Balancing National Security and Privacy Rights under the U.S. Patriot Act: An Interdisciplinary Approach to Tensions and Solutions

Brandon M. Burke

Old Dominion University

IDS 300W: Interdisciplinary Theories and Concepts

Dr. Pete Baker

December 8, 2024

Abstract

In the aftermath of the September 11 attacks, the U.S. Government enacted the U.S. Patriot Act (USPA), significantly broadening surveillance and law enforcement capabilities in a bid to enhance national security. While the USPA aims to prevent terrorism, its swift implementation has raised profound concerns regarding the erosion of individual privacy rights and civil liberties. This paper investigates the complex interplay between national security and personal privacy, advocating for an interdisciplinary approach that integrates perspectives from information technology, political science, and sociology. By analyzing the legal ramifications, ethical considerations, and societal impacts of the USPA, the study highlights ongoing conflicts and shifting public sentiments regarding government surveillance. It calls for collaborative efforts among experts to create comprehensive policies that balance security imperatives with the protection of civil liberties. Ultimately, this paper underscores the urgent need for adaptive legal frameworks and ethical guidelines that reflect the evolving landscape of surveillance technologies, ensuring that the pursuit of national security does not compromise fundamental individual rights.

Keywords: U.S. Patriot Act, National Security, Privacy Rights

Balancing National Security and Privacy Rights under the U.S. Patriot Act: An Interdisciplinary Approach to Tensions and Solutions

In the wake of the September 11 attacks in 2001, the U.S. Government enacted the U.S. Patriot Act as a sweeping response to perceived threats to national security. This legislation significantly expanded the government's surveillance capabilities and law enforcement powers, aiming to prevent future terrorist acts. However, the rapid implementation of these measures raised critical concerns about the erosion of individual privacy rights and civil liberties. As surveillance technologies advanced, the potential for invasive monitoring of citizens became a pressing issue. This has sparked a robust debate around the balance between ensuring national security and protecting personal freedoms. The challenge of balancing national security with personal privacy rights is multifaceted and requires a nuanced approach that integrates various disciplines. The most prominent disciplines for this issue are information technology, political science, and sociology. Information technology plays a crucial role, as advanced surveillance tools—such as data mining and electronic monitoring—have transformed the landscape of law enforcement and national security. Political science offers a framework for understanding the legal implications of the U.S. Patriot Act, examining how its provisions impact governmental authority and the rule of law. Furthermore, sociology provides vital insights into the ethical dimensions surrounding privacy and public trust, questioning how surveillance affects societal norms and individual behaviors. As citizens are increasingly aware of the tension between security measures and their right to privacy, it begs the question: how should national security measures associated with the U.S. Patriot Act be balanced by individual privacy rights? To address this question, it is essential to first understand what the U.S. Patriot Act entails and the ways in which it affects privacy and security.

To understand why an interdisciplinary approach is required for balance, one must understand and conduct an analysis on what the U.S. Patriot Act (USPA) does and how it can erode privacy and how it protects the United States causing the problems and debates we have today. On October 26, 2001, President George W. Bush, signed into law the U.S. Patriot Act (Besthorn, 2008). The USPA has three primary impacts on civil protections. The first places the guaranteed 1st Amendment right of free speech and association in jeopardy by creating a new crime of domestic terrorism. This effectively allows the federal government to label any individual or political group as a domestic terrorist if they are seen as a threat to public order, suspected of promoting terrorist activities, or even if they hold controversial views that conflict with the current administration's policies (Besthorn, 2008). Secondly, the USPA grants all branches of law enforcement increased powers of surveillance. This allows the U.S. Government to monitor all email and internet activity, conduct covert searches without probable cause or court approval, and compel third parties to reveal sensitive personal information, including private records from doctors, social workers, educational institutions, libraries, hospitals, social service agencies, insurance companies, or any businesses (Besthorn, 2008). Finally, the USPA erodes due process rights of non-citizens by permitting federal authorities to arrest foreign nationals, subject them to mandatory protective detention, and even deport them if their political activities are suspected of being terrorist-related (Besthorn, 2008). However, these surveillance programs and arrests increase national security protecting Americans from harm, thus preventing large scale terrorist attacks from occurring on U.S. soil.

