THE SURVEILLANCE STATE EXPANDS: THE POTENTIAL PERVASIVE NATURES OF THE TIKTOK DIVESTITURE LAW, FISA 702, AND THE PATRIOT ACT

ARTUR MIKHLIN, AARYAN PATHAK

ABSTRACT

Recent legislation has, again, raised concerns regarding the First, Fourth, and Fifth Amendment rights of the American people. While the legislation may carry noble intentions, The Protecting Americans from Foreign Adversary Controlled Applications Act (H.R.7521), otherwise referred to as the TikTok Divestiture Law, serves as another building block to the surveillance state of the federal government in the guise of national security, as well as an unreasonable shift in separation of powers. This paper digs into the legislation's language, as well as its implications on personal liberties, in an expansion of broader previous research. This paper argues that this legislation exacerbates the trend of eroding privacy rights and free speech in the modern age. Using a libertarian framework, we explore the incompatibility of personal liberty, the increasing powers of the executive branch, and the legislation at hand. We also explore support for this policy, including direct communication with a key leader in drafting and implementing the bill to provide a well-rounded and nuanced view. The objective of this paper is to advocate for the rollback of overreaching measures found in the PAFACA, the reauthorization of FISA's 702 provision, and the PATRIOT Act. This paper should serve as a blueprint for both the new administration and legislators to restore the right to privacy to the American people.

Table of Contents

I. Background

The delicate balance between personal liberties and national security has historically been tipped in favor of expanding the surveillance state. Even as early as the Sedition Act of 1798,[1] which allowed the executive to criminalize free speech targeted against the government, administrations have usurped unchecked power to infringe upon our First, Fourth, and Fifth Amendment rights. For instance, the Espionage Act, which was signed into law by President Woodrow Wilson in 1917, unconstitutionally imprisoned those outspoken against the United States' involvement in World War I, which was later upheld by the Court in the infamous *Schenck v. United States* (1919) decision.[2] Even beloved American heroes, such as President Abraham Lincoln, suspended the writ of *habeas corpus*, imprisoning many journalists who merely criticized the Union's handling of the Civil War.[3] Though most of these actions curbed free speech and due process rights, we have noticed a broader trend of the federal government encroaching upon the civil liberties of the American people with the same monchar of "national emergency." More recently, in

[1] *Sedition Act of 1798*, ch. 74, 1 Stat. 596 (1798).
[2] *Espionage Act of 1917*, ch. 30, § 3, 40 Stat. 217 (1917) (codified as amended at 18 U.S.C. §§ 792–799); Schenck v. United States, 249 U.S. 47 (1919).
[3] Jordan T. Newport, *Silencing "Sedition": How Abraham Lincoln and John Adams Desecrated the Constitution to Combat Public Reprimand*, 6 Lincoln Mem'l U. L. Rev. (2019).

the aftermath of the horrific September 11 attacks, the Bush administration proposed and implemented the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, more commonly referred to as the USA PATRIOT Act (2001).[4] With immense bipartisan support, the PATRIOT Act granted law enforcement unprecedented access to intercept phone calls, credit card transactions, and even the ability to search private property without a traditional warrant, all in the name of fighting the lackluster War on Terror.[5] Even if the intentions of the Bush administration could be seen as noble, violating fundamental constitutional rights is never justifiable. The commonly cited "Nothing to Hide" argument, which states that a citizen must not to be concerned about surveillance unless they have "something to hide," is fallacious.[6] As time went on, a few provisions of the PATRIOT Act were ruled unconstitutional; however, the surveillance state continues

[4] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[5] American Civil Liberties Union, *Patriot Act: What's at Stake?*, ACLU (2003), https://www.aclu.org/wp-content/uploads/document/patriotactbrochurecolor.pdf.
[6] Alex Abdo, *You May Have Nothing to Hide, But You Still Have Something to Fear*, ACLU (Aug. 2, 2013), https://www.aclu.org/news/national-security/you-may-have-nothing-hide-you-still-have-something-fear#:~:text=August%202%2C%202013,as%20innocent%20until%20proven%20guilty.

to expand, with the intelligence community drastically shifting the Overton window on acceptable practices.[7]

II. Thesis

To these ends, the expansion of federal surveillance through the PATRIOT Act, the more recent Protecting Americans from Foreign Adversary Controlled Applications Act (TikTok Divestiture Law), and the reauthorization of FISA's Section 702 reflect a concerning trend of unconstitutional intrusions and an unjustified increase in executive authority in the name of national security, demanding action to safeguard personal liberties and ensure individual safety in the newfound digital age of America.[8]

---

[7] Anita Ramasastry, *Why the Court Was Right to Declare a USA Patriot Act Provision Dealing with National Security Letter Procedures Unconstitutional,* FindLaw (Oct. 13, 2004), https://supreme.findlaw.com/legal-commentary/why-the-court-was-right-to-declare-a-usa-patriot-act-provision-dealing-with-national-security-letter-procedures-unconstitutional.html.

[8] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); Protecting Americans from Foreign Adversary Controlled Applications Act, S. 139, 117th Cong. (2021); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 702, 92 Stat. 1783, 2438 (1978), as amended by FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, 2438 (2008), and reauthorized by USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 301, 129 Stat. 268, 278 (2015).

