI and US Attorney's Offices, is essential for sharing counterterrorism information at the field level. Joint Terrorism Task Forces, comprised of federal, state, and local law enforcement agencies, serve as vital mechanisms for coordinating counterterrorism efforts and investigating potential threats (Alexander, 2005)[84]. Additionally, Field Intelligence Groups within the FBI enhance intelligence collection and analysis at the local level, complementing DHS's efforts (U.S. DOJ OIG, 2017).

Acknowledging the crucial role of state, local, and tribal entities in homeland security, the United States has established 80 fusion centers (US GAO, 2023, June 26) and regional information sharing systems to facilitate intelligence dissemination at the grassroots level. These fusion centers serve as central points for sharing threat-related information among federal, state, local, tribal, territorial, and private-sector partners (Willman, 2020). Regional Information Sharing Systems (RISS) further bolster law enforcement and public safety agencies by providing resources, analytical support, and training (White House, 2023, June 27)[85] to enhance their capabilities to combat terrorism and major crimes. Table 2 brings these many actors together, summarizing each institution's mandate, its role under FISA, the main challenge identified in this study, and the corresponding reform developed in Section 6.

Table 2. *Institutional Responsibilities and Proposed Reforms within the U.S. Foreign Intelligence Surveillance Framework*

Institution	Core mandate	Role in FISA surveillance	Key challenge identified	Reform proposed in this study
DHS (I&A)	Protect the homeland; share intelligence with federal, state, and local partners (6 U.S.C. § 121)	No direct FISC access; consumer of intelligence shared by others	Dependency on DOJ/NSA; outdated MOUs; internal fragmentation	OCIGS center; updated agreements; structured access to FISC outputs
DOJ (NSD)	Federal law enforcement; legal representation of the government	Prepares and submits FISA applications to the FISC	Gatekeeping position adds bureaucratic layers between collection and DHS	Structured, classified transmission of relevant orders to DHS
NSA	Signals intelligence collection	Principal collector under FISA Title I and Section 702	Concentration of informational power; discretionary sharing	2IC liaison embedded in OCIGS
FBI	Domestic intelligence and law enforcement	Applies for and conducts FISA surveillance; queries Section 702 data	Overlapping mandates and unclear protocols with DHS	Standardized coordination mechanisms; 2IC liaison

[83] ibid

[84] Alexander, B. C. (2005). Strategies to integrate America's local police agencies into domestic counterterrorism. U.S. Army War College.

[85] White House. (2023, June 27). Fact sheet: National strategy for countering domestic terrorism—Strategic implementation update. https://www.whitehouse.gov/briefing-room/statements-releases/2023/06/27/fact-sheet-national-strategy-for-countering-domestic-terrorism-strategic-implementation-update/

CIA	Foreign intelligence collection and analysis	Collector and consumer of foreign intelligence abroad	Foreign–domestic division creates gaps in threat pictures	2IC liaison embedded in OCIGS
ODNI	Coordination of the Intelligence Community	Oversight, transparency reporting, and IC integration	Limited practical authority over interagency turf battles	Oversight of OCIGS performance and compliance
FISC / FISCR	Judicial review of surveillance applications	Approves, modifies, or denies FISA applications; hears appeals	*Ex parte* secrecy; historically high approval rate	Expanded *amici curiae*; limited adversarial review; revised appointments

Table 2, compiled from the statutes, reports, and analyses discussed in Sections 4–6 of this paper, indicates, these challenges are connected rather than isolated. The following subsections examine them in detail.

4.4. Discoordination Within the Intelligence Community

The lack of centralized intelligence sharing has long been identified as a major weakness in U.S. homeland security. Fragmented systems prevent timely information exchange, which is crucial for preventing threats. Moreover, in the existing intelligence operations mechanism, the DHS faces significant challenges, including coordination and effectiveness in safeguarding national security interests, which require immediate attention and reform. This department currently faces difficulty due to the decentralized nature of intelligence gathering (Brown, 2017)[86], with various agencies operating independently. This division hinders the timely and comprehensive assessment of terrorist threats. For example, the Terrorist Threat Information Center (TTIC) and the Counterterrorism Division (CTD) within the FBI operate somewhat autonomously, potentially creating gaps in understanding terrorist networks. Moreover, while some agencies, like the Counterterrorism Center (CTC) at the CIA, focus on overseas operations, others, like the CTD, primarily deal with domestic intelligence. This division can result in incomplete insights into global terrorist networks. In addition, the inability of other federal agencies to communicate effectively due to incompatible computer systems poses a significant challenge to intelligence sharing. For instance, the Border Patrol, now part of the DHS, utilizes a fingerprint identification system that does not integrate with the FBI's criminal records database, resulting in gaps in criminal history information for apprehended individuals (Barlett & Steele, 2004, p. 62). Despite directives to integrate these systems dating back to the 1990s, progress has been slow, leaving critical gaps in intelligence sharing (Barlett & Steele, 2004, p. 62). Furthermore, DHS's heavy reliance on external intelligence sources exacerbates the disconnect between intelligence gatherers and the department, hindering its ability to generate independent intelligence on terrorist threats (Badley, 2004, pp. 1-2). Additionally, bureaucratic power struggle further undermines the DHS's effectiveness, preventing it from competing with major intelligence agencies

[86] Brown, M. (2017). The reality of the DHS enterprise field intelligence information sharing environment. Homeland Security Affairs.

