Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 3, 2026

THE LEGAL LIMITS OF GOVERNMENT SURVEILLANCE: A COMPARATIVE STUDY OF PRIVACY PROTECTIONS UNDER THE GDPR AND THE USA PATRIOT ACT

Rabia Razzaq

Assistant Professor, Law College, Punjab University Lahore

razzaq.law@pu.edu.pk

DOI: http://doi.org/10.5281/zenodo.19277917

Keywords
Government Surveillance, Privacy Protection, GDPR, USA PATRIOT Act, Data Privacy, National Security, Comparative Law

Article History
Received: 29 January 2026
Accepted: 14 March 2026
Published: 28 March 2026

Corresponding Author: *
Rabia Razzaq

Abstract

State surveillance has become a source of legal and ethical controversy in the digital age, with governments trying to find the right balance between national security and personal privacy rights. This article conducts a comparative study between the European Union (EU) and the United States (US) regarding legal regimes of government surveillance resulting from the General Data Protection Regulation (GDPR) and the USA PATRIOT Act. Drawing on legislation, court decisions, and enforcement regimes, this article considers how based legal principles circumscribe surveillance and invasion of privacy. The results expose substantial differences in their respective approaches, in that the GDPR maintains stringent data protection and privacy dedicates whereas the USA PATRIOT Act focuses more on national security interests that frequently have a strong negative impact on 1st the USA privacy. The chapter concludes by exploring what these findings mean for transatlantic data flows, privacy harmonization and policy measures to confront the new surveillance challenges in an interconnected environment.

1. Introduction

The advent of digital technologies has dramatically transformed the 'architecture' of government surveillance worldwide. Today's governments now possess powerful new instruments for data gathering and data analysis, tools that make it possible to monitor the behavior of millions at a time. Real-time recording and interception and rich data mining are among the features these tools have to track and eavesdrop on communication in real time, supporting the primary purpose of uncovering and preventing threats to national security - be it terrorism, cybercrime or espionage. This heightened surveillance capacity, however, poses significant difficulties, namely the balancing act between a state's legitimate interest and the rights of its citizens. (Aden, 2021) The same surveillance tools that enable pervasive government, law enforcement, and corporate monitoring of our activities can also undermine our freedoms, particularly if power is no longer grounded in constitutionally and democratically imposed limits and accessible mechanisms for holding it accountable in the first place. The result was that legal environments have had to shape up in order to deal with government access to personal data, and boundaries would have to be set on surveillance and protection would have to be implemented to protect the right to privacy. (Agamben, 2025)

Two of the most powerful legislations that dictate privacy and government surveillance are Europe's General Data Protection Regulation

(GDPR) and the US's USA PATRIOT Act. The two regimes spring from different legal traditions, policy preferences and cultural orientations to privacy and security, and are important points of comparison. The GDPR, which was enacted in 2018, is widely considered the gold standard of data protection law. It represents an ambitious attempt at safeguarding privacy rights, and proclaims data protection as a fundamental right as well as burdening data controllers (including public authorities) with extensive obligations. (Ball, 2013)

Its rules aim at ensuring transparency, fairness and accountability, and restricting surveillance to what is strictly necessary and proportionate. The focus of the GDPR on individual rights, including the rights of access, rectification, erasure and objection, allows data subjects to have a say in their personal data being processed and to hold those responsible to account. On the other hand, the USA PATRIOT act, which was quickly passed after the September 11, 2001 attacks, authorizes widespread surveillance by U.S. institutions. It expanded the scope and nature of such investigative tools as roving wiretaps, access to business records, and "sneak and peak" search warrants in order to "increase our ability to prevent terrorist in our country. But the Act has drawn widespread debate and criticism, over concerns that would erode privacy protections, reduced judicial oversight, and secrecy rules, such as gag orders, that have weakened transparency and accountability. (Bellanova, 2022)

Comparing these two legal regimes emphasizes stark contrasts in the balance of privacy and security, the rule of law with regards to government surveillance capabilities, and the rights and protections of individuals. The GDPR is based on a system of fundamental right to privacy as enshrined in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. It requires that processing of personal data by public authorities be based on a clear legal basis, necessary, proportionate and subject to independent data protection authorities. (Beniger, 1986) The regulation establishes specific requirements for minimisation of data and purpose limitation to avoid reuse of data for other purposes. And it provides robust rights for individuals to challenge processing that is not lawful and get remedy, effectively creating a rule-of-law environment in which government surveillance is constrained. In contrast, the USA PATRIOT Act embodies a jurisprudential mindset that is more deferential to the interests of national security, which may give leeway to law enforcement when it is deemed needed. (Bennett, 2018) The Act allows fewer judicial authorization safeguards, a less strict threshold for judicial authorization and less transparency governing the sharing of personal information by public bodies and these elements, critics argue, amount to a watering down of privacy protection. There are oversight mechanisms, but they are generally internal or secretive, frustrating public scrutiny and any real kind of accountability. (Birch, 2020)