III. A Brief Outline of the Paper's Goals and Methodologies

This paper will assess the encroachment of the national surveillance state and expansive presidential power via the proposed TikTok Divestiture Law, the passage of the PATRIOT Act, and the reauthorization of FISA's Section 702.[9] The goal of the paper is to assess the constitutionality of these laws using legal arguments regarding the First, Fourth, and Fifth Amendments.[10] Additionally, the paper uses libertarian theory to support an analysis of existing jurisprudence from an ethical perspective and considers corresponding legal and policy reforms. Upon analyzing the legislative history and plain texts of relevant statutes, evaluating Supreme Court precedents, and consulting secondary sources, a policy-driven mandate is proposed to restore individual privacy and prevent government overreach.

IV. Pre-9/11 Surveillance Framework

The earliest statute prohibiting wiretapping was enacted in California in 1862, soon after telegraphs arrived in the West Coast. In the following decades, federal surveillance laws evolved in step with

[9] *Id*.
[10] U.S. Const. amend. I; amend. IV; amend. V.

technological advancements. In 1967, the Supreme Court ruled in *Katz v. United States*[11] that warrants were required for domestic intelligence surveillance,[12] paving way for the Fourth Amendment protections against unreasonable searches within the scope of electronic communications.

The legal concept of a right to privacy in the United States can be traced back to the seminal 1890 Harvard Law Review article "The Right to Privacy" by Samuel Warren and Louis Brandeis. In this innovative piece, both Brandeis and Warren argued for the recognition of a "right to be let alone" as a fundamental aspect of personal liberty.[13] The article laid the theoretical legal foundation for privacy protections in our jurisprudence system and influenced further legal developments. Ironically, Justice Brandeis would subsequently connect these concepts in his well-known dissent in *Olmstead v. United States* (1928), in which the Court dismissed Fourth Amendment protection for wiretapped telephone conversations since no physical intrusion had occurred.[14] Nearly four decades later, the Court recognized Brandeis' vision when it overturned *Olmstead* in *Katz*, holding that the Fourth Amendment "protects people, not places" and

[11] Katz v. United States, 389 U.S. 347 (1967).
[12] *Id*.
[13] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193 (1890).
[14] Leah Burrows, *To be let alone: Brandeis foresaw privacy problems*, BrandeisNOW (July 24, 2013), https://www.brandeis.edu/now/2013/july/privacy.html.

introducing the "reasonable expectation of privacy" test, which is still central to Fourth Amendment analysis today. This judicial evolution coincided with the Court's decision in *Griswold v. Connecticut* (1965), which explicitly established a constitutional right to privacy by placing it within the "penumbras" and "emanations" of many constitutional amendments, including the Fourth Amendment. Together, these developments translated Brandeis' hypothetical "right to be left alone" into a constitutional doctrine with major ramifications for government monitoring restrictions.

The Warren and Brandeis piece has been widely quoted and analyzed in Supreme Court rulings over the years, becoming, according to one researcher, "one of the most influential essays in the history of American law."[15] Though first rejected in *Olmstead*, Brandeis' privacy paradigm eventually prevailed as technological surveillance capabilities grew, forcing the Court to broaden Fourth Amendment protections beyond physical property. In *Carpenter v. United States* (2018), the Court specifically noted this change, holding that government access to cell phone location data requires a warrant precisely because such technology affords "near-perfect surveillance" capabilities not available in previous

[15] Ben Bratman, *Brandeis & Warren's "The Right to Privacy" and the Birth of the Right to Privacy*, 69 Tenn. L. Rev. 623 (2002).

eras. The Court acknowledged that "old-world legal rules don't automatically apply in the digital age," suggesting that Warren and Brandeis' core findings remain relevant today. This legal trajectory—from the initial definition of privacy rights to their gradual integration into constitutional law—established the pre-9/11 legal framework for constraining government surveillance authority, creating critical tension points that became significant after the September 11 attacks and the subsequent expansion of national security surveillance initiatives.

In the days before the tragic terrorist attacks on September 11th, 2001, the capability of the U.S. federal surveillance system was severely constrained and subject to strict oversight. The main legal framework exercising surveillance activities was the Foreign Intelligence Surveillance Act[16] (FISA) of 1978, which established the policy for physical and

[16] *The Foreign Intelligence Surveillance Act of 1978 (FISA)*, Bureau of Justice Assistance (last visited Jan 21, 2025), https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286.

electronic surveillance of foreign agents[17] and powers. The United States federal government was required to obtain a warrant from the Foreign Intelligence Surveillance Court (FISC) for intelligence gathering operations targeting American citizens.