(Victor, 2002, p. 1779). This persistent loose coordination demonstrates the need for structural reform in the U.S. intelligence system to promote unified and efficient information sharing.

4.5. Legislative Reforms and Continued Challenges

Although legislative steps have been taken to improve intelligence integration, many structural problems continue to limit efficiency. To improve this scenario, Congress passed a restructuring bill in November 2004, creating a DNI with increased oversight of the national intelligence budget (Schmitt, 2004, A1). However, challenges persist, with turf battles between intelligence agencies and uncertainties regarding the DNI's authority (Schmitt, 2004, A1). Despite these efforts, the DHS's intelligence analysis division remains underpowered, leaving it reliant on external agencies for secret intelligence and other terrorist threat-related issues (Schmitt, 2004, A1). Consequently, the DHS continues to face challenges in fulfilling its mandate to protect the homeland from terrorist threats. Emphasizing the critical need for enhanced information sharing and collaboration among intelligence agencies, addressing these challenges involves consolidating these efforts within the IC, particularly among the FBI, NSA, and CIA. By establishing centralized platforms or enhancing data integration, exchange, coordination, and collaboration in a timely manner, such as through joint initiatives with other intelligence agencies, the DHS can improve its ability to identify and respond to terrorist threats effectively. Without addressing these structural weaknesses, the cycle of intelligence gaps and delayed responses will likely continue, leaving the nation vulnerable to evolving threats

4.6. DHS and ICs' intelligence sharing dilemma

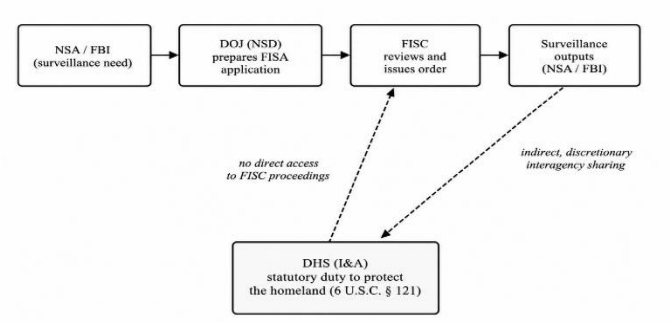
Ensuring effective and efficient information sharing and gathering is crucial for bolstering national security and upholding individual privacy rights in the ongoing battle against terrorism. Nonetheless, recent OIG assessments have uncovered notable hurdles that impede the DHS in this vital area (U.S. DOJ OIG, 2017)[87]. Presented below are the key challenges presently confronting the DHS in its endeavors to safeguard the nation and improve information sharing and gathering. A primary challenge facing the DHS is the inconsistent nature of interagency cooperation, particularly between the DHS and the FBI. Despite both agencies sharing counterterrorism-related information, concerns persist regarding potential overlaps in their conduct (U.S. DOJ OIG, 2017). This ambiguity can lead to confusion among field personnel about information-sharing protocols, potentially weakening trust and communication among law enforcement agencies. To mitigate this, the DHS and FBI should prioritize establishing standardized

[87] U.S. Department of Justice Office of Inspector General [U.S. DOJ OIG]. (2017, March 30). Review of domestic sharing of counterterrorism information (Report No. OIG-17-49).

coordination mechanisms to ensure seamless communication in counterterrorism efforts (US Government Accountability Office, 2023).

While the DHS is involved in homeland security and intelligence activities, it does not file any applications directly with the FISC. The NSA, as part of the United States government and the broader intelligence community, has the authority to apply to the FISC for secret surveillance. Typically, the Attorney General of the DOJ's National Security Division (Purnell, 2022)[88] is responsible for preparing and submitting applications to the FISC on behalf of agencies such as the NSA. After obtaining a surveillance warrant, the NSA conducts surveillance of foreigners or foreign agents who intend to do harm or destabilize US national security. NSA collects all secret information regarding plans or acts of terrorism, sabotage, or attacks by visible and invisible enemies. Although the DOJ, NSA, and DHS are tasked with safeguarding the nation from future threats, the DHS lacks a mechanism to obtain this information directly. It depends on information from the DOJ or the NSA. So, there needs to be an effort to solve this issue. Figure 2 illustrates this arrangement: the authorization chain runs from the collecting agencies through the DOJ to the FISC, while DHS sits outside that chain and receives its outputs only indirectly.

Figure 2: *Overview of the Surveillance Authorization and Information-Sharing Chain and the DHS Status*



Another significant difficulty is the lack of updated strategies and agreements governing information sharing within the DHS. The current Memorandum of Understanding (MOU) was created before the establishment of agencies like ODNI and the NCTC, rendering it ineffective for addressing the current threat landscape. Without clear guidance and updated agreements, the DHS is unable to cope with the evolving threats. It is imperative that the DHS, along with relevant federal partners, undertake a comprehensive review and update of these

[88] Purnell, E. (2022). The American right to privacy: Legacies of the 1975 Church Committee in U.S. public memory (1976–2021) (Doctoral dissertation, Carnegie Mellon University).

agreements to reflect current priorities and responsibilities in counterterrorism information sharing.

