Oltre la vendita dei dati

Il vero prezzo dei servizi digitali

Alberto Pianon – **Array** – pianon@array.eu

LinuxDay - Poggibonsi - 24/10/2026

© 2026 Alberto Pianon (Array)

Mi presento

«Other lawyers talk, I code» 🤘

IT Lawyer, Vicenza, Array
FOSS & Digital liberties advocate
25+ anni di esperienza FOSS
Member, FSFE Legal Network
Committer Member, Eclipse Foundation
FOSS user & contributor (Yocto, Fossology, Scancode…)
De-Microsofted dal 2000, De-Googled dal 2013

© 2026 Alberto Pianon (Array)

Il problema dei servizi digitali

- «There’s no cloud, just other people’s computers» (FSF(E))
- «Se non stai pagando per un prodotto, allora il prodotto sei tu» (The Social Dilemma)
- Ma c’è dell’altro…

© 2026 Alberto Pianon (Array)

Che cos'è questo?



https://transparencyreport.google.com/user-data/us-national-security

© 2026 Alberto Pianon (Array)

Non-content requests under FISA

A FISA request can include non-content metadata—for example, the "from" and "to" fields in an email header and the IP addresses associated with a particular account.

Reporting period	Number of requests	Number of accounts
Jan 2026 – Jun 2026	Data subject to six month reporting delay	Data subject to six month reporting delay
Jul 2025 – Dec 2025	0 – 499	61500 – 61999
Jan 2025 – Jun 2025	0 – 499	75500 – 75999
Jul 2024 – Dec 2024	0 – 499	51500 – 51999
Jan 2024 – Jun 2024	0 – 499	40500 – 40999
Jul 2023 – Dec 2023	0 – 499	31500 – 31999
Jan 2023 – Jun 2023	0 – 499	33000 – 33499
Jul 2022 – Dec 2022	0 – 499	27500 – 27999
Jan 2022 – Jun 2022	0 – 499	35500 – 35999
Jul 2021 – Dec 2021	0 – 499	28500 – 28999
Jan 2021 – Jun 2021	0 – 499	27500 – 27999
Jul 2020 – Dec 2020	0 – 499	22500 – 22999
Jan 2020 – Jun 2020	0 – 499	22000 – 22499

© 2026 Alberto Pianon (Array)

Content requests under FISA

A FISA request can include a demand for a user's content, such as Gmail messages, documents, photos, and videos.

Reporting period	Number of requests	Number of accounts
Jan 2026 – Jun 2026	Data subject to six month reporting delay	Data subject to six month reporting delay
Jul 2025 – Dec 2025	0 – 499	211000 – 211499
Jan 2025 – Jun 2025	0 – 499	177500 – 177999
Jul 2024 – Dec 2024	0 – 499	138500 – 138999
Jan 2024 – Jun 2024	0 – 499	127000 – 127499
Jul 2023 – Dec 2023	0 – 499	118000 – 118499
Jan 2023 – Jun 2023	0 – 499	115000 – 115499
Jul 2022 – Dec 2022	0 – 499	106000 – 106499
Jan 2022 – Jun 2022	0 – 499	103000 – 103499
Jul 2021 – Dec 2021	0 – 499	95500 – 95999
Jan 2021 – Jun 2021	0 – 499	89000 – 89499
Jul 2020 – Dec 2020	0 – 499	80000 – 80499

© 2026 Alberto Pianon (Array)

Non solo Google...