V. Post-9/11 Expansion

During George W. Bush's presidency, a piece of legislation marked a seismic shift in American surveillance law. The PATRIOT Act was enacted 45 days after 9/11 with very little debate. The legislation broadened the

[17] 50 U.S.C §1801(b) "Agent of a foreign power means—
(1) any person other than a United States person, who— (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; (C) engages in international terrorism or activities in preparation therefore; (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or (2) any person who— (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

authority of the state to access business records, administer "sneak and peek" searches, and share gathered intelligence across federal agencies under Section 215, which enabled the collection of telephone metadata in bulk.[18] Sponsors of the law called it a tool to fight terrorism, yet these provisions were used by the National Security Agency to collect metadata on millions of Americans while weakening Fourth Amendment protections against unreasonable searches even more.[19]

More than a decade later, lawmakers proposed the USA FREEDOM Act (2015), which nominally ended bulk collection, with the requirement of "specific selection terms" for data requests, yet critics argue it preserved loopholes. For example, it allows the FBI to access "business records" through Section 215 with minimal oversight from the judiciary, and it extended provisions such as "roving wiretaps" and "lone wolf" monitoring until 2019.[20] While the intention may have been reform, the FREEDOM Act ultimately expanded normalized surveillance, green-lighting agencies to

[18] Madeleine Carlisle, *How 9/11 Radically Expanded the Power of the U.S. Government*, TIME (Sept. 11, 2021), https://time.com/6096903/september-11-legal-history/.
[19] *PATRIOT Act*, EPIC (Sept. 2, 2020), https://epic.org/issues/surveillance-oversight/patriot-act/
[20] Alex Byers, *USA Freedom Act vs. USA PATRIOT Act*, Politico (May 31, 2015), https://www.politico.com/story/2015/05/usa-freedom-act-vs-usa-patriot-act-118469

mine narrower datasets that still encroach upon the privacy of thousands of Americans.[21]

FISA Section 702, codified in 2008, further cements warrantless surveillance by targeting non-Americans abroad. Its "incidental collection" of communications of American citizens would then be stored in databases queried by the FBI for domestic cases without warrants issued.[22]

The 2023 reauthorization of FISA expanded Section 702 to coerce any U.S. service provider with "access to equipment" transmitting communications to comply, expanding the surveillance net.[23] Despite their claims of a foreign focus, internal FBI audits reveal rampant abuse of Section 702, including queries made by the agency targeting journalists,[24]

---

[21] Richard L. Russo, *A Comparative Analysis of the USA PATRIOT Act of 2001 to the USA FREEDOM Act of 2015: Balancing Security with Liberty* (B.A. thesis, Univ. of Cent. Fla. 2015), https://stars.library.ucf.edu/honorstheses1990-2015/1885.

[22] Caitlin Chin-Rothmann, *Reforming Section 702 of the Foreign Intelligence Surveillance Act for a Digital Landscape*, CSIS (Dec. 8, 2023), https://www.csis.org/analysis/reforming-section-702-foreign-intelligence-surveillance-act-digital-landscape

[23] Greg Nojeim & Silvia Lorenzo Perez, *FISA 702 Expansion: Impact on the EU-U.S. Data Privacy Framework,* Center for Democracy & Technology (July 18, 2024), https://cdt.org/insights/fisa-702-expansion-impact-on-the-eu-u-s-data-privacy-framework/.

[24] William Barr & Dan Coats, *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Submitted by the Attorney General and the Director of National Intelligence 60 (July 2021), https://www.intel.gov/assets/documents/702%20Documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf.

protestors,[25] members of Congress,[26] and ~19,000 donors to a congressional campaign.[27] The Brennan Center for Justice observes that these backdoor searches effectively nullify Fourth Amendment safeguards, enabling dragnet surveillance under the guise of foreign intelligence.[28]

The executive authority over surveillance has vastly expanded through legislative deference and secretive interpretations of statutes, such as Executive Order 12333. Originally signed by President Ronald Reagan in 1981, it permits warrantless monitoring of foreign targets without necessary transparency, permitting agencies like the NSA to collect "netflows" of global internet traffic, including the personal data of American citizens.[29] Following 9/11, the Bush administration used this legal framework for operations such as STELLARWIND, which enabled them to conduct warrantless wiretaps that were eventually legitimized by Congress

---

[25] Privacy & Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 197 (Sept. 28, 2023), https://documents.pclob.gov/prod/Documents/OversightReport/e9e72454-4156-49b9-961a-85570 6216063/2023%20PCLOB%20702%20Report%20(002).pdf.

[26] Rebecca Beitsch, *FBI improperly used Section 702 surveillance powers on US senator*, The Hill (July 21, 2023), https://thehill.com/homenews/administration/4110850-fbi-improperly-used-702-surveillance-powers-on-us-senator/.

[27] Foreign Intelligence Surveillance Court, Memorandum Opinion and Order 29 (Apr. 21, 2022), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.

[28] *Section 702 of FISA: A "Foreign Intelligence" Law Turned Domestic Spying Tool*, Brennan Center for Justice (May 19, 2023), https://www.brennancenter.org/media/10730/download.

[29] Jake Laperruque, *Executive Order 12333: The Spy Power Too Big for Any Legal Limits, Project on Government Oversight*, Project on Government Oversight (Mar. 24, 2022), https://www.pogo.org/analysis/executive-order-12333-the-spy-power-too-big-for-any-legal-limits.

through the FISA amendments.[30] The Court has often deferred to executive claims of "national security," as seen in *Hawaii v. Trump* (2018),[31] which upheld President Donald Trump's travel bans under broad immigration authorities. The FBI's use of Section 702 for domestic queries—without probable cause—exemplifies how executive agencies bypass constitutional checks.