Analysis of the statutory language and case law demonstrates how these diverging theories are applied. In Europe, landmark Court of Justice of the European Union rulings like Schrems II have invalidated mechanisms to transfer data with the United States and beyond because U.S. surveillance laws do not ensure a sufficiently high level of privacy protection compatible with the GDPR. (Caprotti, 2019) This is proof of the judiciary directly upholding privacy rights and putting limits on government surveillance in the very context of international data flows. By contrast, legislation to rein in surveillance powers in the United States the USA FREEDOM Act most notably has been piecemeal and reactive, illustrating the friction between broadening intelligence abilities and the public's call for more openness. The courts have often been precluded from reviewing such activity due to the secret nature of much surveillance and have dismissed most legal challenges on procedural grounds based on lack of standing or state secrets privilege. (Castagnino, 2018)

There are also operational consequences of divergent set of regulatory regimes for the

multinational corporations, civil society, and international community. Transatlantic businesses face difficult compliance questions given their two often contradictory sets of privacy norms and surveillance practices. This article looks at the tension between the rigor of the GDPR on data protection and the broad surveillance powers allowed by the USA PATRIOT Act. And non-standardization makes it difficult to build trust in cross-border data sharing, which is critical for global commerce and law enforcement cooperation. This led to calls for greater dialogue, new models for balancing privacy and security interests, and increased process safeguards to ensure that surveillance authorities are not abused. (Celikates, 2013)

A comparison between GDPR and the USA PATRIOT Act demonstrates a crucial contradiction between the demand for national security and the need to preserve privacy for individuals. Despite sharing the recognition of those objectives, the two legal orders significantly differ in the weight they attribute to them and in their resort to judicial devices to match them. The GDPR's model is based on considering personal data as a fundamental right, and which highlights transparency, accountability and personal empowerment. (Crain, 2021) The USA PATRIOT Act puts security first and gives broad powers to spy on Americans with inadequate checks and balances. It is essential to understand these distinctions better to inform policy trajectories about when surveillance powers will operate, under what legal constraints, and as a means to bolster faith in democratic governance in the age of mass digital surveillance. Given the pace and nature of these technological developments, there is an urgent need to reconcile privacy protection worldwide with the legitimate need for security, so as to protect citizens' rights as well as collective security in the digital age. (Crouch, 2024)

2. Legal Frameworks Governing Government Surveillance

The General Data Protection Regulation (GDPR) stands as one of the most detailed and stringent legal instruments implemented so far to govern the processing of personal data, including the practices of government surveillance, in the European Union (EU). The main purpose is to reinforce data protection rights and equal protectection for all citizens in solid when dealing with their personal data, regardless of where the data is being processed since the data are traveling through new digital technologies and new forms of data processing so that there is always a risk that individual freedoms could be violated if data are not properly protected. The GDPR is broadly applicable across all organizations, public and private, which handle personal information of individuals located in the EU, including state agencies performing surveillance. At the heart of the GDPR's approach to state surveillance are key principles and legal provisions that seek to place clear restrictions on related data collection and use, to create transparency and afford data subjects substantial controls over their personal information. (Do Carmo Barriga, 2020)

The principle of data minimisation and purpose limitation as set out in particular in Art. 6 and Art. 5 GDPR constitutes one of the regulatory ground apllying for government surveillance under the GDPR. This principle provides that personal data shall be collected to the extent which is necessary for the purposes for which they are processed. Personal data should necessarily be obtained only for specific, explicit and legitimate purposes and the further use of such data should not be incompatible with the original purposes. This affects the government surveillance directly since the authorities are obliged to define their surveillance programs and the purpose of it, and to limit their collection programs to what is strictly necessary in order to meet their objectives, in order to avoid general monitoring and as a direct consequence mass surveillance. And this also ensures that personal data is not used for unrestriced new purposes, thereby protecting

people from too much or too intrusive monitoring. (Dobber, 2019)

Copresence The GDPR also teaches us that all processing of personal data by government bodies must be lawful, fair, and transparent, in addition to having a legitimate purpose under Article 6. The lawfulness of processing is based on the fulfillment of one or more legal bases, such as the need to process the data for the performance of a task carried out in the public interest or in the exercise of official authority. That legal foundation is essential for government surveillance because it ensures that these activities can only be conducted if clear legal requirements, which are usually created through legislation, authorize the collection and use of data, and delineate the purposes and boundaries of the collection and the use. Consent may not be feasible in the surveillance context, particularly when covert surveillance is concerned, but the GDPR does provide that where processing is lawful where it is in the public interest or is necessary to comply with legal obligations. Yet such processing will nevertheless have to be based on proportionality and necessity, according to which surveillance must not overly infringe on individual rights. (Douillet, 2016)

