

Microsoft wins data privacy appeal against USA - blueAPACHE

Canonical: <https://www.blueapache.com/blog/microsoft-wins-data-privacy-appeal-against-usa>

Details:

Summary

This blueAPACHE post reports: Microsoft has landed a significant win in its ongoing legal battle against the US government over the privacy of its customer data located in offshore datacentres. The US Court of Appeals ruled that the US Federal Government cannot compel companies to turn over electronic data that is stored exclusively on servers located outside the United States. It concerns emPOWER Cloud, Microsoft Practice, emPOWER Core Network & Data Centre Interconnect. It names Microsoft, Google in connection with the announcement. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Services referenced	emPOWER Cloud, Microsoft Practice, emPOWER Core Network & Data Centre Interconnect
Named products or vendors	Microsoft, Google

Article

Electronic data hosted on overseas servers are off-limits for US government

Microsoft has landed a significant win in its ongoing legal battle against the US government over the privacy of its customer data located in offshore datacentres. The US Court of Appeals ruled that the US Federal Government cannot compel companies to turn over electronic data that is stored exclusively on servers located outside the United States. While government and law enforcement agencies can still obtain access to data held domestically in the US under the Stored Communications Act (SCA), the court has determined that the SCA does not apply to electronic data, like emails, held on servers located overseas. This deals the US government the latest setback in its struggle with the tech industry over the reach of law enforcement and the limits of personal privacy.

Background

The case of Microsoft vs the United States of America began in late 2013 when the US Department of Justice (DoJ) issued a warrant to Microsoft under the SCA. The DoJ was attempting to seize contents of an email account stored on Microsoft's servers in Ireland. If Microsoft handed over the data, it would be in violation of Irish data protection laws. Microsoft refused to comply and challenged the warrant, but

was unsuccessful. The court's initial ruling stated that the SCA applies extraterritorially as Microsoft is an US-based service provider. Microsoft subsequently appealed the court's decision resulting in the current ruling. The crux of the issue was a critical question that remains a concern for many organisations, cloud service providers and private users across the world – who has jurisdiction over private data stored in the cloud?

Safe Harbor Agreement

The result of this case has significant impact in Europe. In October last year, the Court of Justice of the European Union declared invalid a “safe harbor” agreement, on which thousands of companies including Google, Facebook, and Apple rely for the transfer of personal data. Declaring the safe harbor agreement invalid directly impacted the transmission of personal information between the US and Europe. A new Privacy Shield data protection agreement was quickly published to remediate the situation, but nervousness around data protection remained. The overturning of the DoJ warrants is expected to alleviate some of the trepidation around privacy, data protection and data sovereignty in the region.

Implications

The final outcome is important as it will resolve a myriad of questions around data ownership; questions that have serious implications for public cloud adoption. It is not just the physical location of the server, but as highlighted in this case, it could be where your cloud provider is headquartered. Australian businesses have a legal obligation to ensure that their customer data and confidential information is protected in line with the Australian Privacy Act . Failure to do so requires full disclosure and can result in hefty penalties for each breach, making data privacy a critical consideration that businesses cannot afford to ignore. For Australian businesses that are currently using overseas-based cloud providers, Microsoft's victory offers a precedent for preserving data sovereignty and protecting the privacy of personal and business information – so long as the data remains securely and solely within Australia. Assuming of course, that our government and local Microsoft entity have an appetite to contest claims from foreign governments and law enforcement agencies beyond geographic borders. Assumptions aside, this risk is something that organisations need to consider. If data sovereignty and privacy are important, the best way to ensure compliance is to partner with a cloud provider who can guarantee that all your data, including any redundancy, backups, billing and reporting remain solely within Australia. Locally owned and operated, blueAPACHE's emPOWER Cloud is an enterprise-grade private cloud platform residing exclusively within three geographically diverse datacentres in Australia. We deliver our complete suite of cloud, telephony and unified communications, network, security and support services locally – guaranteeing data sovereignty for those who need it, and offering direct public cloud integration for those that do not. For more information on data sovereignty and how it may impact your organisation's cloud strategy, contact the blueAPACHE account team .

