Strategic Risks in Europe’s Reliance on U.S. Cloud Services

Executive Summary

European organizations increasingly rely on digital infrastructures for communication, data storage, and operational continuity. In addition to widely recognized cyber threats from state actors such as Russia, China, and Iran, a less acknowledged but equally critical vulnerability persists: dependence on U.S.-based cloud and collaboration platforms.

U.S. surveillance laws, extensive commercial data collection practices, and the weaponization of digital supply chains combine to create a risk environment incompatible with European data protection principles and sovereignty needs. Recent incidents, including interruptions of Microsoft services to the International Criminal Court in May 2025, demonstrate how geopolitical pressure can translate directly into operational disruption.

This whitepaper explores why U.S.-based cloud services pose unique risks when used for sensitive communication. It synthesizes insights from legal frameworks, geopolitical dynamics, case studies, and sector-specific vulnerabilities to support European organizations making long-term digital infrastructure decisions.

The conclusion is clear: Europe must urgently shift to sovereign digital infrastructure to safeguard operational integrity, legal compliance, and strategic independence.

Introduction

The global digital landscape is undergoing rapid change. Governments, private enterprises, and international institutions all face growing exposure to cyberattacks, surveillance regimes, and geopolitical manoeuvring through digital dependencies. For European organizations, selecting a cloud service provider is no longer a mere IT procurement choice: it has become a matter of strategic autonomy.

The Scale of Data Collection

Technology platforms rely on extensive data collection, both for commercial purposes and to support core service functionality. Even when the communication content is protected with end-to-end encryption, as in services such as Signal, Teams, WhatsApp, or iMessage, surrounding metadata, such as who communicated with whom, when, and from where, remains highly revealing and is essential to the operation of these platforms.

Unauthorized access to metadata can reveal:

- Organizational structures
- Communication networks
- Project timelines
- Operational routines
- Sensitive relationships

Transparency reports from Microsoft, Google, Meta, Apple, and others routinely show **hundreds of thousands of U.S. government data requests annually** [1]. These requests may involve:

- Communication data
- Account details
- Device identifiers
- Cloud-stored content
- Metadata detailing activities, interactions and networks

European organizations cannot assume their data is exempt from these flows. For adversaries, metadata-derived insights constitute valuable intelligence; for competitors, particularly in high-stakes or strategic sectors, they can translate into significant informational advantage.

The Critical Importance of Master Keys

In secure communication systems that use end-to-end encryption, user keys protect the content of individual messages. However, the **centrally managed master keys** used to attest and certify those user keys—typically through digital certificates—**are far more critical**. Master keys, typically controlled by Certificate Authorities (CAs), form the foundation of trust, **ensuring that a user key genuinely belongs to the claimed individual.**

Without exclusive control over master keys, as is the case with cloud services like Signal, Teams, WhatsApp and iMessage, organizations face significant risks [2]:

- **Identity Spoofing**: an attacker with knowledge of the master keys can impersonate any user in the system.
- **Man-in-the-Middle Attacks**: an attacker with a privileged network position and knowledge of the master keys can intercept, decrypt, or manipulate messages.
- **Geopolitical Vulnerability**: Master keys controlled under foreign jurisdictions may be compelled or accessed by governments.

While user keys protect individual messages, **the master keys that attest them determine the security, authenticity, and trustworthiness of the entire system**. Exclusive control over master keys is therefore the single most important factor for operational security and digital sovereignty.

U.S. Surveillance Law

The greatest structural risk arises from the clash between U.S. surveillance laws and EU data protection standards.

Key laws include:

- **FISA (Foreign Intelligence Surveillance Act)** [3]
- **FISA Section 702** [3]**;** targeting non-U.S. persons
- **Executive Order 12333** [4]**;** authorising broad foreign intelligence collection
- **CLOUD Act** [5]**;** enabling access to data stored abroad

These laws allow U.S. authorities to force U.S.-based companies, including global IT and cloud providers, to grant access to data regardless of storage location.

The EU and U.S. have repeatedly attempted to create lawful data transfer frameworks, but each has been struck down due to legal incompatibility:

- **Safe Harbor** (invalidated by Schrems I, 2015) [6]
- **Privacy Shield** (invalidated by Schrems II, 2020) [7]
- **Data Privacy Framework** (already facing legal challenges; a “Schrems III” is anticipated) [8].

Repeated failure highlights systemic legal instability and reinforces that **U.S. surveillance practices remain fundamentally incompatible with EU privacy standards**.

The Geopolitical Dimension

For decades, Europe assumed stable strategic alignment with the United States. This assumption is no longer guaranteed. In fact, the U.S. and EU increasingly diverge in several strategic areas:

- Industrial and trade policy
- Control of strategic technologies
- Global geopolitical perspectives
- Territorial interests (e.g. Greenland) [9]

Historically, technological evolution and IT strategies changed far more rapidly than geopolitical alliances. Organizations could adopt new platforms or migrate data with little consideration of long-term geopolitical implications. Today, the situation has reversed: **geopolitical dynamics and alliances are shifting faster than IT adoption cycles**, meaning organizations are now more exposed if their infrastructure depends on providers in geopolitically sensitive jurisdictions.

When geopolitical tensions rise, digital dependencies become leverage points. U.S. based cloud providers **can become tools of coercion**

Weaponization of Digital Supply Chains

Digital infrastructure has become a potent but often overlooked instrument of geopolitical power. U.S.-based cloud providers increasingly find themselves at the centre of foreign-policy disputes, **caught between clients and Washington’s strategic interests**.