VI. Fifth Amendment Concerns

While the TikTok Divestiture Law raises no Fifth Amendment concerns that haven't been addressed by the Courts,[32] the reauthorization of FISA 702 presents a vast swath of potential constitutional violations, challenging established legal precedent. In the case *Mathews v. Eldridge* (1976),[33] the Court ruled on a due process challenge by an individual, Eldridge, whose Social Security benefits were terminated. Eldridge argued that the Social Security Administration (SSA) violated his Fifth Amendment

[30] *NSA inspector general report on email and internet data collection under Stellar Wind – full document*, The Guardian (June 27, 2013), https://www.theguardian.com/nsa-inspector-general-report-document-data-collection.
[31] Andrew Serwin & Neil Richards, *Who is who, and what do they do? Executive powers over surveillance*, International Association of Privacy Professionals (Jan. 29, 2019), https://iapp.org/news/a/who-is-who-and-what-do-they-do-executive-powers-over-surveillance.
[32] *National Security Update: Court Upholds Divest or Shutdown Order for TikTok*, Debevoise & Plimpton LLP (Dec. 2024), https://www.debevoise.com/insights/publications/2024/12/national-security-update-court-upholds-divest-or.
[33] Mathews v. Eldridge, 424 U.S. 319 (1976).

due process rights as his benefits were prohibited unfairly because he was not provided a prior evidentiary hearing.[34] The Court held that the prohibition of disability benefits does not require a pre-deprivation hearing because pre-existing hearings were sufficient. [35] However, the Court established a *three-part balancing test*[36] to address future related concerns and to determine procedural safeguards that are required for due process. The *three-part balancing test* includes:

1. "The private interest that will be affected by the official action."
2. "The risk of an erroneous deprivation of such interest through the procedures used, and probable value, if any, of additional procedural safeguards."
3. "[T]he Government's interest, including the fiscal and administrative burdens that the additional or substitute procedures would entail."

According to the *Mathews* test, FISA 702 fails to account for necessary procedural safeguards for those whose communications are collected. With regards to the first part of the test, FISA 702 violates a

[34] *Id.*
[35] *Id.*
[36] *Id.*

significant privacy interest: an individual's personal communications. Different from losing disability benefits in *Mathews*, warrantless surveillance can lead to long-term and permanent consequences, which includes critical misuse of personal online data. FISA 702 may also not comply with the second part of the test, as the statute's "incidental collection" presents a potentially high risk that innocent Americans will be surveilled without adequate justification. Unlike *Mathews*, FISA 702 demonstrates no meaningful process for individuals to challenge law enforcement. Lastly, while the government may argue that FISA 702's efficiency justifies national security concerns, *Mathews* establishes that efficiency alone cannot override constitutional due process.[37] Since FISA 702 offers no framework for affected individuals to challenge law enforcement, it deliberately intrudes on constitutional tests established by *Mathews*.

With regards to reasonable judicial oversight, the Supreme Court held in *Boumediene v. Bush* (2008)[38] that Guantanamo Bay detainees have the right to challenge their detention in federal court. The Court asserted that the detainees had the right to file *habeas corpus* petitions, ensuring

[37] *Id*.
[38] Boumediene v. Bush, 553 U.S. 723 (2008).

judicial oversight over law enforcement actions that infringe on civil liberties.[39] Using a similar balancing test found in *Mathews*, the Court weighted the government's national security interest against individual rights to habeas corpus and due process.[40] Similarly, under FISA 702, individual privacy and communication rights are often infringed without any judicial oversight and opportunity to challenge the surveillance measures.[41] *Boumediene* reinforced the Fifth Amendment's Due Process Clause and emphasized the right to contest law enforcement actions that infringe upon personal liberty, including the very unwarranted surveillance practices FISA 702 allows for.

VII. First Amendment Concerns

The First Amendment of the U.S. Constitution plainly states, "Congress shall make no law [...] abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[42] Our Founding Fathers were very intentional with their words. James Madison, the architect of the

[39] *Id*.
[40] *Id*.
[41] *Warrantless Surveillance Under Section 702 of FISA*, ACLU (last visited Mar. 2, 2025), https://www.aclu.org/warrantless-surveillance-under-section-702-of-fisa.
[42] U.S. Const. amend. I

Constitution, spoke on the importance of freedom of speech, asserting, "[I]f we the people are to govern ourselves; we must have these rights even if they are misused by a minority."[43] This view was affirmed in the Supreme Court decision *New York Times Co. v. Sullivan (1964),* in which Justice William J. Brennan Jr. asserted, "Thus we consider this case against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."[44] It does not matter if an American decides to write a blog post or burn the American flag, both actions are protected under the First Amendment. Directly contradicting these founding principles, the PATRIOT Act has eroded not only trust in government but also faith in our free speech protections.[45] For instance, the PATRIOT Act broadens the definition of "material support" for terrorism, which criminalizes mere speech or advocacy that could be interpreted as supporting foreign terrorist organizations, regardless if it

[43] James Madison, *Our First Amendment freedoms give us the right to think what we like and say what we please*, GoodReads (last visited Feb. 3, 2025), https://www.goodreads.com/quotes/11450566-our-first-amendment-freedoms-give-us-the-right-to-think.
[44] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)
[45] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

was done with peaceful intentions.[46] This provision was upheld by the Court in *Holder v. Humanitarian Law Project* (2010),[47] holding that the prohibition of "material support" to foreign terrorist organizations, including merely legal advice on peaceful dispute resolutions, does not violate the First Amendment. However, criminalizing certain speech based only on its content is a gross misunderstanding of what the Framers intended and what *Sullivan* established.