National security advocates argue that enhanced surveillance powers are necessary to protect the country from the ever-present threat of terrorism. These proponents highlight the effectiveness of the USPA in enabling law enforcement agencies to thwart terrorist plots, track

criminal networks, and monitor suspicious activities through advanced technologies like data mining and surveillance tools. According to Garlinger (2009), the use of national security letters and surveillance powers has been credited with preventing 54 terrorist attacks since the September 11 attacks, offering a compelling justification for these expanded powers. To find a solution, an interdisciplinary approach that incorporates the expertise of information technology, political science, and sociology is necessary.

To solve the ongoing problem of balancing national security and privacy under the USPA, it requires an interdisciplinary approach from multiple disciplines. As noted earlier, information technology, political science, and sociology are the foremost disciplines to tackle this issue and create insights as each offers a unique lens through which the complex dynamics of national security and privacy can be understood. However, with these unique lenses, conflicts arise, preventing a comprehensive solution from being developed. Technological advancements may outpace the legal and ethical frameworks needed to regulate them, while political actors may prioritize security concerns over privacy, resulting in policies that undermine public trust. Furthermore, the rapid evolution of digital tools, surveillance methods, and data analytics presents new challenges that were not fully anticipated when the Patriot Act was passed, raising concerns about the adequacy of the law's provisions in addressing emerging threats. As technology advances, new forms of data collection—such as real-time location tracking, facial recognition, and artificial intelligence-driven analytics—create unprecedented opportunities for government surveillance. For example, shortly after the September 11 attacks and the USPA was passed, the FBI began using a computer program called the Key Logger System (KLS). One of the most controversial applications of such technologies can be seen in the case of Nicodemo

Scarfo, where government surveillance programs were used in ways that raised significant ethical questions.

KLS was used to violate civil liberties in the case and conviction of Nicodemo Scarfo. Officials installed the KLS program on his computer and covertly monitored his keystrokes capturing passwords to the accounts Scarfo owned (Etzioni, 2005). This was later used in court to prove that Scarfo was committing crimes such as racketeering. Scarfo's legal team tried to suppress the evidence, since it was unlawful obtained, but it was denied in court. Lawmakers and political scientists did not explicitly state that such programs could be used under the USPA, but it was implicitly interpreted that the FBI could use this program and other information technology to gather intelligence for the sake of national security (Etzioni, 2005). After hearing the case, sociologists began seeing changes in citizen behavior towards the approval of governmental actions. According to Westin, "a survey done shortly after 9/11 recorded very high public approval of new governmental investigative powers … 93% approved expanded undercover activities [and surveillance programs] in suspected groups" (2003). However, in 2002, support for law enforcement monitoring of Internet forums fell to 42% and support for government monitoring of cell phones and email fell to 32% (Westin, 2003). This is just one example of many conflicts that have risen from the passing of the USPA. The rapid evolution of surveillance technologies, coupled with shifting public attitudes and evolving legal interpretations, underscores the necessity for an interdisciplinary approach to address the tension between national security and privacy. Only through collaboration among experts in technology, political science, and sociology can comprehensive solutions be developed that balance security needs with the protection of civil liberties, ensuring that policies are both effective and ethically

sound. Building upon these examples, we can now explore how information technology, political science, and sociology continue to play a significant role in this ongoing debate.

