The USA PATRIOT Act and the Use of Cloud Services: Q&A

Enterprises must consider a range of benefits and costs as they evaluate migrating their IT functions and data to cloud-based computing services, including the impact of the cloud services on the security and privacy of their data. In this regard, one of the principal privacy-based concerns raised in connection with US cloud-based services is that the use of such services will afford the US government greater access to the enterprise customer's data, including in particular under the "**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism Act of 2001" (also known as the USA PATRIOT Act or Patriot Act). This concern—which has been prevalent in the press in connection with EU enterprises' use of cloud services—is often based on a misunderstanding of the Patriot Act and the law governing government access to data both in the United States and abroad.

To start, contrary to many popular descriptions of it, the Patriot Act was not itself a vehicle for the US government to access user data, but rather a compilation of amendments to pre-existing federal statutes. These amendments, which have been modified several times since they were first enacted, were a direct response to the September 2001 attacks and were aimed at strengthening the ability of the US government to combat terrorism. The amendments, for example,

- authorized the US government to apply to terrorism matters certain investigative tools that it previously was authorized to use to fight organized crime;
- enhanced the US government's authorities to investigate foreign intelligence surveillance activity to encompass activities of terrorist organizations and other clandestine intelligence activities directed at the US;
- expanded authorities to combat international money laundering and financing of terrorism;
- strengthened US border security and removed barriers for information sharing among US government intelligence and law enforcement agencies, which had contributed to the failure to prevent the 9/11 attacks; and
- streamlined government searches that were already permitted when undertaken pursuant to a valid judicial order. For example, the Act amended federal law to allow a single search warrant to be obtained for disclosure of data held by communications providers in multiple states, instead of having to seek separate search warrants (from separate judges) in those circumstances.

Thus, the Patriot Act did not create the underlying authorities for the US government to access online data. Rather, those authorities already existed in various criminal statutes and procedures.

In addition, the Patriot Act amendments did not provide for unfettered US government access to online data. Rather, to the extent that the amendments applied to online data, they focused on government access to data only for investigations relating to the narrow national security-based purposes of the Act.

Also contrary to many popular descriptions of the Patriot Act, the statutory provisions amended by the Patriot Act remain subject to the protections of the US judicial system. In fact, US law provides multiple levels of privacy protection for data stored in the cloud, and places limitations on the power of the US

government to require cloud providers to disclose their customers' data. These protections are not limited to US citizens; they extend to the data belonging to non-US enterprises that are located outside of the US.

Moreover, the US does not assert jurisdiction over foreign companies or their data any more broadly than many, if not most, other countries, including some European countries. This includes jurisdiction over data stored outside the country.

Finally, an EU enterprise can use cloud services from a US-based provider without impairing the enterprise's ability to comply with the EU Data Protection Directive. If the US-based provider certifies and complies with the EU-US Safe Harbor Agreement and makes appropriate contractual commitments as mandated by the Directive to the EU enterprise, the EU enterprise would be in essentially the same position, from a compliance perspective, as if it stored data in-house.

* * *

1. ***Does US law, including the Patriot Act, allow the US government to obtain access to any information it wants for any purpose?***

   US laws provide multiple levels of privacy protection for individual and enterprise data, including data stored in the cloud. These laws place important limitations on the power of the US government to require cloud providers to disclose their customers' data. Before obtaining data — whether located in the US or overseas — law enforcement must comply with established processes to protect against unfettered governmental access. These protections are not limited to US citizens; they extend to foreign subscribers (including businesses) located outside the US.

2. ***Did the Patriot Act introduce new exposure of foreign companies' data to access by the US government?***

   Approximately ten years ago, long before the creation of cloud services, the US Congress enacted the Patriot Act. Pre-existing federal law authorized the US government to compel disclosure of data to the US government for law enforcement purposes, even if that data was stored outside the United States. The Patriot Act introduced amendments to strengthen the ability of the US government to combat terrorism and clandestine intelligence activities directed at the US. The targeted nature of the Patriot Act means that its data access provisions will not be relevant for the vast majority of cloud customers.

3. ***Is the Patriot Act is the source of the US government's ability to access online data?***

   The Patriot Act was a series of amendments to existing law, including laws that applied to the US government's lawful access to online data. Specifically, in the online context, the principal federal law governing law enforcement's ability to access data and providing privacy protections for the data is the Electronic Communications Privacy Act ("ECPA"). In the United States, online service providers that host data may be subject to compliance with orders under ECPA that are not generally applicable to other businesses. These orders do not change the US government's fundamental ability to access information from enterprise customers, since the government can serve valid process on businesses to get access to data on premises, but they potentially could enable access through an online service provider rather than through the business itself.