The recently passed TikTok Divestiture Law shows a potential continuation of these same trends. In the recent Supreme Court case *TikTok v. Garland* (2025),[48] the plaintiff argued that the legislation violated their First Amendment rights as the law disproportionately affected communities who use TikTok as a means of expression, mobilization, and organization.[49] This restriction could be viewed as a suppression of speech based on the content of political ideas expressed by the users of the platform. In a unanimous decision, the Supreme Court upheld the law, holding that no First Amendment rights were violated and siding with the

---

[46] *Supreme Court Ruling Criminalizes Speech in Material Support Law Case*, Center for Consitutional Rights (June 21, 2010), https://ccrjustice.org/home/press-center/press-releases/supreme-court-ruling-criminalizes-speech-material-support-law-case.
[47] Holder v. Humanitarian Law Project, 561 U.S. 1 (2010).
[48] TikTok Inc. et al. v. Merrick Garland, 604 U. S. ____ (2025).
[49] Transcript of Oral Argument at 1, United States v. XYZ, No. 24-656 (U.S. Jan. 2024), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2024/24-656_1an2.pdf.

government's position that TikTok's national security threats were legitimate.[50] Additionally, the Court contended that the law was not restricting speech based on content, rather based on the ownership of the platform, a "foreign adversary." Admittedly, while much credible research has been done revealing TikTok's erosive and robust data collection measures, the ultimate choice about whether to use the platform should still rest in the hands of the American people.[51]

When asked about one of his many controversial dissenting opinions, former Supreme Court Justice Antonin Scalia once said, "I'm not king, and I haven't been charged with making the Constitution right all the time."[52] Just as many Americans may resent setting fire to an American flag or the cruelty of TikTok spyware, it may not be up to politicians to play "king" and decide sporadically whether a statute complies with standing doctrine. While the Court ruled that the law did not violate the First Amendment, they made no strong mention of its constitutionality regarding the Fourth Amendment.

---

[50] *TikTok Inc.*, 604 U. S. ____.
[51] Emily Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BuzzFeed News (June 17, 2022), https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.
[52] Hoover Institution, *Uncommon Knowledge with Justice Antonin Scalia*, YouTube (Oct. 30, 2012), https://www.youtube.com/watch?v=DaoLMW5AF4Y.

VIII. Fourth Amendment Concerns

Several significant court cases have brought to light the rapidly evolving landscape of digital surveillance and its constitutional ramifications, shaping the relationship between national security imperatives and individual privacy rights. In *Riley v. California* (2014), the Supreme Court unanimously held that warrantless searches of cell phones consequent to arrest violate the Fourth Amendment, recognizing that modern devices encompass "the privacies of life" and hence require heightened privacy protection.[53] The ruling established a much-needed barrier against unfettered state access to digital data, highlighting that technological evolution necessitates the need to interpret existing constitutional safeguards by applying them to these technological advancements.

Similarly, *Carpenter* extended Fourth Amendment guardrails to historical cell-site location information (CSLI), rejecting the State's claim that such data fell under the "third-party doctrine[54]" and required warrants

[53] Riley v. California, 573 U.S. 373 (2014)

[54] A United States legal doctrine that holds that people who voluntarily give information to third parties—such as banks, phone companies, internet service providers (ISPs), and e-mail servers—have "no reasonable expectation of privacy" in that information. A lack of privacy protection allows the United States government to obtain information from third parties without a legal warrant and without otherwise complying with the Fourth Amendment prohibition against search and seizure without probable cause and a judicial search warrant.

for its acquisition.[55] Together, these rulings establish that digital footprints—whether saved on devices or in the cloud—require strong privacy safeguards, rejecting claims that non-physical possession or third-party sharing undermines constitutional obligations.

Nonetheless, subsequent cases reveal the judiciary's struggle to balance these principles against claims guised in the name of national security. In *FBI v Fazaga* (2022), the Supreme Court prioritized the state secrets privilege over judicial scrutiny of surveillance programs, allowing the state to dismiss claims of religious discrimination in FBI surveillance practices without substantive review. In the case, a covert FBI operation targeted Muslim communities in Southern California, where agents used an informant to infiltrate mosques, record private conversations and collect personal data —including political and religious beliefs — without a warrant.[56] Plaintiffs claimed that this surveillance violated the Fourth Amendment and the Religious Freedom Restoration Act, but the Court concluded that Section 1806(f) of the Foreign Intelligence Surveillance Act

[55] Michael Price, *Carpenter v. United States and the Future Fourth Amendment*, National Association of Criminal Defense Lawyers (Nov. 14, 2023), https://www.nacdl.org/getattachment/1dc6c2eb-56c1-4e96-b7be-7ee8a6c44a70/price_michael_carpenter-v-united_states_june_2018_champion.pdf.
[56] *FBI v. Fazaga*, Global Freedom of Expression (Sept. 12, 2023), https://globalfreedomofexpression.columbia.edu/cases/fbi-v-fazaga/.

(FISA) did not supplant the government's power to use *Reynolds* privilege[57] to dismiss lawsuits.[58] By insulating classified monitoring tactics from judicial review, the decision effectively shielded intelligence agencies from objections to racially or religiously motivated espionage, eroding checks on executive power. This precedent stresses how national security claims can permit discriminatory surveillance, curtailing liberties of free association and worship granted by the First Amendment while expanding the scope of the surveillance state.

