**USA PATRIOT Act**

The [USA PATRIOT Act](https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf), officially known as the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,” was a keystone in the national security enhancement strategy passed by the United States (**US**) Government after the September 11, 2001 terrorist attacks. Its provisions have considerably broadened the surveillance and investigative authorities of federal agencies. It was intended to mitigate future attacks by giving the government broad authorities to track and access communications and financial data across international borders and within the US.[[1]](#footnote-1)

The Act has profound implications for data privacy, particularly in the context of cloud services. It grants US government agencies access to any kind of personal data stored by a US-based cloud provider, no matter the country of origin of the owner or where the data lies. This means that even if a business or individual outside the US chooses a cloud service that operates within the US or has headquarters there, their data could still be subject to scrutiny under the PATRIOT Act.[[2]](#footnote-2)

Sections 215 and 505 of the PATRIOT Act raise concerns for data privacy:

* Section 215 of the Act, often referred to as the “business records” provision, allows federal agencies to request any person or entity to hand over “any tangible things” relevant to a terrorism investigation. This section grants the government broad authority to collect a wide range of business records without requiring a court order. Importantly, according to the original version of the Act, this authority could be used to gather information in bulk, even if the data pertains to individuals not directly under investigation, raising significant concerns about overreach and privacy.
* Section 505 authorises the issuance of National Security Letters (**NSLs**), which are administrative subpoenas that allow federal agencies to demand certain types of records from companies, such as telecommunication firms and internet service providers, without prior judicial approval. Unlike Section 215, NSLs are more targeted but come with a “gag order” that prevents companies from informing individuals about the government's data request. This secrecy adds another layer of concern regarding transparency and the potential misuse of these powers.

The PATRIOT Act is criticised as undermining the ability of other countries to enforce their own data privacy laws, leading to legal complexities and confusion. This has implications for companies that handle sensitive or personal data and must comply with strict data protection regulations, such as the:

* [General Data Protection Regulation (GDPR)](https://gdpr-info.eu/) in the European Union,
* [Personal Data Protection Act (PDPA)](https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act) in Singapore, or
* Russian [Federal Law on Personal Data (152-FZ)](https://www.consultant.ru/document/cons_doc_LAW_61801/).

The PATRIOT Act's provisions may conflict with such legislation.[[3]](#footnote-3)

Additionally, the Act raises ethical concerns about the balance between national security and individual privacy. Public awareness of these issues grew significantly after Edward Snowden's 2013 revelations about the extent of US government surveillance, particularly the bulk data collection under section 215. Snowden's disclosure further turned the public eye to such surveillance powers, eventually followed by legal reforms (the [USA FREEDOM Act](https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.htm) of 2015, which tried to limit some of the more controversial practices). While the USA FREEDOM Act curtails bulk data collection, many of the core provisions affecting cloud hosting, such as access to information stored by US-based providers, remain largely intact. This underlines ongoing ethical concerns of trading off national security against personal privacy, especially to the disadvantage of non-US citizens who are using US-based cloud services.[[4]](#footnote-4)

1. Rackow, S. H., "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, vol. 150, no. 5 (2002), p. 1651 [↑](#footnote-ref-1)
2. David Bender, ‘Privacy and Security Issues in Cloud Computing’ (2012) 29 The Computer & Internet Lawyer <http://link.gale.com/apps/doc/A303642866/AONE?u=anon~5970f3a4&sid=googleScholar&xid=49d89645>  [↑](#footnote-ref-2)
3. Aaronson, S., Data Is Disruptive: Hinrich Foundation White Paper (2021) <https://www.wita.org/wp-content/uploads/2021/08/Data-is-disruptive-Hinrich-Foundation-white-paper-Susan-Aaronson-August-2021.pdf>  [↑](#footnote-ref-3)
4. The Snowden Effect Six Years On (2019) <https://www.justsecurity.org/64464/the-snowden-effect-six-years-on/>  [↑](#footnote-ref-4)