The DHS Intelligence Enterprise faces internal challenges that hinder its ability to share intelligence with the Intelligence Community (IC). The lack of cohesion between I&A and other intelligence programs within DHS hampers intelligence reporting and coordination. Additionally, the shortage of field staff and difficulties accessing classified systems further hinder the DHS's ability to gather and disseminate intelligence effectively (Homeland Security Advisory Council, 2023, March 16)[89]. To address these challenges, the DHS should prioritize efforts to enhance cohesion and coordination within its Intelligence Enterprise, ensuring that all components work together seamlessly to fulfill their mission of safeguarding the nation against terrorist threats.

At the local and state levels, fusion centers play a key role in counterterrorism efforts. Fusion centers serve a dual purpose, functioning not only to help prevent terrorist attacks but also to support the response to such incidents (U.S. DOJ OIG, 2017)[90]. However, these centers often face challenges due to unpredictable federal support and varying requirements for security clearances. This lack of consistency, together with the tendency of participating agencies to prioritize their own missions rather than collective efforts (U.S. DOJ OIG, 2017)[91], can hinder fusion centers' access to classified information and impede their ability to contribute effectively to counterterrorism efforts. To overcome these challenges, the DHS and other federal agencies should prioritize consistent support to fusion centers and streamline security clearance processes to facilitate information sharing at all levels of government (U.S. Government Accountability Office, 2023)[92]. By tackling these obstacles, the DHS can strengthen its ability to gather, analyze, and share intelligence, thereby enhancing national security and safeguarding citizens from future terrorist threats. Building on this diagnosis, Section 6 evaluates how to address these challenges through theory-informed reform.

5. Theory-Informed Normative Analysis and Policy Reform

5.1 Theoretical Underpinnings of Surveillance and Privacy

The theoretical understanding of surveillance and privacy protection explores how different theories explain the need to balance government security measures with individual rights in a democratic society. In the present study, the Foreign

[89] Homeland Security Advisory Council. (2023). Intelligence and information sharing: Final report. https://www.dhs.gov/sites/default/files/2023-03/Intelligence%20and%20Information%20Sharing%20Final%20Report%2003162023.pdf

[90] U.S. Department of Justice Office of Inspector General [U.S. DOJ OIG]. (2017, March 30). Review of domestic sharing of counterterrorism information (Report No. OIG-17-49).

[91] ibid

[92] U.S. Government Accountability Office. (2023, June 26). Counterterrorism: Action needed to further develop the information sharing environment (GAO-23-105310).

Intelligence Surveillance Court (FISC), operating under the provisions of the Foreign Intelligence Surveillance Act (FISA), addresses issues and applications related to foreign intelligence surveillance. Federal agencies, particularly the NSA and the FBI, conduct surveillance to ensure domestic and national security by following the FISA process, which requires submitting detailed applications to the FISC outlining the target, purpose, and legal justifications for surveillance requests. Permission is granted only when judges find probable cause to believe that the target is a foreign agent or foreign power, balancing national security needs with individual privacy rights. Although the court process is conducted *ex parte* and in a highly secret manner, it plays a key role in safeguarding against potential abuses of surveillance powers by the agencies.

This operational logic reflects the Security–Liberty Dilemma Theory, which argues that democratic governments must balance protecting the nation and safeguarding civil liberties, especially in times of heightened security threats (Waldron, 2003; Zedner, 2005)[93]. After major security crises such as 9/11, surveillance powers tend to expand, often shifting the balance toward security at the expense of individual rights. The *ex parte* and secret nature of FISC proceedings illustrates this dilemma: secrecy is justified in the name of national security. However, it simultaneously raises constitutional concerns about transparency and due process. Surveillance is widely considered essential to preventing terrorism, espionage, cyberattacks, and transnational crime. For example, counterterrorism investigations often rely on electronic surveillance to identify foreign agents or domestic extremists before they commit harmful acts. However, during periods of heightened security concerns, government surveillance powers may expand, potentially eroding transparency and privacy protections. Following the September 11 attacks, the USA PATRIOT Act (2001)[94] and later Section 702 of the FISA Amendments Act expanded surveillance authority to improve national security response capability. This theory explains why surveillance systems like FISA and FISC are maintained as necessary tools despite concerns about individual rights.

Although the Department of Homeland Security (DHS) plays a significant role in counterterrorism and domestic threat prevention, it does not submit applications directly to the FISC. Instead, it relies on the NSA and DOJ for intelligence collection. This institutional arrangement aligns with Security Governance Theory, which emphasizes that in modern states, national security is decentralized across multiple agencies (Krahmann, 2003)[95]. However, such fragmentation often

[93] Waldron, J. (2003). Security and liberty: The image of balance. Journal of Political Philosophy, 11(2), 191–210. https://doi.org/10.1111/1467-9760.00174
[94] The USA PATRIOT Act: Preserving life and liberty. (2001). U.S. Department of Justice. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf
[95] ibid

creates inter-agency dependency and delays, limiting DHS's proactive threat response capacity. While agencies like the NSA conduct electronic surveillance to identify foreign threats, DHS is responsible for preventing threats within the U.S. homeland, including those targeting transportation, borders, and critical infrastructure. DHS's access to surveillance information is limited because it cannot apply to FISC for warrants and must depend on interagency intelligence-sharing mechanisms. These structural limitations may slow the response to threats. Security Governance Theory supports examining reforms, such as a DHS-led intelligence-sharing platform, to improve operational coordination within the Intelligence Community without undermining lawful surveillance practices.