Pending before the Ninth Circuit, *United States v. Hunt* (2024) evaluates the applicability of the Fourth Amendment to digital data stored on "abandoned" cell phones. Authorities seized an iPhone left at a crime scene in 2017 yet waited almost three years to search its contents, again without a warrant. In court, they argued that the owner of the iPhone relinquished their right to privacy by losing a physical possession.[59] The American Civil Liberties Union (ACLU) and other data privacy advocates argued that abandoning property does not equate to surrendering a trove of

[57] A legal principle that allows the US executive branch to withhold classified information in civil court cases. This privilege is based on the state secrets privilege, which is a judicially recognized extension of presidential power.
[58] Edward C. Liu, FBI v. Fazaga: Supreme Court Examines Interplay of State Secrets Privilege and the Foreign Intelligence Surveillance Act, Congressional Research Service (Jan. 12, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10683.
[59] *United States v. Hunt*, American Civil Liberties Union (Jun. 5, 2024) https://www.aclu.org/cases/united-states-v-hunt-cell-phone-abandonment.

personal information—photos, location history, emails—stored digitally, which in prior precedent established by *Riley,* deserves heightened protection.[60] A ruling permitting warrantless searches would create a catastrophic loophole, allowing law enforcement to exploit minor lapses in physical possession to access sensitive data indefinitely. This case highlights the urgent need to decouple digital privacy from physical property norms to prevent state overreach.

In a landmark decision, the Eastern District of New York ruled in *U.S. v. Hasbajrami* (2025) that warrantless "backdoor searches" of Americans' communications under FISA Section 702 violated the Fourth Amendment.[61] The case centered on Agron Hasbajrami, a U.S. resident whose emails with foreign targets were collected without a warrant and were later used to secure FISA warrants against him. The state argued that such incidental collection was legal; the Court ultimately held that querying databases for Americans' communications constituted a distinct violation of privacy requiring individualized suspicion.[62] The case marked the first

---

[60] *Id*.
[61] Andrew Crocker, *VICTORY! Federal Court (Finally) Rules Backdoor Searches of 702 Data Unconstitutional*, Electronic Frontier Foundation (Jan. 22, 2025), https://www.eff.org/deeplinks/2025/01/victory-federal-court-finally-rules-backdoor-searches-702-data-unconstitutional.
[62] Court Rules Warrantless Section 702 Searches Violated the Fourth Amendment, American Civil Liberties Union (Jan. 22, 2025) https://www.aclu.org/press-releases/court-rules-warrantless-section-702-searches-violated-the-fourth-amendment.

judicial rejection of the state's "foreign intelligence exception" to warrant requirements for American queries, exposing Section 702's unconstitutionality.[63] The ruling preserved Hasbajrami's conviction under the "good faith" exception, yet it delivered a massive blow to bulk surveillance practices and bolstered arguments for requiring warrants in future cases. The decision highlights the incompatibility of surveillance with constitutional safeguards, illustrating how unchecked executive authority to access private communications ought to be prevented.

James Otis, an early American revolutionary and the man who coined the famous phrase "no taxation without representation," felt strongly about the right of every American to be the sole keepers and decision-makers of their property.[64] Otis writes in his *Writs of Assistance* (1763), "A man's house is his castle; and whilst he is quiet, he is as well guarded as a prince in his castle."[65] Otis effectively conveys the importance of protecting one's personal and valuable property. This, of course, is a sentiment captured by the Fourth Amendment of the United States

[63] Patrick G Eddington, *Federal Court Rules FISA Section 702 "Back Door" Searches Unconstitutional*, CATO Institute (Jan. 22, 2025), https://www.cato.org/blog/federal-court-rules-fisa-section-702-back-door-searches-unconstitutional.
[64] James Otis, *The Rights of the British Colonies Asserted and Proved* (1764).
[65] Writs of Assistance (1763), quoted in James Otis, *The Rights of the British Colonies Asserted and Proved* 21 (1764).

Constitution, which states that Americans are "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[66]

Unfortunately, the enforcement of the PATRIOT Act broke these exact promises, not only destroying our castles but also nabbing the crowns off our princes. Most notably, Section 215 of the Act allows law enforcement to seize "tangible things," such as phone records and internet search history, without requiring any warrant.[67] This violates the precedents set in *Riley* by allowing warrantless seizure of digital records, contradicting the Court's precedent that modern digital data requires increased Fourth Amendment protections. More recently, under the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA) in April 2023, the government extended its ability to practice warrantless surveillance by gathering data involving American citizens under the loose concept of "incidental" collection.[68] In other words, if a U.S. citizen communicates with a foreign adversary under inspection by an intelligence agency, their personal data may be seized as well. Using programs such as Upstream and PRISM, the government can intercept not

[66] U.S. CONST. amend. IV.
[67] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001)
[68] 50 U.S.C. § 1881a (2018); Associated Press, *Biden Signs Reauthorization of Surveillance Program into Law Despite Privacy Concerns*, NPR (Apr. 20, 2024), https://www.npr.org/2024/04/20/1246076114/senate-passes-reauthorization-surveillance-program-fisa.