The stakes came into sharp focus in early 2025, when President Donald Trump issued an executive order sanctioning the International Criminal Court [10] after it issued arrest warrants for Israeli Prime Minister Benjamin Netanyahu. The court’s reliance on Microsoft’s suite of services, including tools for communication, document management, and case processing capabilities, meant that the subsequent service outage effectively paralyzed key aspects of its daily operations.

The risks are even more challenging for industries facing direct competition from the United States, such as defence, aerospace, and advanced manufacturing. Reliance on U.S. cloud services potentially opens the door to:

- exposure of sensitive project data
- insights into procurement strategies or R&D pipelines
- visibility into collaboration networks
- strategic advantages in global defence markets

For Europe, these vulnerabilities threaten long-term competitiveness, weaken economic sovereignty, and expose key sectors exposed to political pressure from a foreign power that is also a rival.

Conclusion

U.S. cloud services present exceptional strategic, legal, and geopolitical risks for European organizations handling sensitive communication and data. The combination of U.S. surveillance law, unclear data access obligations, and demonstrated political influence over commercial providers creates systemic vulnerability.

Historically, organizations could adapt IT strategies faster than geopolitical developments. Today, geopolitical shifts outpace IT modernization, making dependence on foreign cloud providers increasingly problematic.

For European organizations—particularly those in government, critical infrastructure, and strategic industries digital sovereignty is no longer optional. **It is a prerequisite for operational independence, long-term competitiveness, and national security**.

References

1. **Transparency Reports and Government Data Requests**
   Meta, Apple, Google, and Microsoft publish transparency reports twice a year detailing the volume of government data requests received. These reports show a consistent year-over-year increase.

   https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data
   https://transparencyreport.google.com/user-data/us-national-security?hl=en
   https://transparency.meta.com/reports/government-data-requests/
   https://www.apple.com/legal/transparency/us.html

2. **Security Risks of Compromised Master keys or Certificate Authorities (CAs)**

   - **National Institute of Standards and Technology (NIST) ITL Bulletin** explains that if a CA’s signing key is compromised, attackers can issue fraudulent certificates, including counterfeit revocation lists, causing forged certificates to appear valid.
     https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul2012-07.pdf

   - **European Information Technologies Certification Academy (EITCA)** describes how compromise of a CA’s private (master) key enables attackers to generate fraudulent certificates, enabling identity spoofing, impersonation, and MITM attacks.
     https://eitca.org/cybersecurity/eitc-is-acss-advanced-computer-systems-security/network-security/certificates/examination-review-certificates/what-are-the-potential-vulnerabilities-and-limitations-of-the-certificate-authority-ca-system-and-how-can-these-be-mitigated/

   - **InfoSec Institute** details how attackers can use fraudulent or rogue certificates to impersonate legitimate services or perform man-in-the-middle attacks.
     https://www.infosecinstitute.com/resources/cryptography/cybercrime-exploits-digital-certificates/

3. **Foreign Intelligence Surveillance Act (FISA)**
   FISA (1978) authorizes certain types of foreign intelligence collection, including compelled cooperation from U.S. telecommunications and technology companies.
   https://www.nsa.gov/Signals-Intelligence/FISA/

4. **Executive Order 12333**
   EO 12333 defines the U.S. intelligence community’s authority to collect, retain, and analyze foreign signals intelligence. It governs surveillance activities targeting non-U.S. persons outside the United States
   https://www.nsa.gov/Signals-Intelligence/EO-12333/

5. **Clarifying Lawful Overseas Use of Data (CLOUD) Act**
   The CLOUD Act (2018) enables U.S. authorities to compel U.S.-based service providers to disclose data under their control **regardless** of where the data is geographically stored.
   https://www.justice.gov/criminal/cloud-act-resources

6. **Schrems I (Court of Justice of the European Union, 2015)**
   The Court of Justice of the European Union invalidated the EU–U.S. Safe Harbor framework, ruling that it did not adequately protect EU citizens’ data from U.S. government surveillance.
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362

7. **Schrems II (Court of Justice of the European Union, 2020)**
   The Court of Justice of the European Union struck down the EU–U.S. Privacy Shield, concluding that U.S. surveillance laws (including FISA 702) did not provide adequate protections or effective redress mechanisms for EU citizens.
   https://www.gdprsummary.com/schrems-ii/
   https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677

8. **Anticipated “Schrems III” Challenge**
   Privacy advocates including Max Schrems and NOYB have announced plans to challenge the new EU–U.S. Data Privacy Framework (DPF) before the Court of Justice of the European Union, arguing that it fails to sufficiently limit U.S. surveillance or provide meaningful redress for EU citizens.
   https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

9. **U.S. Interest in Greenland**
   BBC articles detailing interest shown by U.S. president Donald Trump to purchase or otherwise acquiring control of Greenland.
   https://www.bbc.com/news/world-us-canada-49367792
   https://bbc.com/news/articles/c74x4m71pmjo

10. **2025 Executive Order Targeting the International Criminal Court (ICC)**
    In February 2025, U.S. President Donald Trump issued an executive order instructing U.S. companies, including Microsoft, to block services to the International Criminal Court following the issuance of arrest warrants for senior Israeli officials in late 2024.
    https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/