Despite efforts by FISA and FISC to strike a reasonable balance between national security and privacy, both institutions face enduring criticism. Civil libertarians argue that the lack of transparency undermines public trust and accountability. Critics highlight warrantless wiretapping (Patel & Koreh, 2021)[96], bulk metadata collection (Sommer, 2014)[97], and mass surveillance programs as violations of civil liberties (Baker, 2010)[98]. Such practices reflect the dangers identified by Foucault's Surveillance Theory, warning that surveillance systems can become tools for institutional domination and unchecked power rather than purely instruments of public safety (Foucault, 1977)[99]. Foucault suggests that surveillance functions not only as a security tool but also as a mechanism for social control by concentrating informational power within select institutions. In the U.S. context, agencies like the NSA possess extensive access to surveillance data through programs such as PRISM, while DHS must rely on external sharing arrangements. This creates asymmetry in operational capability and institutional influence. Foucault's perspective does not argue against surveillance; instead, it highlights the importance of fairly distributing access among the agencies responsible for national security while maintaining oversight to prevent the concentration of authority.

The approval rate for FISC surveillance warrants is extremely high, raising concerns about whether true judicial scrutiny takes place. This criticism is grounded in Accountability Theory, which stresses that institutions exercising controlled power must be subject to meaningful oversight (Bovens, 2007)[100]. Because surveillance involves access to personal communications and sensitive information, oversight mechanisms are essential to prevent misuse. Judicial review by FISC, congressional reporting under 50 U.S.C. §1871, and Inspector General audits are designed to promote accountability. However, the absence of

[96] ibid
[97] Sommer, J. (2014). FISA authority and blanket surveillance: Gatekeeper without opposition. Litigation, 40(4), 40–46.
[98] Baker, S. (2010). Skating on stilts. Hoover Institution Press.
[99] Foucault, M. (1977). Discipline and punish: The birth of the prison (A. Sheridan, Trans.). Pantheon Books.
[100] ibid

adversarial judicial proceedings and the lack of an opposing party in FISA hearings create a structural imbalance that undermines judicial neutrality (Chin, 2021)[101]. Even though the USA Freedom Act of 2015 introduced *amicus curiae* provisions, these safeguards remain underutilized (Patel & Koreh, 2021)[102], weakening mechanisms intended to protect constitutional rights. Patel and Koreh (2021) further note that *amicus curiae* briefs are not consistently disclosed, hindering the public's access to the full arguments presented by *amici* to the court. Strengthening these mechanisms through mandatory *amicus curiae* participation or structured transparency protocols could reinforce institutional accountability without jeopardizing operational secrecy.

Furthermore, Social Contract Theory argues that government authority is legitimate only when it upholds citizens' rights in exchange for public consent (Locke, 1689/1988; Rousseau, 1762/1973)[103]. The rise of secret surveillance and cases of past abuse, such as the FBI's COINTELPRO and the NSA's warrantless wiretapping, arguably violates this very foundational democratic principle. Critics argue that without transparency and judicial independence, FISA threatens constitutional democracy rather than protecting it. Some scholars even question whether FISC functions as a court at all, given its one-sided proceedings and lack of public hearings (Chin, 2021)[104]. Mayer (2002)[105] famously framed this debate as whether FISC acts as a "watchdog or a lapdog." Although the Freedom Act of 2015 incorporated the *amicus curiae* provision to enhance public trust, most cases have gone unattended, and the lack of consistent disclosure continues to erode confidence in the system. In this context, surveillance is not inherently incompatible with the right of privacy if conducted within constitutional and legal limits. FISA was enacted in 1978 to establish such limits after earlier unauthorized surveillance operations raised public concern. Judicial oversight by the FISC is intended to ensure that surveillance remains lawful, although debates continue over whether secrecy may affect accountability. In the case of DHS, while it plays a major role in national security, it lacks independent surveillance authority and relies on shared intelligence from agencies such as the NSA and the FBI. Social Contract Theory helps explain why surveillance authority must be balanced with the right of privacy as a safeguard that maintains public confidence in government institutions.

Taken together, these five theories — Security–Liberty Dilemma, Social Contract, Security Governance, Accountability, and Surveillance — provide a comprehensive framework for evaluating the legal, institutional, and normative

[101] Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. Yale Law Journal, 131(2), 655–725.
[102] ibid
[103] ibid
[104] ibid
[105] ibid

dimensions of U.S. surveillance policy. They reveal that while FISA and FISC are designed to protect national security within constitutional bounds, they face persistent challenges related to transparency, accountability, and institutional equity. Addressing these challenges requires not only legal reform and interagency coordination but also a renewed commitment to democratic principles and public trust. These lenses also point in different directions, and the differences matter for the analysis. Waldron (2003)[106] warns that the language of "balancing" can conceal real losses of liberty, while Dinh and Keefer (2006)[107] treat the post-9/11 expansions as proportionate responses to genuine threats; Foucault's account is skeptical of surveillance institutions as such, whereas accountability theory accepts them on the condition that oversight actually works. This study takes the middle position that the doctrinal record best supports: surveillance under FISA is constitutionally tolerable, but only when its oversight mechanisms are real rather than formal—which is precisely what the FISC's *ex parte* structure and its underused *amicus* provisions call into question (Chin, 2021; Patel & Koreh, 2021)[108].