only communications linked to foreign intelligence but also unrelated data.[69] This violates the recently decided *Hasbajrami* precedent by permitting the warrantless "incidental" collection of data, despite the Second Circuit's ruling that such "incidental" collection raises significant Fourth Amendment concerns when used in criminal prosecutions. While the TikTok Divestiture Law itself does not explicitly grant the government surveillance authority over user data on the application, its parent company, ByteDance, operates out of China, which the United States has deemed a "foreign adversary."[70] This designation raises concerns that executive agencies could potentially stretch the boundaries of the FISA 702 reauthorization alongside the TikTok Divestiture Law to collect "incidental" information from American users that interact with accounts based in China.[71] While national security concerns may justify certain surveillance actions, there needs to be a clear and transparent framework to ensure that incidental data collection doesn't morph into warrantless surveillance of

[69] Grayson Clary, *Another Shot at Challenging Secret Surveillance?* Reporters Committee for Freedom of the Press (Sept. 6, 2022), https://www.rcfp.org/nsa-upstream-surveillance/.
[70] Laura He, *Wait, Is TikTok Really Chinese?*, CNN (Mar. 28, 2024), https://edition.cnn.com/2024/03/18/tech/tiktok-bytedance-china-ownership-intl-hnk/index.html.
[71] Anunay Kulshrestha & Jonathan Mayer, *Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum*, in Proceedings of the 31st USENIX Security Symposium 1705 (Boston, MA: USENIX Association, 2022).

U.S. citizens without proper oversight or judicial review.

IX. Policy Support

The arguments made by those in favor of the TikTok Divestiture Law are grounded and follow a reasonable thought process. David Dorfman, Deputy Staff Director and Chief Counsel for the U.S. House Select Committee on China, as well as a key leader in drafting and implementing the bill, shared multiple counterpoints during a personal interview.[72] Dorfman clearly outlined that the bill was designed to address the critical security threat posed by ByteDance's ownership of TikTok, a looming concern based on reputable and numerous investigations and ByteDance's jurisdiction under the Chinese Communist Party. Furthermore, when questioned about the claim that the law grants the President overreaching powers to decide what country is considered a "foreign adversary," Dorfman highlighted Section 2(g)(4) of the bill,[73] which plainly states that the law applies only to a country specified in section United States Code.[74] In the U.S. Code, "covered countries" include the Russian Federation, People's Republic of China (PRC), the Islamic Republic of Iran, and the

[72]David Dorfman, Personal Communication (Jan. 14, 2025, 5:00 PM EST).
[73] H.R. 7521, 118th Cong. § 2(g)(4) (2024).
[74] 10 U.S.C. § 4872(d)(2).

Democratic People's Republic of Korea (North Korea).[75] In short, the President cannot stretch the definition of "foreign adversary" unless the U.S. Code is changed via legislation passed by Congress. Finally, when asked about concerns regarding the First Amendment, Dorfman highlighted the Supreme Court's unanimous decision in *TikTok v. Garland*.[76] The Court unanimously dismissed ByteDance's claims, concluding, "There is no doubt that, for more than 170 million Americans, TikTok offers a distinctive and expansive outlet for expression, means of engagement, and source of community. But Congress has determined that divestiture is necessary to address its well-supported national security concerns regarding TikTok's data collection practices and relationship with a "foreign adversary."[77] With a concrete statutory definition of "foreign adversary" and a unanimous Court decision, proponents of the bill present a well-crafted case for their proposal.

X. Counterargument

Though the arguments made by Dorfam and many who favor the TikTok Divestiture Law are made in good faith, there is a valid

[75] *Id*.
[76] *TikTok Inc.*, 604 U. S. ____.
[77] *Id*.

counterargument to be made. For instance, while the law indeed delineates what constitutes a "foreign adversary" through U.S Code,[78] the Bill still gives the President unreasonable executive power, undermining the role of the legislative and judicial branch in making credible and equal determinations on such a significant piece of legislation. Most notably, the law allows the President, through the Department of Commerce, to designate certain applications or websites as national security threats; however, the law does not define clear criteria or standard for how an app is to be deemed a threat. While the application must be operated by a "covered company" and controlled by a "foreign adversary," it is worth noting that the law does not provide highly specific or any quantitative criteria for what counts as a "significant threat to national security," leaving room for interpretation.[79] At its worst, the law may allow the President the power to ban apps without a strong justification. Additionally, the law provides no requirement for any judicial oversight, potentially sidestepping due process protections, acting without a court hearing or legislative approval. Ruling on the presidential judgement on national security, the Supreme Court held, "In reviewing the constitutionality of the Act, however, we 'must accord substantial deference to the predictive

[78] 10 U.S.C. § 4872(d)(2).
[79] TikTok Inc. v. Garland, 24 F.4th 1113 (D.C. Cir. 2024).

judgments of Congress' and the Executive regarding national security threats."[80] Essentially, the Court acknowledged that the President's determinations under the law will be upheld unless they are wholly unreasonable. Although the Court made this ruling, the law itself provides no methodical means to accurately assess whether or not the executive overeaches his power. Raising these very concerns, Justice Neil Gorsuch noted, "I worry that litigation over [the various tiers of scrutiny] can sometimes take on a life of its own and do more to obscure than to clarify the ultimate constitutional questions."[81] While Justice Gorsuch concurred in the Court's majority opinion, he still expressed legitimate worry regarding the President's power under the law to be used in unpredictable ways in the future. As such, the question of the law's total constitutionality deserves to be revisited.