In the field of information technology, the debate over national security and privacy is highly divisive. Advocates for national security argue that strong measures, such as those outlined in the U.S. Patriot Act (USPA), are essential for safeguarding the country from terrorist threats and ensuring public safety. The USPA enhances government powers, enabling it to intercept internet traffic and combat cybercrime. This expanded authority includes communications networks, which millions of Americans rely on daily for postal services, telephone communication, and internet access (Kerr, 2003). All of these communications serve a common purpose: enabling users to send, receive, and store information. However, they also provide opportunities for criminal activity, as malicious actors can exploit these networks for organized crime, terrorism, and other illicit acts that jeopardize national security (Kerr, 2003). Proponents of the USPA argue that these enhanced surveillance powers are necessary for law enforcement to combat such threats. According to political scientists who support stronger national security measures, the law allows authorities to retrieve electronic communications and customer records without a search warrant if an emergency exists—specifically when there is an imminent threat of death or serious injury (Ebenger, 2008). This applies to a wide range of digital communications, including emails, phone calls, and internet search history, thereby enabling surveillance with fewer restrictions or oversight, which proponents claim is crucial for national security. Furthermore, although the USPA was originally designed to target foreign adversaries, its provisions have been interpreted by some sociologists to extend to U.S. citizens. Since the internet is a global network and many forms of communication transcend national borders, these expanded surveillance powers are sometimes seen as necessary for detecting and

preventing international terrorism—though often at the cost of individual privacy. However, not everyone agrees with the expansive surveillance measures laid out by the USPA. Privacy advocates argue that such measures infringe upon fundamental rights, particularly the right to privacy.

Advocates for privacy and civil liberties in the information technology field argue that measures like the USPA infringe upon fundamental rights, particularly the right to privacy. According to Ebenger, the USPA, specifically under Section 215, undermines several privacy protections provided by the Electronic Communications Privacy Act (2008). The Electronic Communications Privacy Act was designed to protect the privacy of communications while they are being made, in transit, or stored on computers. However, the USPA weakens these protections by allowing the U.S. Government to employ computer programs, such as the Key Logger System, mentioned earlier, and other technological tools to capture data. A notable example is the study of library surveillance, where the U.S. Government monitors who enters and leaves libraries, what books individuals check out, and how library computers are used (Matz, 2008). In this case, the government used software to obtain this data. According to Matz, Section 215 has expanded government surveillance to include access to library records, which undermines public trust. As a result, citizens may become increasingly reluctant to engage in everyday activities or freely express themselves, knowing their actions could be monitored or recorded (2008). While concerns about privacy are valid, political scientists are also divided on the issue of balancing security and civil liberties under the USPA.

Under the U.S. Patriot Act, political scientists have largely been divided, supporting both national security measures and the protection of privacy rights. According to Garlinger, Congress's unanimous passage of the Patriot Act (USPA) after 9/11 expanded the Federal Bureau

of Investigation's authority to issue national security letters (2009). These national security letters have reportedly helped thwart about 54 terrorist attacks since 9/11. This is viewed as a positive development by many political scientists who favor national security, as it has enabled intelligence agencies to more effectively identify and prevent potential threats, thereby enhancing national security. Additionally, technological tools like CCTV, data mining, and communication surveillance have allowed authorities to detect patterns of terrorist activity that might otherwise have gone unnoticed. When used within the framework of the Patriot Act, these advancements have significantly strengthened law enforcement's ability to track and disrupt terrorist networks, both domestically and internationally. On the contrary, privacy advocates within political science and sociology question the extent to which these measures have been effective or justified.

On the other hand, some political scientists and sociologists advocate for a more privacy-oriented solution. According to U.S. Senator and political scientist Patrick Leahy, current surveillance programs—such as those under the Foreign Intelligence Surveillance Act (FISA) and the U.S. Patriot Act—have expanded too far, infringing on privacy without clear justification or demonstrable effectiveness (2013). Leahy argues that these Acts have only prevented 54 terrorist plots against the United States, while infringing upon the privacy rights of U.S. citizens as more people became aware of their implications (2013). Moreover, Leahy and sociologist Alan Westin agree that public awareness of the Acts' impact on individual privacy is growing. Westin points out that "a survey of Internet users in early 2002 found that 87% were still concerned about privacy," particularly under the U.S. Patriot Act (2003). These concerns highlight a fundamental tension between national security and individual privacy, where political scientists like Leahy emphasize the potential overreach of surveillance measures. They suggest