5.2. Constitutionally Grounded Policy Options and Recommendations

In the ongoing dilemma to uphold both national security and individual privacy rights, the DHS and the FISC should strive to strike a careful balance and adopt assertive strategies to overcome their current challenges. The following measures may be considered:

Before turning to the individual proposals, their constitutional foundations should be made explicit. Any reform in this area must respect three doctrinal boundaries. First, Article III: because the FISC is staffed by Article III judges but normally operates without adverse parties, reforms that introduce adversarial participation—such as expanded *amici curiae* or designated counsel—strengthen rather than weaken the court's constitutional footing (Chin, 2021; Vladeck, 2015)[109], and Congress moved in this direction when RISAA (2024)[110] expanded the use of *amici* and designated counsel in FISC proceedings. Second, the Fourth Amendment: since *United States v. U.S. District Court* (*Keith*) (1972), domestic security surveillance has required prior judicial approval, so any expanded DHS access to surveillance outputs must flow through, not around, the warrant framework. Third, separation of powers: FISA itself was Congress's response to unchecked executive surveillance (Boykin, 2015)[111], so proposals that increase

[106] ibid
[107] ibid
[108] ibid
[109] ibid
[110] Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, 138 Stat. 862 (2024).
[111] Boykin, S. A. (2015). The Foreign Intelligence Surveillance Act and the separation of powers. University of Arkansas at Little Rock Law Review, 38(1), 33–62. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827313

judicial involvement and congressional reporting are consistent with the statute's original design. The proposals below are therefore framed as adjustments within the existing constitutional structure, not departures from it. Table 3 summarizes each proposal, its theoretical basis, and its implementing mechanism. Each proposal is elaborated in the numbered discussion that follows

Table 3. *Reform Proposals, Theoretical Basis, and Implementing Mechanism*

Proposal	Theoretical basis	Implementing legal/institutional mechanism
1. Structured DHS access to FISC surveillance outputs	Security governance (Krahmann, 2003)	Amendment to FISA; classified transmission of relevant orders to the DHS Secretary or Privacy Officer
2. Consolidation of the DHS Intelligence Enterprise	Accountability theory (Bovens, 2007)	Internal DHS reorganization; investment in technology and training
3. DHS-led OCIGS with 2IC liaisons from FBI, NSA, and CIA	Surveillance theory: redistribution of informational power (Foucault, 1977)	Interagency memorandum of understanding under ODNI oversight
4. FISC transparency and limited adversarial review	Accountability theory (Bovens, 2007)	Expanded § 1803(i) amici; classified adversarial hearings before the FISCR
5. Reform of FISC judicial appointments	Separation of powers; accountability	Presidential appointment with Judges Appointment Council consultation (Lindner, 2015)
6. Privacy-enhancing technologies	Security–liberty dilemma (Waldron, 2003)	Legislative standards for technical safeguards in collection and sharing
7. Public engagement and transparency	Accountability; social contract	Reporting obligations; consultation with civil society organizations
8. International cooperation on oversight standards	Security governance (Krahmann, 2003)	Common oversight standards with allied partners
9. Prohibition of identity-based surveillance	Social contract theory (Locke, 1689/1988)	Probable-cause standard enforced through judicial review

Firstly, DHS should seek to gather intelligence by establishing a direct pathway to the FISC, as other federal agencies do. The DHS can request a copy of the previously issued surveillance order, or the FISC can *suo moto* transmit a copy of its surveillance order to the Privacy Officer or the Secretary of the DHS in a classified manner, ensuring they are informed about security threat issues. Moreover, there is potential to amend existing FISA legislation to facilitate the presence of a DHS representative, particularly from I&A or the Privacy Officer, at court sessions to ensure the DHS remains informed about national security threats. This process will provide the DHS with a seamless connection to court proceedings and updated information on threats. This proactive measure will free the DHS from dependence on the NSA or DOJ to access surveillance reports, empowering the department to prepare in advance for potential actions against threats. By adopting this strategy, the DHS can streamline bureaucratic procedures and eliminate unnecessary intermediaries, such as the NSA and DOJ. Additionally, this process will give the DHS a new window to advocate for enhanced transparency from the NSA and DOJ and stronger oversight mechanisms within the FISC, guaranteeing that surveillance activities uphold constitutional principles and undergo rigorous scrutiny. This policy proposal reflects Security Governance Theory, which emphasizes the decentralized nature of modern security institutions and the need for interagency coordination (Krahmann, 2003)[112]. By reducing DHS's dependency on other agencies and

[112] ibid

enhancing its direct access to surveillance information, this strategy addresses fragmentation and improves operational responsiveness.