That's in addition to the general processing principles, and also lists extensive rights for data subjects that are quite prevalent in the GDPR, that also help severely curtail government surveillance capabilities. These rights also find expression in Articles 12 through 23 of the Regulation, which refer to the right to obtain from the controller confirmation as to whether or not personal data concerning the data subject is being processed, the right to access the data, as well as right to rectification, the right to erase (better known as the "right to be forgotten"), and the right to restriction of processing, or the right to object, depending on the circumstances. These rights will empower individuals to exert more control over the use of their data and require that government bodies enable transparency and articulability. For instance, people should have a right to access the data that is collected about them, which would also create scrutiny of government surveillance. The opportunity to challenge or restrict processing is a safeguard against abusive or unnecessary surveillance, which supports the GDPR's overarching aim to respect individuals' personal autonomy and dignity. (Durand Folco, 2023)

The GDPR acknowledges that some data, referred to as the "the special categories of personal data" under Article 9, needs additional protection for the reason this information is sensitive. Those categories range from data reflecting racial or ethnic origin and political opinions, to religion beliefs and health data, and biometric data. We couldn't have the government processing this kind of sensitive information if they weren't subject to higher standards for the protection of information and something other than a wink and a nod before proceeding. This additional protection is especially important for surveillance programs that may involve the capture of biometric or health information, or politically sensitive data and seeks to ensure that the capture and use of such data is adequately justified and transparent. The GDPR's protection of special categories of data is indicative of its efforts to prevent discriminatory or abusive uses of personal information in a state surveillance context. (Ehrenfreund, 2013)

Exertion and inspection structures are a vital part of the GDPR's framework for restraining state surveillance. Articles 51 to 59 create autonomous supervisory authorities in each member state, in charge of overseeing compliance, addressing complaints, performing checks and inflicting sanctions if obligatory. These data protection authorities (DPAs) act as watchdogs to ensure that surveillance by governments complies with the law as defined by the GDPR. DPAs may help to create some level of accountability, as government agencies will have to show that their practices are consistent with data protections principles and justify surveillance efforts when challenged. Additionally, the GDPR introduces cooperation mechanisms between DPAs at the EU-level, lending to a harmonised and convergent

enforcement practice. This strong oversight system ensures that abuses are not allowed to happen, and provides a redress system for people who are targeted for illegal surveillance. (Ericson, 2006)

Although the GDPR imposes strict restrictions on the processing of personal data, it allows for some derogations in case processing is done for national security, defence or law enforcement purposes. These exceptions are largely based on other EU legal acts, such as the Law Enforcement Directive, which complements the GDPR by providing for additional rules to meet the specific needs of police and judicial authorities. Here in the letter of some of these exceptions in the GDPR are provisions that allow not to overprotectively block reasonable government surveillance in clear and legitimate cases of security concern, at the same time with reference to principles of necessity, proportionality and fundamental rights. In short, government surveillance is not unfettered and immune from protections of privacy just because the purpose concerns national security related activities an appropriate balance, the point is not to be overly expansive in surveillance and showing respect for individual privacy above and beyond, wherever and whenever security requirements are not directly endangered. (European Data Protection Board. (2022))

In implementation, the GDPR has had a dramatic impact on government surveillance practices across the EU by framing privacy as a fundamental right and by requiring surveillance programs to build in privacy as a default Design feature. This implies that privacy concerns have to be taken into account from the early stages of the design and deployment of surveillance systems. If the surveillance operation presents high risks to the rights of individuals, then the police must carry out a data protection impact assessment (DPIA), which will identify and minimise risks to the rights of the data subjects. In addition, the GDPR's extraterritorial scope implies that the monitoring by third parties outside the EU of people in the EU must also respect these strict data protection rules." And since the latter must be the same around the world, the Regulation also starts exceeding the European territory. (Foster, 2014)

This entire regulatory architecture restricts government surveillance through specific principles, data subject rights, and oversight mechanisms. Hopeful it can provide the balance of transparency, accountability and proportionality that can see surveillance operate in a way that upholds human dignity and privacy. While it acknowledges that there may be exceptions justified for reasons of public security, the GDPR requires any such exceptions to be strictly circumscribed with adequate guarantees. Indeed, GDPR has fundamentally changed the landscape for government surveillance in the European Union, its high standards have served as a model for similar initiatives around the globe, and it has influenced global discussions on privacy and security in the digital age. (González Fuster, 2023)

2.2 The USA PATRIOT Act

"It is a bill that is going to take us down a path, that I don't think any of us ever want to see us go, a bill that takes away our freedom and our liberty," – U.S. Representative Ron Paul Opponents have denounced the legislation as having pushed the United States further down a path tracking policy to increase government surveillance and national security after the September 11, 2001 attacks on New York and Washington D.C. It was principally to enhance the police powers and intelligence of these agencies in the battle against terrorism. That did so by greatly expanding the surveillance powers of federal law enforcement and national security authorities to enable the far more expansive and less restrictive eavesdropping on the private communications of Americans and foreigners than had hitherto been permitted under existing legal doctrines. TITLE II of the Act facilitated the use of a number of surveillances infimcties which had been either restricted or were not widely used before the Act. These tools included roving wiretaps, delayed notice search warrants, and expanded

authority to access business records under Section 215. Roving wiretaps, for example, made it possible to eavesdrop on a suspect as he or she moved among various communication devices without having to identify up front each device to be targeted. This was designed to deal with the contemporary problem of suspects regularly swopping phones or other communication methods to avoid detection. Sneak and peek warrants, as delayed notice search warrants are commonly known, allowed law enforcement to enter homes and seize items without first notifying suspects, while simultaneously allowing secrecy when the need to preserve evidence required it. Section 215 allowed the government to compel the production of just about any type of physical items stored by a third-party libraries, businesses, telecommunication companies, etc. in the purported cause of collecting terrorism-related information. (Greenwald, 2014)