4. Did the Patriot Act expand the territorial reach of US law or provide a basis for US cloud service providers to respond to US government requests that might encompass foreign user data?

Long before the Patriot Act was enacted, US courts held that a company with a presence in the United States was obligated to respond to a valid demand for information from the US government – regardless of the location of that information – so long as the company retained "possession, custody or control" of the data.[1] This legal principle, which is not dissimilar to the approach followed by some EU Member States (whose rules permit law enforcement to exercise jurisdiction over data that is "accessible" in-country), has long required companies that have contacts with or a presence in the US to comply with lawful US government requests for information — including EU companies and their data held in the EU.

5. Are US cloud service providers prohibited from notifying users when they receive a request from US law enforcement officials or comply with lawful US process requests?

As a general matter, US providers are not precluded from notifying customers of governmental requests, and can, in most instances, simply direct the governmental request to the customer to afford it the opportunity to determine how to respond. In limited circumstances, such as investigations relating to terrorism or clandestine intelligence activities, which by their very nature are kept secret, service providers may be prohibited by law from notifying users when they receive a request from US law enforcement officials.

6. Are EU cloud service providers able to offer customers a greater level of protection against US government access than US cloud service providers?

The touchstone for US jurisdiction is not where a provider is incorporated, but rather whether it has a presence in, or other sufficient contacts with, the US. Thus, EU cloud service providers that have a presence in the United States are just as susceptible to requests from US law enforcement as US cloud service providers. Given the economies of scale involved in cloud computing, it is reasonable to wonder whether any company that aspires to be a significant cloud service provider could avoid significant contacts with — and the jurisdiction of — the United States. Moreover, all EU cloud providers are subject to compliance requests that result from the use of traditional legal tools such as Mutual Legal Assistance Treaties and court-to-court requests, which enable the US, like many other countries, to access foreign-based information.

7. Could the use of cloud services offered by a US cloud service provider potentially reduce an EU enterprise's ability to comply with the EU's Data Protection Directive?

A number of US cloud service providers abide by the EU-US Safe Harbor Agreement – a formally recognized framework through which US companies can demonstrate that their data protection practices meet the data protection adequacy requirements of the EU's Data Protection Directive and the implementing legislation of the EU Member States. Cloud providers that adhere to the Safe Harbor are obligated to provide adequate privacy protections, as defined under the Directive.

---

[1] This jurisdictional test was most famously articulated in *United States v. Bank of Nova Scotia*, 691 F.2d 1384 (11th Cir. 1982), which is widely regarded as the seminal case addressing when a business subject to U.S. criminal process may be required to disclose information located abroad.

Specific cloud providers can reinforce their Safe Harbor compliance by making appropriate contractual commitments regarding privacy to their EU customers.

8. Would disclosing EU user data to the US government violate the Safe Harbor Agreement between the US and EU?

The Safe Harbor agreement does not supplant, and in fact allows for compliance with, long-standing US laws that authorize the US government to compel any entity that has a presence in the US to turn over information under its control, even if that information is stored outside the United States. Indeed, the Safe Harbor Agreement specifically permits adherence to the Safe Harbor principles to be limited to the extent necessary to meet national security, public interest, or law enforcement requirements.

9. Do US laws, such as the Patriot Act, have a broader extra-territorial reach than the laws of other countries and, therefore, place users of US cloud service providers at greater risk of government access?

While law enforcement in different countries may follow different rules or practices under which they will assert jurisdiction over user data, many, if not most, countries assert jurisdiction very broadly. For example, Belgium has asserted jurisdiction over data held in the US that Belgian law enforcement officials asserted was related to criminals in Belgium; prosecutors in Italy likewise have asserted jurisdiction over data in the US related to their investigations of criminal activities in Italy; and the UK and France have rules that are broad enough to permit data stored in third countries to be seized in certain circumstances.

10. If an EU or other foreign-headquartered company utilizes a US cloud service provider, will its data be more susceptible to access under applicable US laws, including the Patriot Act?

If a company using cloud services has contacts with or a presence in the US, its information may already be susceptible to access by US law enforcement regardless of whether it is stored on premises anywhere in the world or hosted by a service provider. Even for those enterprises that have no presence in or contacts with the US, law enforcement authorities in the US, like other nations, have legal tools such as Mutual Legal Assistance Treaties and court-to-court requests that enable them to access foreign-based information.

11. Are cloud service providers the only companies that are subject to US government requests for data?

Under long-standing US law, any company with a presence in the US (whether US based or not) can be required to provide to the government data within its possession, custody or control. This includes data that is stored outside the US and data that is in the hands of a subsidiary or affiliate.