Secondly, DHS should address internal barriers that hinder its intelligence-sharing capabilities. Inconsistency within the DHS Intelligence Enterprise weakens the agency's effectiveness in gathering and disseminating vital information. To overcome this obstacle, DHS should consolidate its intelligence operations and staff resources and prioritize collaboration among its various components. Investing in cutting-edge technology and comprehensive training programs will further strengthen DHS's intelligence capabilities, enabling the agency to stay ahead of evolving threats. This aligns with Accountability Theory, which stresses that institutions exercising strong power must maintain internal coherence and operational integrity to ensure responsible governance (Bovens, 2007)[113]. Strengthening DHS's internal systems enhances its ability to fulfill its surveillance responsibilities while remaining subject to oversight.

Thirdly, there is a need for structural changes within the DHS's Intelligence and Analysis Division to ensure it remains up to date on intelligence-gathering and sharing processes. Creating an integrated One-stop Center for Intelligence Gathering and Sharing (OCIGS) under DHS leadership would streamline operations and strengthen interagency trust by positioning liaisons from the FBI, CIA, and NSA to enhance coordination, secure communication, and collaborative intelligence efforts (**Figure 3**).

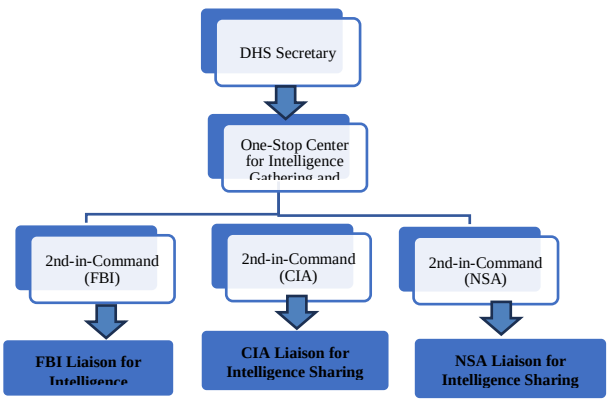


Figure 3: *Integrated Intelligence Gathering and Sharing (OCIGS Model)*

In this scenario, Second-in-Command (2IC) officials from the FBI, NSA, and CIA, with specialized and additional assignments, could be deployed to the newly created center under the leadership of the Secretary of the DHS. This would

[113] ibid

enhance inter-agency coordination and intelligence transmission within the Intelligence Community (IC). Designating high-ranking officials from each agency to oversee intelligence operations would prioritize intelligence sharing efforts across agencies. These 2IC officials would have the authority to ensure efficient communication and coordination. Establishing dedicated liaisons for intelligence sharing among the FBI, NSA, CIA, and DHS would facilitate faster, more secure information exchange. Rather than relying on ad hoc arrangements or bureaucratic channels, direct lines of communication between these key agencies would ensure the prompt and secure sharing of vital intelligence. Moreover, assigning 2IC officials to specific intelligence-sharing tasks underscores the importance of collaboration in addressing national security threats. It signals that intelligence cooperation is a primary consideration in counterterrorism and homeland security efforts. Furthermore, this initiative can help build trust and confidence among IC agencies. Close relationships on intelligence matters can foster mutual respect, expertise, and capabilities, leading to a culture of cooperation and partnership that strengthens overall IC effectiveness. Overall, appointing 2IC officials focused on intelligence gathering and sharing represents a proactive approach to addressing information-sharing challenges within the IC, aiming to enhance national security while protecting individual privacy rights. This proposal is supported by Foucault's Surveillance Theory, which cautions against the concentration of informational power within select institutions (Foucault, 1977). By redistributing surveillance authority and fostering interagency collaboration, this initiative promotes a more balanced and democratic intelligence structure.

Fourthly, FISC should undergo structural reforms to enhance transparency and accountability. The court's secretive proceedings and limited public oversight erode public trust and raise concerns about the fairness of its decisions. To restore confidence, FISC should take measures to increase transparency, such as appointing *amici curiae*, particularly in applications for domestic surveillance, to represent citizen privacy interests. Adversarial but secret proceedings can be allowed during the review hearings in the FISCR and the writ of Certiorari in the Federal Court of Appeal. Additionally, FISC should establish clear guidelines and mandatory reporting requirements for the use of surveillance powers, ensuring they are not abused for political or ideological purposes. These policy proposals are grounded in Accountability Theory, which demands meaningful oversight of institutions wielding coercive authority. Enhancing transparency and adversarial review mechanisms would strengthen judicial neutrality and public trust in FISC's operations.

Fifthly, legislative reform is essential to modernize surveillance laws and establish clear legal standards that balance national security and civil liberties. By