Admittedly, while Courts usually defer to the executive branch on national security matters (e.g. *U.S. v. Curtiss Wright Export Corp.*),[82] our increasingly globalized society allows for almost any conflict to fit under the umbrella of foreign affairs. With a staggering 96% of U.S adults using the internet,[83] interaction with individuals from a "foreign adversary" is

[80] *TikTok Inc.*, 604 U. S. ____.
[81] *Id*.
[82] United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936).
[83] *Internet/Broadband Fact Sheet*, Pew Research Center (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

inevitable. Despite the TikTok Divestiture Law not mentioning any regulations regarding individual users who use the platform, there is still legitimate concern with "incidental information" collection on TikTok via FISA 702. While a further extensive inquiry must be completed, data collection from executive agencies still seems plausible, given the dangerous precedent established and exploited by the PATRIOT Act. Therefore, decisions made about national security in our increasingly globalized world ought not to rest solely in the hands of the executive occupying the White House.

XI. Blueprint for Restoring Privacy Rights

A principled approach requires the dismantling of this surveillance architecture through specific steps:

Regardless of First, Fourth, or Fifth Amendment concerns, the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) grants the executive branch unprecedented authority to ban or force the divestiture of foreign-owned applications like TikTok, bypassing traditional checks on presidential power. It is a dangerous legal precedent to allow future presidents to target platforms for ideological or political reasons under the guise of national security. To prevent overreach,

Congress should amend PAFACA to require consent from the Senate—akin to treaty ratification under Article II—for any presidential designation of a "foreign adversary-controlled application." Such a reform would ensure bipartisan scrutiny, uphold constitutionally prescribed separation of powers, and prevent the weaponization of national security claims to suppress free speech. By anchoring this authority in legislative collaboration, the law's noble intent—addressing genuine data privacy risks—can be preserved without sacrificing democratic accountability.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) allows for warrantless "backdoor searches" of U.S. citizens' communications gathered through foreign monitoring programs, a practice recently deemed unconstitutional by a federal court.[84] The Trump administration should respond to this decision by proposing legislation that would codify a warrant requirement for queries incidentally targeting Americans, thereby aligning surveillance techniques with the Fourth Amendment's restriction on unreasonable searches. If Congress fails to act, allowing Section 702 to expire in April 2026 will necessitate a major rethinking of mass surveillance. According to the Electronic Frontier Foundation, warrantless searches of 702 databases occurred 3.4 million

[84] United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019).

times in 2021 alone. Either reform or repeal is required to put an end to this unfettered encroachment.[85]

Key elements of the USA PATRIOT Act, such as Section 215's bulk data collection, have long allowed for widespread surveillance of Americans with no accountability. Congress must opt against reauthorizing these provisions when they expire, restoring the old sunset framework that required periodic review. The Act's broad definitions, such as "domestic terrorism" (which includes nonviolent civil disobedience), have the potential to curb free expression and association. By sunsetting these rules, policymakers can reaffirm the Founders' vision of a government that conducts focused, suspicion-based inquiries. This approach is supported by historical precedent–when Section 215 momentarily lapsed in 2015, no catastrophic security gaps emerged.

XII. Conclusion

The TikTok Divestiture Law presents itself as legislation with noble intentions: to fight looming national security threats curated by nations that appear to be “foreign adversaries.” However, upon close review, the law signals potential encroachment of our First, Fourth, and Fifth Amendment

[85] Crocker, *supra* note 61.

protections. For instance, the banning of social media platforms may intrude on our First Amendment right to free speech, suppressing users' ability to express their opinions, share information, and communicate. Despite the Supreme Court upholding its constitutionality, constitutional concerns regarding the expansive power the law grants to the executive branch remain unresolved. While the definition of "foreign adversary" is strict, the law allows the president to unilaterally decide the fate of every platform covered by the definition that poses a national security threat. Therefore, PAFACA ought to be amended to require approval from the Senate, similar to treaty ratification under Article II of the Constitution.

With respect to the reauthorization of Section 702 of the Foreign Intelligence Surveillance Act, surveillance tools have been misused and abused, violating Fourth Amendment protections against warrantless surveillance of American citizens. This stance was supported by the recent *U.S. v. Hasbajrami*[86] decision; therefore, both the District Court's opinion and a warrant requirement in FISA ought to be codified into law.

Twenty-four years since it was enacted, the USA PATRIOT Act has manifested in unlawful surveillance systems, unnecessary data collection, and infringement upon our constitutional rights. In particular, Section 215

[86] *Hasbajrami*, 945 F.3d 641.

of the Act should be repealed or sunsetted. Many legal statutes defined in the PATRIOT Act ought to be revisited to restore the rights of free association and affiliation for all Americans.

In the twenty-first century, national security interests have been a predominant force in shaping public policy, often leading to legislation that is recklessly passed with minimal debate. While many lawmakers merely intend to safeguard the American people, the means by which they achieve this goal have resulted in an encroachment upon our basic civil liberties. This paper hopes to have changed the Overton window of national surveillance policy, not just for those in the majority, but for those in the minority as well. No matter how well-intentioned a bill may seem, the Constitution remains the supreme law of the land. It is the greatest civic duty for both lawmakers and private citizens to protect the Constitution. Without our Constitution, there is no Republic.