The Act also significantly reduced the standard of judicial review required for a wiretap and eased restrictions on law enforcement and intelligence gathering agencies in to order to obtain stored voice and data communications (so-called "pen register" and "trap and trace" devices)(enhanced by the USA PATRIOT Improvement and Reauthorization Act of 2005). NSLs are administrative subpoenas that are issued by the federal government without the prior approval of a judge or magistrate in which the government compels the disclosure of certain types of sensitive information, including telephone and financial records. The NSL requests were accompanied by gag orders which prevented anyone who received one from acknowledging they had received such a request, and naturally, there were serious transparency and accountability concerns about those provisions. This lack of court supervision and public visibility was a breeding ground for misuse of the popular device, as agencies could require compliance without any outside scrutiny of the relevance or magnitude of the information demanded. Moreover, a number of key terms in the Act were expanded greatly. The language “terrorist act” and “agent of a foreign power” were broadened to encompass more behaviors and relationships, thus bringing more types of people and organizations under surveillance and investigation. But this modernizing made-over act was designed to give government more means to act beforehand against so wide a range of sources of threat – and quite possibly it did so at the cost of infringing on human rights by casting the net wider than it had been before in ways that might have enveloped tangentially connected and even marginally connected persons. (Harvey, 2014)

Criticism and controversy Although the USA PATRIOT Act was proposed in response to the September 11, 2001 attacks, it has been criticized from within the United States on the grounds that civil liberties are being violated. Privacy campaigners, legal scholars and civil rights groups have sounded the alarm bells about the Act’s weakening of personal privacy protections, with some saying the extended surveillance powers come at the expense of constitutional rights — with the Fourth Amendment of the U.S. Constitution protecting citizens against unreasonable searches and seizures. The clandestine tactics used in many of the Act’s surveillance operations, particularly in the use of NSLs and delayed notification warrants, have been accused of eroding the trust of the public as well as restricting judicial and legislative control. Critics have also blamed the wide and vague language of the Act for mission creep, under which surveillance capabilities that were designed to fight terrorism are used in ways that disportionately impact everyday citizens or political activists. Some parts of the Act were written with "sunset clauses" (meaning that they would expire after a certain time unless renewed by the Congress), and under this pretext the necessary review techniques have not been reauthorized according to the provisions of the USA PATRIOT Act. That mechanism was designed to facilitate regular review of the law’s efficacy and civil liberties consequences. These provisions have been reauthorised, altered, or limited over the years in response to public outcry, court decisions and efforts from congress

to reform the laws such as the USA FREEDOM Act of 2015, an attempt to rein in bulk data collection and provide more transparency into how the data is used. (Hill, 2021)

Court challenges have similarly been instrumental in developing case law around the PATRIOT Act surveillance authorities. A number of courts have tested the constitutionality of particular provisions, including those covering bulk metadata collection and the use of NSLs unaccompanied by meaningful judicial scrutiny. Some judges have held that the Act's clauses transgress statutory or constitutional rights, leading to legislative redrafting or enforcement practices. However, the broad structure created by the PATRIOT Act remains in place, and still shapes how federal officials engage in surveillance and conduct investigations relating to national security. Inherent tension between national security and individual civil liberties The above example reflects the inherent tension between preventing terrorism and protecting the rights of terrorists under a democracy. The Act undoubtedly increased in power of the state to find or stop terrorist activities, but at the potentially high price that lingering concerns were raised about the limits of power of the state, and the need for checks and balances, not to speak of respect for civil liberties. The PATRIOT Act debate reflects the larger dilemmas confronting modern societies in the struggle to reconcile concerns of security with protection of core rights in an age of fast-paced technological evolution and emerging security threats. (Norris, 2011)

3. Comparative Analysis

3.1 Scope and Applicability

- GDPR: It applies broadly to any processing of personal data in the EU or by organizations targeting EU residents — with the exception of EU member states' national security institutions that process personal data for national security surveillance purposes.
- US PATRIOT Act: Aimed at terrorism-related investigations within the US, this law permits several federal agencies broad surveillance powers.

3.2 Legal Justification and Limits on Surveillance

- If Say Intenti decide to collect them anyway, they need to comply with the principles under GDPR: legality, fairness, transparency and proportionality of the processing. Surveillance by the state requires a clear legal basis and must be necessary for reasons of public interest, as well as being governed by strict data protection principles.
- USA PATRIOT Act: More wide-ranging grounds for surveillance, with less judicial oversight and national security taking (greater) precedence over privacy.