enacting legislation that enhances privacy protections and limits the scope of government surveillance activities, Congress can ensure that surveillance practices are conducted within a framework that respects individual rights. To mitigate the existing challenges in the FISC, there is a need to reform the appointment system for judges to ensure their independence and alleviate any fears they may have while performing their duties. In this case, transitioning to a traditional presidential appointment process with consultation of the Judges Appointment Council (JAC), composed of three senior Justices headed by the Chief Justice of the Supreme Court of the USA, may be a crucial step towards achieving this goal (Lindner, 2015)[114]. This approach would align the appointment process for FISA judges with that of Article III judges, promoting separation of powers and philosophical balance within the judiciary (Lindner, 2015)[115]. Appointing full-time judges with expertise in FISA law can ensure a more robust and effective judicial system that upholds constitutional rights while addressing national security concerns (Lindner, 2015)[116]. Judge John Bates, a former FISC member, raised concerns about the potential consequences of incorporating political considerations into the selection process, emphasizing the risk of creating vacancies that could disrupt court operations and compromise national security (Lindner, 2015)[117]. Judge John also stated that a democratic appointment process is crucial to ensuring transparency and accountability in judicial appointments. Judge John suggests that cooperative political appointments may be a potential solution (Lindner, 2015)[118]. Reforming judicial appointments ensures that surveillance oversight remains legitimate and democratically accountable. The 2024 RISAA shows that incremental legislative reform is achievable; at the same time, its two-year sunset (April 20, 2026) means that Congress soon will revisit Section 702, creating a realistic legislative window for the reforms proposed here (Congressional Research Service, 2025)[119].

Sixthly, it is essential to strike a balance between individual privacy and national security. As there is a continuous debate over private and public space (Baker, 2010)[120], to achieve a proper balance, an attempt should be made to develop privacy-enhancing technologies and encryption tools without compromising intelligence-gathering capabilities. Additionally, policymakers should leverage technological innovations to implement robust safeguards against abuses of power, ensuring that surveillance activities are conducted in a manner that

[114] Lindner, D. (2015). Revisiting the FISA Court appointment process. New York University Journal of Legislation and Public Policy Quorum, 28.
[115] ibid
[116] ibid
[117] ibid
[118] ibid
[119] Congressional Research Service. (2025). FISA Section 702 and the 2024 Reforming Intelligence and Securing America Act (CRS Report No. R48592). https://www.congress.gov/crs-product/R48592
[120] ibid

respects citizens' rights while efficiently confronting security challenges. This proposal reflects the Security–Liberty Dilemma Theory, which emphasizes the need to balance protective surveillance with civil liberties (Waldron, 2003)[121]. Technological safeguards can help recalibrate this balance, ensuring that security measures do not erode constitutional rights.

Seventhly, according to the Homeland Security Advisory Council (2023)[122], meaningful public awareness, engagement, and transparency are essential to fostering trust and accountability in surveillance practices. Government agencies should prioritize transparency by providing precise and accessible information about surveillance activities and compliance measures. Talking to groups such as civil rights organizations and privacy advocates can help policymakers address people's concerns about surveillance and ensure that government oversight is trusted, which is consistent with Accountability Theory, which stresses that public institutions must be transparent and responsive to citizen concerns. Engaging civil society strengthens democratic oversight and reinforces the legitimacy of surveillance practices.

Eighthly, in addition to citizens' cooperation, in the event of international threats from enemies, international cooperation (White House, June 27)[123] is essential for effective oversight of surveillance and intelligence sharing. By working collaboratively with international partners to establish common standards for surveillance oversight and promote respect for human rights, the DHS, in coordination with other federal agencies, particularly the FBI, NSA, and CIA, can enhance collective security while upholding citizens' rights to privacy and freedom of expression. Moreover, strengthened international cooperation (White House, 2023, June 27)[124] can facilitate information-sharing mechanisms that enable DHS and other agencies to address security threats without compromising individual privacy rights. This approach reflects Security Governance Theory, which recognizes that national security is increasingly transnational and requires coordinated governance across borders (Krahmann, 2003)[125]. International collaboration ensures that surveillance practices are harmonized with global human rights standards.

Ninthly, after the 9/11 attacks, the secretive police unit of the NYPD significantly expanded its surveillance efforts, targeting Muslim organizations, mosques, and various activist groups. This has raised concerns about the balance between

[121] ibid
[122] Homeland Security Advisory Council. (2023). Intelligence and information sharing: Final report. https://www.dhs.gov/sites/default/files/2023-03/Intelligence%20and%20Information%20Sharing%20Final%20Report%2003162023.pdf
[123] ibid
[124] ibid
[125] ibid

security measures and civil liberties (Goldstein, 2016)[126]. Surveillance should not be conducted solely on suspicion or on grounds of religion or ethnicity, as it may allow the actual perpetrators to evade detection. It should have probable cause to believe the threat is imminent and that surveillance is required. Following a lawsuit challenging its surveillance practices on Muslims in New Jersey mosques after the September 11, 2001, attacks, the New York Police Department has reached a settlement that it will not conduct surveillance based on religion or ethnicity (Alvarado, 2018)[127]. This development signifies a significant step towards ensuring that law enforcement activities are not rooted in religion and ethnicity, setting a positive example for other police departments across the country to follow a similar path.

This approach is consistent with Social Contract Theory, which holds that governmental authority is legitimate only when it protects the rights of all citizens equally and operates with their consent (Locke, 1689/1988; Rousseau, 1762/1973)[128]. Discriminatory surveillance practices violate this core democratic principle by undermining trust between the state and its citizens. Upholding constitutional protections, such as equal treatment under the law and freedom of religion, is essential to maintaining the legitimacy of surveillance programs. Ensuring that surveillance is based on credible threats rather than identity-based profiling reinforces the social contract and strengthens public confidence in national security institutions.