that the costs to personal freedoms may outweigh the security benefits—and vice versa. In line with these concerns, the U.S. Patriot Act, as noted by Rackow (2002), compromises constitutional rights, particularly the Fourth and First Amendments, by expanding government surveillance powers. Its rushed passage also undermines the balance between national security and civil liberties. From a sociological perspective, Westin's observation reflects the growing public awareness of privacy issues, signaling a societal shift towards questioning the balance between personal rights and government control—an issue that continues to shape the broader political debate on surveillance policy. As we continue to analyze the conflict between national security and privacy, it is clear that there are differing views on the effectiveness and ethics of the USPA. The tension between security and civil liberties is rooted in different interpretations of the Act's provisions.

The conflict between the insights offered by national security proponents and privacy advocates is primarily rooted in differing priorities and interpretations of the U.S. Patriot Act. National security advocates, such as Garlinger (2009), argue that the expansion of surveillance powers under the USPA is necessary for safeguarding public safety and preventing terrorism. They view the trade-off between privacy and security as an acceptable risk, especially in the face of significant threats like terrorism. The prevention of 54 terrorist plots, as cited by Garlinger, serves as evidence that these measures are effective in achieving their intended goal of national security. However, privacy advocates like Patrick Leahy (2013) and sociologists like Alan Westin (2003) challenge the effectiveness and ethical implications of these measures. Leahy critiques the USPA for allowing government surveillance without clear justification, and he highlights the erosion of privacy rights as a consequence of its implementation. This is in direct conflict with the arguments of national security proponents, who see surveillance as a necessary

tool in the fight against terrorism. Furthermore, sociologists like Westin (2003) note the decline in public support for surveillance programs over time, suggesting that the erosion of privacy has led to a shift in societal values. This tension underscores the ethical dilemma between protecting the collective security of the nation and respecting individual freedoms.

Despite the stark differences in perspectives, there exists potential for common ground among the disciplines involved in the discussion of the U.S. Patriot Act (USPA). As the research from each discipline proposes, there are privacy violations that occur under the USPA; however, the USPA does provide some degree of national security against terrorism and crime. To combat this, political scientists, sociologists, and information technology experts must come together to design a framework that incorporates both robust security measures and the protection of civil liberties. As indicated by the research and complications, this can include implementing stronger oversight mechanisms for surveillance programs, establishing clearer definitions of what constitutes "terrorism" to prevent overreach, and ensuring transparency in how personal data is accessed and used by law enforcement agencies. The most recent attempt at creating common ground was the U.S. Freedom Act (USFA) which was passed in 2015. This Act was seen as a solution to some controversial elements of the USPA, particularly the mass surveillance practices that had been widely criticized. The USFA aimed to curb the excesses of the Patriot Act by ending the bulk collection of telephone metadata under Section 215. Rather than allowing the government to indiscriminately collect vast amounts of phone data, the Freedom Act required more targeted and specific warrants for data collection. The USFA also introduced greater transparency and oversight by mandating the declassification of certain government surveillance practices, including some opinions from the Foreign Intelligence Surveillance Court, which had

previously operated in secrecy. In addition, the law placed restrictions on the use of National Security Letters, requiring greater judicial oversight and limiting the use of gag orders.

However, while the USFA addressed specific issues, it did not fully resolve the broader problem of balancing national security and privacy rights. Although the bulk collection of phone metadata was curtailed, other surveillance activities authorized by the USPA—such as the monitoring of foreign communications and internet data—remained largely untouched. The USFA did not address the broader scope of surveillance, meaning intelligence agencies could still collect significant amounts of information without offering meaningful privacy protections under the Patriot Act. A more profound common ground and solution would be to establish a law that takes into account each discipline's issues. For instance, a modification of the Freedom Act could introduce more comprehensive privacy protections that extend beyond telephone metadata to other forms of digital communications, such as emails, internet browsing history, and social media activity. While the Freedom Act curtailed the bulk collection of phone metadata, it still permits the surveillance of foreign communications that may involve U.S. citizens. This creates a potential loophole where U.S. citizens could still be targeted without proper safeguards. A key reform attempted in the Freedom Act was to refine Section 215, which originally allowed the government to collect large amounts of data, including phone metadata, without adequate oversight or individualized suspicion. However, since the Freedom Act lacks specificity in certain areas, it could be further improved by drawing on insights from information technology, political science, and sociology to make Section 215's provisions more narrowly defined and specific. Moreover, there is a need for a clearer framework that ensures both security needs and individual privacy are considered in tandem, with enforceable limits on data collection that protect civil liberties.