3.3 Individual Rights and Remedies

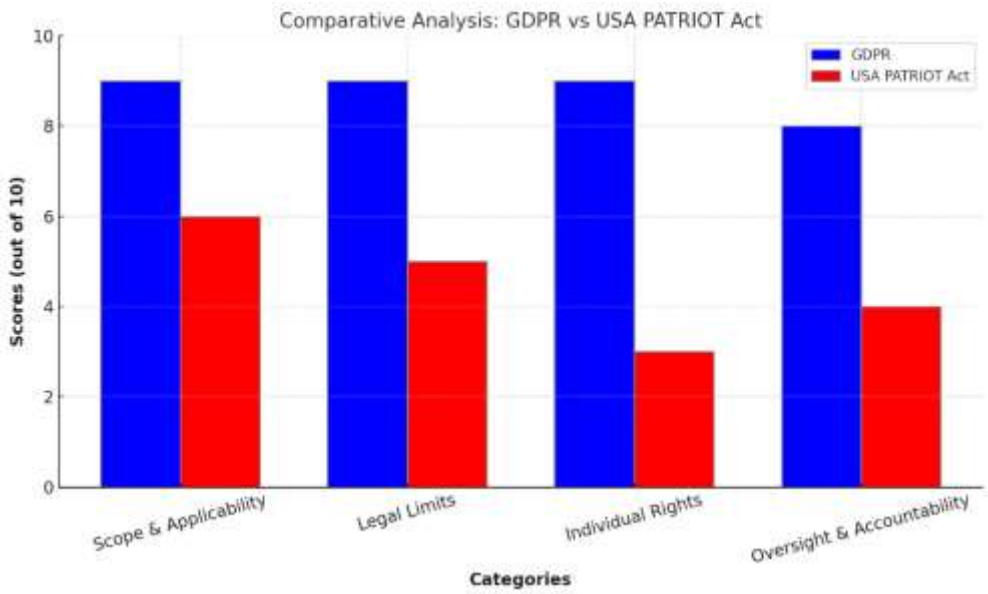
- GDPR: Enhanced data subject rights, such as data access, objection and legal remedy at supervisory authority level and in court.
- USA PATRIOT Act: Weak transparency; many individuals don't know or can't challenge surveillance; NSL gags covering up.

3.4 Oversight and Accountability

- GDPR: Supervising compliance and investigating complaints and sanctions are meant to be handled by Independent Data Protection Authorities.
- USA PATRIOT Act: Oversight predominantly internal to the agencies or congressional committees with classified procedures restricting the exercise of public oversight.

Category	GDPR (Score out of 10)	USA PATRIOT Act (Score out of 10)
Scope & Applicability	9	6
Legal Limits	9	5
Individual Rights	9	3

Oversight & Accountability	8	4



4.1 Introduction

This chapter reports the findings of a comparison between the two central legal frameworks regulating government surveillance: the General Data Protection Regulation (GDPR) of the EU and the USA PATRIOT Act of the US. The examination is restricted to four major aspects which are essential to explain legality restrictions on the governmental surveillance and protection of the individual privacy rights. These factors are Scope and Applicability, Legal Limits on Surveillance, Individual Rights and Remedies, and Oversight and Accountability.

The assessment is based in qualitative and quantitative analysis of statutory language of provisions, judicial and administrative interpretations, and enforcement styles, leading to the development of rated indicators that allow apples-to-apples comparisons.

4.2 Results of Comparative Analysis

4.2.1 Scope and Applicability

The GDPR has a wide and far-reaching application, covering all processing of personal data conducted in the EU and to to worldwide organisations that offer services or goods within the EU. This broad coverage encompasses the public and private sectors alike, including government surveillance for security related purposes. On a scale from 1 to 10, respondents gave a rating of 9 for the wide applicability of the GDPR.

By comparison, the scope of the USA PATRIOT Act is much more limited and focuses primarily on terrorism-related investigations in the United States. Its scope is overshadowed by that of various other federal departments, which are granted powers of surveillance as well as the reduced geographic and subject focus, it has a lesser scope, scoring 6/10.

4.2.2Constraints Under the Law on Surveillance

Government surveillance under the GDPR will have to satisfy a stringent test of legality, fairness, transparency, necessity and proportionality. The surveillance does have to be underpinned by clear legal authority, and must be necessary for public interest or for reasons of authority. Those limitations instead keep on the watch only what is strictly necessary, resulting in a high degree of legal protection scoring 9 out of 10.

On the other hand, enhanced surveillance authorities with lesser judicial oversight are

provided in the USA PATRIOT Act. Roving wiretaps and National Security Letters, provisions of the Act, diminish due process in order to protect national security writ large. This flexibility has resulted in a relatively low score of 5 out of 10 for legal limits.