Related

emPOWER Cloud

emPOWER Cloud (pillar)

Microsoft Practice (pillar)

emPOWER Core Network & Data Centre Interconnect

emPOWER Connectivity (pillar)

Frequently asked questions

What did the US Court of Appeals rule in the Microsoft case described in this article?

The court ruled that the US Federal Government cannot compel companies to turn over electronic data stored exclusively on servers located outside the United States, finding the Stored Communications Act does not apply to data like emails held on overseas servers.

Where was the disputed data stored, and what law did the original 2013 warrant invoke?

The disputed email account data was stored on Microsoft's servers in Ireland, and the US Department of Justice's original warrant was issued under the Stored Communications Act (SCA).

What does the article say happened to the EU-US Safe Harbor agreement, and what replaced it?

The article says the Court of Justice of the European Union declared the EU-US Safe Harbor agreement invalid in October the previous year, and that a new Privacy Shield data protection agreement was then published to remediate the situation.

What does the article say about blueAPACHE's emPOWER Cloud in relation to data sovereignty?

The article describes emPOWER Cloud as a locally owned and operated, enterprise-grade private cloud platform residing exclusively within three geographically diverse Australian datacentres, offered for organisations that need guaranteed data sovereignty.

Is the information in this post still current?

No. It reports a 2016 US court ruling and the EU Privacy Shield agreement that was itself later invalidated; for current guidance on data sovereignty, see the emPOWER Cloud service page rather than this post.

Source

<https://www.blueapache.com/blog/microsoft-wins-data-privacy-appeal-against-usa/>

Knowledge Base

What did the US Court of Appeals rule in the Microsoft data privacy case?

The US Court of Appeals ruled that the US Federal Government cannot compel companies to turn over electronic data that is stored exclusively on servers located outside the United States.

What triggered the Microsoft vs. United States case?

The case began in late 2013 when the US Department of Justice (DoJ) issued a warrant to Microsoft under the Stored Communications Act (SCA), attempting to seize the contents of an email account stored on Microsoft's servers in Ireland.

Why did Microsoft refuse to comply with the DoJ warrant?

If Microsoft handed over the data stored in Ireland, it would be in violation of Irish data protection laws, so Microsoft refused to comply and challenged the warrant.

What was the outcome of the initial court ruling before Microsoft's appeal?

The court's initial ruling stated that the SCA applies extraterritorially because Microsoft is a US-based service provider, which was unfavorable to Microsoft before it appealed.

Does the Stored Communications Act (SCA) still apply to data held domestically in the US?

Yes, government and law enforcement agencies can still obtain access to data held domestically in the US under the Stored Communications Act (SCA); the court determined only that the SCA does not apply to electronic data held on servers located overseas.

What key jurisdictional question did this case raise?

The case raised the critical question of who has jurisdiction over private data stored in the cloud, a concern for organisations, cloud service providers and private users across the world.

How did the invalidation of the Safe Harbor agreement relate to this case?

In October the prior year, the Court of Justice of the European Union declared the 'safe harbor' agreement invalid, which thousands of companies including Google, Facebook, and Apple relied on for transferring personal data; this directly impacted transmission of personal information between the US and Europe, and the overturning of the DoJ warrants in the Microsoft case was expected to alleviate some of the resulting trepidation around privacy, data protection and data sovereignty in the region.

What replaced the invalidated Safe Harbor agreement, ?

A new Privacy Shield data protection agreement was quickly published to remediate the situation after the Safe Harbor agreement was declared invalid, but nervousness around data protection remained.

What do you offer as a solution for organisations concerned about data sovereignty?

Our emPOWER Cloud is a locally owned and operated, enterprise-grade private cloud platform residing exclusively within three geographically diverse datacentres in Australia, delivering cloud, telephony and unified communications, network, security and support services locally to guarantee data sovereignty, while also offering direct public cloud integration for those who do not need it.