A potential improvement to the current balance between national security and privacy under the U.S. Patriot Act would be the development of a new, more nuanced solution that moves beyond the limitations of the U.S. Freedom Act. While the Freedom Act made strides in curbing some of the more controversial aspects of surveillance, such as the bulk collection of phone metadata, it still left significant gaps in privacy protections, particularly in areas like internet communications and social media data. A better solution could involve the creation of a hybrid framework that incorporates the concerns of privacy advocates while maintaining robust security measures. This could include a multi-tiered surveillance authorization process, where requests for surveillance are reviewed by an independent oversight committee comprising legal scholars, privacy experts, and technology professionals to ensure that each request is necessary and proportionate. Additionally, a dynamic "sunset clause" could require regular reviews of surveillance programs to keep pace with technological advancements and changing threats. To address overreach, clearer and more narrowly defined provisions should specify what constitutes "terrorism" to prevent surveillance from targeting nonviolent political activity. These reforms would create a more balanced approach to protecting both national security and individual privacy rights, moving beyond the piecemeal approach of the Freedom Act to provide a more comprehensive and forward-looking solution.

In conclusion, the tension between national security and privacy under the U.S. Patriot Act highlights a complex ethical dilemma that requires a comprehensive, interdisciplinary solution. While the Patriot Act has proven effective in thwarting terrorist plots, it has also raised significant concerns regarding the erosion of civil liberties and the overreach of government surveillance. To address these concerns, a collaborative effort that brings together experts from information technology, political science, and sociology is essential to design policies that strike

a balance between safeguarding national security and protecting individual freedoms. By introducing more stringent oversight, clearer definitions, and periodic reviews, a more ethical and effective framework can be developed—one that both addresses evolving security threats and respects the privacy rights of individuals. Such a framework would ensure that the lessons learned from the past are applied in creating a more secure and just future.

References

Besthorn, F. H. (2008). Post 9-11 Terror Hysteria: Social Work Practice and The US Patriot Act. *Advances in Social Work*, *9*(1), 17–28. https://doi.org/10.18060/169

Ebenger, T. (2008). The USA PATRIOT Act: Implications for Private E-Mail. *Journal of Information Technology & Politics, 4*(4), 47–64. https://doi.org/10.1080/19331680801978759

Etzioni, A. (2005). *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism* (1st ed.). Routledge. https://doi.org/10.4324/9780203997130

Garlinger, P. P. (2009). PRIVACY, FREE SPEECH, AND THE PATRIOT ACT: FIRST AND FOURTH AMENDMENT LIMITS ON NATIONAL SECURITY LETTERS. *New York University Law Review (1950)*, 84(4), 1105. https://odu-primo.hosted.exlibrisgroup.com/permalink/f/1ucqpjv/TN_cdi_proquest_journals_207658470

Kerr, O. S. (2003). Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't. *Northwestern University Law Review*, 97(2), 607. https://doi.org/10.2139/ssrn.317501

Leahy, P. (2013). *Statement of Senator Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee, Hearing on "Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs," July 31, 2013.* https://www.proquest.com/docview/1679098702

Matz, C. (2008). Libraries and the USA PATRIOT Act : Values in Conflict: Ethics and Integrity in Libraries. *Journal of Library Administration, 47*(3–4), 69–87. https://doi.org/10.1080/01930820802186399

Rackow, S. H. (2002). How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations. *University of Pennsylvania Law Review*, *150*(5), 1651–1696. https://doi.org/10.2307/3312949

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453. https://doi.org/10.1111/1540-4560.00072