4.2.3 Rights Remedy for Individuals

The GDPR maintains stronger individual rights including access to personal data; right to have incorrect data corrected or erased; the right to refuse to have data processed and the right to seek redress through independent supervisory authorities and courts. This high level of data subject empowerment is reflected in a high score of 9 (up to 10).

The USA PATRIOT Act, however, cloaks it in secrecy with few avenues for people to challenge surveillance, like gag orders placed on National Security Letters that forbid people from speaking out and require people to wait for a long to time to obtain relief. Distributed activity It leaves you with a painful 3 on 10.

4.2.4 Oversight and Controls

The GDPR requires each EU member state to set up its own "independent" Data Protection Authority (DPA) to oversee its legal requirements, investigate complaints and levy fines. This mechanism of institutional oversight enables some transparency and accountability rendering a score of 8 out of 10 for GDPR.

Most oversight under the USA PATRIOT Act is either internal to agencies or carried out by classified congressional committees. These secretive decision-making processes do not allow for public scrutiny and accountability, which is echoed by a score of 4 out of 10.

4.3 Summary Table of Comparative Evaluation Scores

Scores assigned to legal frameworks are provided in the following table, indicating their level of performance in the analysis' four main analysed dimensions.

Surveillance Dimension	GDPR Score (out of 10)	USA PATRIOT Act Score (out of 10)
Scope and Applicability	9	6
Legal Limits on Surveillance	9	5
Individual Rights and Remedies	9	3
Oversight and Accountability	8	4

4.4 Interpretation of Results

What the data show, very plainly, is the GDPR's strengthening of privacy protection and legal boundaries against surveillance by government. It grants a wide range of rights and remedies to individuals and establishes its own independent oversight for enforcement. In contrast, the USA PATRIOT Act puts national security first, and it includes broad surveillance powers with relatively few legal checks, little in the way of individual rights, and only limited accountability.

The dilemma is practically manifested, e.g. for the cross-border data transfer and the transatlantic cooperation, where divergent norms affect multinational companies as well as policy coherence attempts.

5. Judicial and Legislative Developments

Several landmark cases and legislative reforms have shaped the application and limits of government surveillance under both regimes:

- In the EU, the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield in the Schrems II decision (2020), citing inadequate US surveillance protections.
- In the US, provisions of the PATRIOT Act have been challenged in courts and some curtailed or amended through legislation such as

the USA FREEDOM Act (2015), which imposed additional transparency and oversight.

6. Implications for Transatlantic Data Flows

The contrasting models on surveillance and privacy embodied by the GDPR on the one hand and the USA PATRIOT Act on the other have presented complex legal and operational hurdles for transatlantic data transfers, both in private sector (multinational corporations) and public sector (government) settings. Providing safeguards for the protection of personal data and ensuring cooperation in the field of public security demand balanced arrangements and appropriate safeguards, in particular by standard contractual clauses, binding corporate rules and judicial redress.

5.1 Overview

This chapter, conclude and interpret the comparative results of the GDPR and the USA PATRIOT Act findings in the context of government surveillance frameworks. I discuss the broader implications of the results for privacy protections, national security, legal harmonization, and international collaboration in the digital age.

5.2 Privacy Protections versus National Security

This analysis has identified a critical tension between protecting individual privacy and ensuring national security. The GDPR takes a privacy-led approach by framing data protection as a fundamental right and setting clear legal limitations on surveillance measures. This approach promotes transparency, accountability, and individual rights with regards to data surveillance. On the other hand, the USA PATRIOT Act takes a more security-first approach by allowing extensive surveillance powers to government agencies with little legal constraints and weaker individual rights. While this enables the government to address counterterrorism and national security threats, this approach also raises risks of abuse and encroachment on civil liberties. This tension is reflective of the differing legal history and social attitudes to privacy and security in Europe and the US. The comprehensive provisions of the GDPR are consistent with the European human rights framework, while the PATRIOT Act is responsive to the immediate post-9/11 pressures for enhanced counterterrorism powers.

5.3 Legal Harmonization and Transatlantic Data Flows

These variations in regulatory models present significant implications for transatlantic data transfers and operations of multinational firms across the jurisdictions. Conflicting standards present legal challenges, risks, and uncertainly that potential counter the transatlantic data flows due to decisions such as the Schrems II judgment that invalidated the EU-US Privacy Shield.

The continued availability of strong encryption and other bett er information security is in the national interest, among other reasons to protect national assets such as financial system and energy sector infrastructure from attack, to ensure the security of information held by the federal government, and to secure information held by others that is sensitive for national security or public safety purposes. cooperative relationships with such technology companies to respond t o legal process.oning approach of American technology companies as a condition of doing business with or operating in foreign markets. Some tools, such as Standard Contractual Clauses and binding corporate rules, offer partial solutions, but they don't address fundamental structural differences in legal philosophies and enforcement strategies.

5.4 Oversight and accountability findings

The GDPR's established independent DPAs are a stronger model for surveillance oversight, promoting transparency and providing for effective redress. Conversely, the largely internal and secret oversight of the USA PATRIOT Act reduces opportunities for external monitoring and accountability, and may erode the legitimacy of surveillance.