Finally, the DHS and other federal agencies should work together closely to find a middle ground between national security and civil liberties. It emphasizes the importance of balance, highlighting its essence as maintaining a middle ground rather than veering towards extremes such as overreaching or underachieving, drawing on insights from Baker's (2010) "Skating on Stilts." This requires open communication, mutual respect, and a shared commitment to upholding constitutional principles. By embracing transparency, accountability, modification, and innovation, DHS, FBI, NSA, CIA, NCTC, ODNI, and FISC can navigate the complexities of modern surveillance practices while maintaining civil liberties and constitutional mandates.

6. Conclusion

The Department of Homeland Security (DHS), FISA, and the FISC hold central positions in the United States' framework for balancing national security and individual privacy rights. This article examined a narrower and more consequential problem than the general tension between privacy and national

[126] Goldstein, J. (2016, June 16). Decades-old police surveillance files lead to discovery of the 'mother lode.' The New York Times. https://www.nytimes.com/2016/06/17/nyregion/new-york-police-department-surveillance.html

[127] Alvarado, M. (2018, April 5). NYPD settles lawsuit over spying on Muslims at NJ mosques, schools after 9/11. North Jersey. https://www.northjersey.com/story/news/new-jersey/2018/04/05/nypd-settles-lawsuit-over-spying-muslims-nj-mosques-schools-after-9-11/489725002/

security: DHS bears a central homeland-protection responsibility but remains outside the FISA authorization chain and depends on other agencies for surveillance-derived intelligence. Although concerns regarding secrecy, limited transparency, and structural challenges persist, these institutions remain integral to the nation's intelligence and security apparatus. The study finds that (1) the evolution of FISA has left DHS outside the surveillance-authorization process on which it depends; (2) fragmented agreements, technological incompatibility, internal DHS coordination problems, and agency gatekeeping can impair timely and accountable sharing; and (3) stronger intelligence access and stronger judicial review can be designed together, provided that DHS receives structured access to relevant outputs rather than independent surveillance authority and that access remains subject to minimization, auditing, reporting, and judicial safeguards.

The analysis suggests that the primary challenge lies not in the existence of surveillance authorities but in ensuring that clear safeguards, oversight mechanisms, and interagency coordination accompany such powers. Drawing from established theoretical perspectives, the Security–Liberty Dilemma Theory helps explain the inherent tension between expanding surveillance to address security threats and maintaining civil liberties. Accountability Theory emphasizes the need for institutional checks to prevent misuse of surveillance powers, while Social Contract Theory supports the view that surveillance authority must remain consistent with public consent and constitutional guarantees. Security Governance Theory provides insight into the operational fragmentation among agencies such as the DHS, NSA, and FBI, and Foucault's Surveillance Theory highlights the potential for concentrated state power in the absence of oversight and transparency. The central theoretical contribution of this study is to demonstrate that these five theoretical perspectives collectively suggest that effective intelligence operations and judicial oversight need not be viewed as competing objectives. Rather, the findings indicate that institutional design plays an important role in strengthening both national security and privacy protections.

The legal implications of these findings follow the constitutional boundaries set out in Section 5.2. Because the FISC is staffed by Article III judges, reforms that add adversarial participation strengthen, rather than weaken, the court's constitutional footing. Because the Keith decision requires prior judicial approval for domestic security surveillance, any expanded DHS access to surveillance outputs must operate through the existing warrant framework rather than around it. And because FISA was enacted to check unilateral executive surveillance, reforms that deepen judicial and congressional involvement remain faithful to the statute's original separation-of-powers design.

In light of these frameworks, the strategies presented in this study propose practical steps to strengthen existing mechanisms. Establishing a direct

intelligence-sharing pathway for DHS, enhancing judicial review within FISC proceedings, and updating statutory provisions under FISA could contribute to more efficient and accountable governance. Expanding the role of amicus curiae, allowing limited adversarial participation, and implementing structured transparency measures would reinforce judicial oversight while maintaining operational confidentiality. Similarly, creating a DHS-led One-Stop Intelligence Sharing Center and assigning Second-in-Command (2IC) interagency liaisons could improve coordination, reduce redundancy, and enhance situational awareness across the Intelligence Community.

These reforms may involve administrative adjustments and resource allocation, but their potential to improve coordination and accountability justifies consideration. Integrating privacy-preserving technologies, encouraging measured transparency, and refining oversight mechanisms can strengthen both public trust and operational effectiveness. A balanced approach recognizes that national security and civil liberties are not opposing priorities but complementary aspects of democratic governance.

Enhancing DHS's intelligence role, refining FISC oversight procedures, and recalibrating FISA's legislative framework can support a more accountable and transparent surveillance system. With sustained reform and consistent oversight, it is possible to preserve national security interests while adhering to the constitutional principle of privacy protection.

6.1. Limitations and future research

This study acknowledges its limitations. Due to the sensitive nature of national security and the incumbent restrictions, the FISA Court does not disclose detailed case or surveillance statistics, unlike other US courts. Accordingly, the analysis predominantly relies on secondary sources, declassified materials, and scholarly interpretations. As a result, some institutional processes may not be fully observable, and the qualitative scope of the analysis limits broader generalization beyond the context examined. Future research drawing on access to classified oversight materials, expert interviews, or empirical case studies could offer deeper insight into the practical implications of FISA reform and DHS intelligence operations.