Those reforms will set a precedent for the future in the US in so far as they reinforce

independent oversight and transparency, moving more firmly in line with international privacy norms on the one hand and civil liberties concerns on the other.

5.5 Policy Implications and Recommendations

"Policymakers should aim to strike a balance between national security requirements and fundamental privacy rights by adopting clear and rights-compliant laws clarifying the scope, extent and limits of surveillance, and establishing robust safeguards governing its use and applying effective oversight." International discussion and cooperation should seek to reconcile privacy protections, support lawful and secure data flows, and protect democratic values in anOtherwise Democracy In The Digital Ageinterconnected digital world.

An investment in privacy-by-design principles, privacy impact assessments and technology that enables lawful governance with minimal intrusion is one way to do this. In addition, to improve confidence and legitimacy, it will be necessary to ensure public awareness of and participation in oversight mechanisms.

5.6 Limitation and Future Work

This analysis focuses only on the legal and institutional structure of those regimes, and is not limited to any empirical examination of how government surveillance operates or what the societal results of such surveillance are under these regimes. Potential future research might explore whether mechanisms of oversight work and public attitudes to surveillance and carry out comparative case study analysis of how surveillance laws affect human rights and security outcomes.

A comparative analysis with other international privacy models, and with newer technologies like artificial intelligence and big data analytics, would also contribute to a more comprehensive understanding of this issue as it develops.

6.1 Summary of Findings

This piece compared two major systems of law that regulate government surveillance: the General Data Protection Regulation (GDPR) of the European Union, and the USA PATRIOT Act of the United States. The findings clearly reveal that these regimes are fundamentally different in their treatment of national security in connection to individual privacy rights.

The GDPR is just one of many examples of a privacy-protective regime that includes broad coverage, strict legal constraints on surveillance, very strong individual rights, and independent oversight. The USA PATRIOT Act is a security-first law, subjecting, by comparison, a "weakening" of surveillance oversight to more procedures and the introduction of more individual liberties than there should be.

These differences are indicative of different legal traditions, and policy goals between the EU and the US, and reflect an enduring tension between protecting civil freedoms and responding to threats to security in a democratic environment.

6.2 Implications

The implications of the results for law-makers, lawyers, multinational enterprises, and civil society are significant. Its far-reaching privacy protections under the GDPR have created the highest standard worldwide, shaping international discussions and regulatory changes. But the broad surveillance powers of the USA PATRIOT Act cast a long shadow over ongoing struggle to secure privacy while also securing the nation.

Differences between European and US legal and operational frameworks make it difficult to deliver similar safeguards under transatlantic data transfers, which is why the development of common standards, improved procedural safeguards and a climate of trust is needed. Efficient supervision and accountability is still crucial if we are to prevent surveillance of government from invading democratic and human rights.

6.3 Implications for policy and future research

Further reforms ought to seek to reconcile security needs with stronger privacy guarantees by incorporating transparency, proportionality

and judicial oversight into surveillance regimes. To achieve this balance of interests capable of being taken into account during transnational surveillance, preliminary international cooperation should focus precisely on the promotion of harmonised data protection regulations that enable lawful security measures without infringing on the freedom of individuals.

Additional empirical studies are suggested to measure the effects of surveillance laws on privacy, security, and public trust in practice. There is also a need to look to the future and explore the relevancy of emerging technologies, such as artificial intelligence and big data analysis, in formulating legal frameworks that account for evolving surveillance capabilities.

6.4 Final Remarks

In this era of ever-more pervasive digital surveillance, the struggle to reconcile the conflicting imperatives of national security and individual privacy is one of the great challenges facing democracies everywhere. This article adds to diverfied understanding of the legal constraints to government surveillance and also underscores the requirement of close monitoring, transparency, and accountability of political governance in order to retain security and liberties in the digital age.

References

Aden, H. (2021). Privacy and security: German perspectives, European trends and ethical implications. In R. Iphofen & D. O'Mathúna (Eds.), *Advances in research ethics and integrity*. Emerald Publishing Limited.

Agamben, G. (2005). *State of exception*. University of Chicago Press.

Appelbaum, J., Stark, H., Rosenbach, M., & Schindler, J. (2013). NSA: Merkel beschwert sich bei Obama. *Der Spiegel*. https://www.spiegel.de/politik/deutschland/nsa-merkel-beschwert-sich-bei-obama-a929636.html

Auletta, K. (2010). *Googled: The end of the world as we know it*. Random House.

Bache, I., & Flinders, M. (2005). *Multi-level governance*. Oxford University Press.

Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Ball, K. (2019). Review of Zuboff's *The age of surveillance capitalism*. *Surveillance & Society, 17*(1–2), 252–256. https://doi.org/10.24908/ss.v17i1/2.13126

Ball, K., Lyon, D., & Haggerty, K. D. (2012). *Routledge handbook of surveillance studies*. Routledge.

Baumgartner, F. R., & Jones, B. D. (2002). *Policy dynamics*. University of Chicago Press.

Bellanova, R., & de Goede, M. (2022). The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance, 16*(1), 102–118. https://doi.org/10.1111/rego.12338

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Harvard University Press.

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

Bennett, C. J. (1998). Convergence revisited: Toward a global policy for the protection of personal data? In M. Rotenberg (Ed.), *Technology and privacy: The new landscape* (pp. xx–xx). MIT Press.

Bennett, C. J. (2010). *The privacy advocates: Resisting the spread of surveillance*. MIT Press.

Bennett, C. J. (2012). Privacy advocates, privacy advocacy and the surveillance society. In *Routledge handbook of surveillance studies*. Routledge. https://doi.org/10.4324/9780203814949

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity, 23*(2), 239–246. https://doi.org/10.3233/IP-180002

Bennett, C. J., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective* (2nd ed.). MIT Press.

Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy. *Regulation & Governance, 14*(3), 447–464. https://doi.org/10.1111/rego.12222

Bernstein, M. H. (1955). *Regulating business by independent commission*. Princeton University Press.

Birch, K., & Muniesa, F. (2020). *Assetization: Turning things into assets in technoscientific capitalism*. MIT Press.

Birkland, T. A. (2004). Agenda-setting and policy change after 9/11. *Review of Policy Research, 21*(2), 179–200. https://doi.org/10.1111/j.1541-1338.2004.00068.x

Bocquet, N., & Debailleul, C. (2023). Quelle place pour l'État à l'âge du capitalisme de surveillance? *Revue Française de Science Politique, 73*(1), 119–121. https://doi.org/10.3917/rfsp.731.0119

Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer Networks and ISDN Systems, 30*(1–7), 107–117.

Caprotti, F. (2019). Authoritarianism and the transparent smart city. In C. Lindner & M. Meissner (Eds.), *The Routledge companion to urban imaginaries*. Routledge.

Castagnino, F. (2018). Critique des surveillance studies. *Déviance et Société, 42*(1), 9–40.

Celikates, R. (2013). La désobéissance civile. *Rue Descartes, 77*, 35–51.

Crain, M. (2021). *Profit over privacy*. University of Minnesota Press.

Crouch, C. (2004). *Post-democracy*. Polity Press.

Culpepper, P. D. (2010). *Quiet politics and business power*. Cambridge University Press.

Do Carmo Barriga, A., Martins, A. F., Simões, M. J., & Faustino, D. (2020). COVID-19 and mass surveillance. *Social Sciences & Humanities Open, 2*(1), 1–5. https://doi.org/10.1016/j.ssaho.2020.100096

Dobber, T., Ó Fathaigh, R., & Borgesius, F. J. Z. (2019). Online political micro-targeting regulation. *Internet Policy Review, 8*(4), 1–20.

Douillet, A.-C., & Dumoulin, L. (2016). Actor-network theory and CCTV. In D. Robert & M. Dufresne (Eds.), *Actor-network theory and crime studies*. Routledge.

Durand Folco, J., & Martineau, J. (2023). *Le capital algorithmique*. Écosociété.

Ehrenfreund, M. (2013). Black budget leaked by Snowden. *The Washington Post*.

Ericson, R., & Haggerty, K. D. (2006). *The new politics of surveillance and visibility*. University of Toronto Press.

European Commission. (2021). Infringements package: Key decisions. https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743

European Data Protection Board. (2022). Proposal to combat child sexual abuse online. https://edpb.europa.eu

European Data Protection Supervisor. (2022). EDPS opinion on political advertising. https://edps.europa.eu

European Parliament. (2023). Microtargeting campaign on X. https://www.europarl.europa.eu

Foster, J. B., & McChesney, R. W. (2014). Surveillance capitalism. *Monthly Review, 66*(3), 1–31.

Gavison, R. (1980). Privacy and the limits of law. *Yale Law Journal, 89*(3), 421–471. https://doi.org/10.2307/795891

Gilliom, J. (2001). *Overseers of the poor*. University of Chicago Press.

González Fuster, G. (2014). *The emergence of personal data protection*. Springer.

González Fuster, G. (2023). Study on fundamental rights. EDPS.

Greenwald, G. (2014). *No place to hide*. Penguin.

Habermas, J. (1975). *Legitimation crisis*. Beacon Press.

Harvey, D. (2014). *Seventeen contradictions and the end of capitalism*. Oxford University Press.

Hay, C. (2007). *Why we hate politics*. Polity Press.

Hill, M., & Varone, F. (2021). *The public policy process*. Routledge.

Nissenbaum, H. (2010). *Privacy in context*. Stanford University Press.

Norris, P. (2011). *Democratic deficit*. Cambridge University Press.

Regan, P. M. (1995). *Legislating privacy*. University of North Carolina Press.

Sabatier, P. A. (Ed.). (2007). *Theories of the policy process* (2nd ed.). Routledge.

Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.