https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF

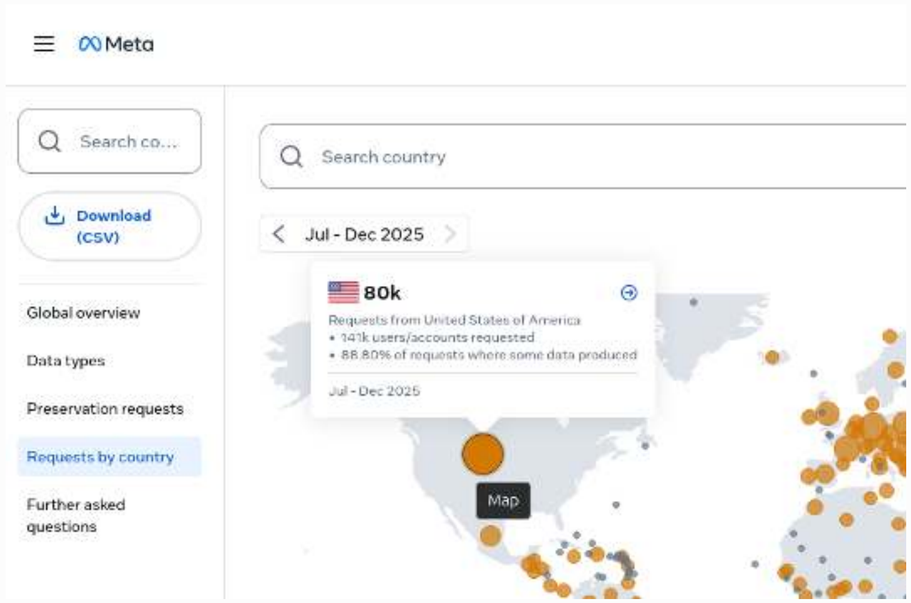


https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data

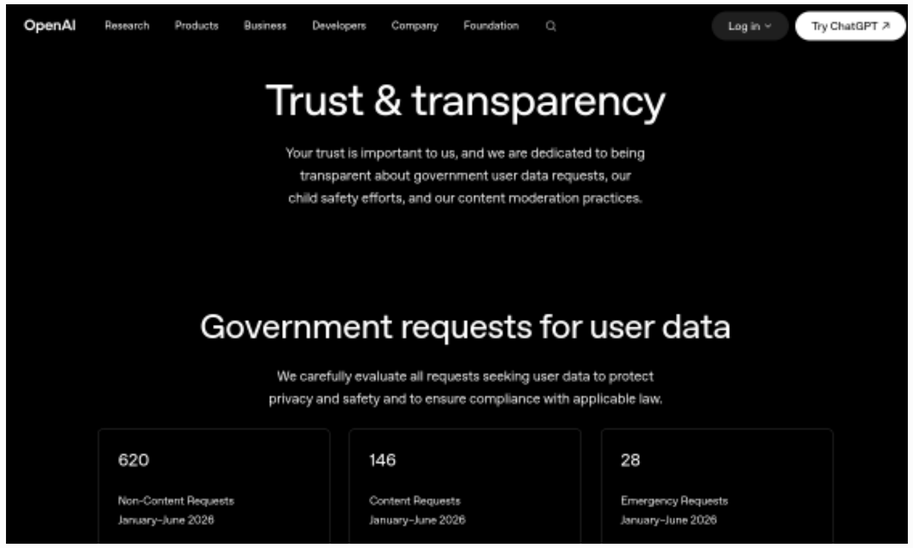


© 2026 Alberto Pianon (Array)

https://transparency.meta.com/reports/government-data-requests/country/



https://openai.com/trust-and-transparency/



© 2026 Alberto Pianon (Array)

FISA e Section 702: che cosa sono (1)

FISA (1978)

- Legge USA che regola la sorveglianza **a fini di intelligence estera** (non indagini penali)
- Nasce dopo gli abusi degli anni ‘70 per mettere la sorveglianza sotto il controllo di un giudice
- Istituisce un tribunale speciale e segreto: la **FISA Court** (11 giudici federali)

© 2026 Alberto Pianon (Array)

FISA e Section 702: che cosa sono (2)

Section 702 (2008)

- Consente di raccogliere comunicazioni di **persone non statunitensi che si trovano fuori dagli USA**
- Lo fa **obbligando i provider americani** (email, cloud, social, telecomunicazioni) a consegnare i dati
- **Nessun mandato individuale**: il giudice approva il *programma*, non i singoli bersagli
- Legge “a scadenza”: rinnovata più volte, **decaduta a giugno 2026**, ma le autorizzazioni in corso restano valide fino a **marzo 2027 circa** (un rinnovo “postumo” è attualmente in discussione)

© 2026 Alberto Pianon (Array)

Come funziona: certificazione → target → selettori (1)

1. Certificazione (una volta l’anno)

- Il Ministro della Giustizia e il Direttore dell’intelligence indicano le **categorie di informazioni** da raccogliere (oggi quattro: terrorismo, governi stranieri, proliferazione di armi, narcotraffico)
- La FISA Court verifica **le regole**, non le persone

© 2026 Alberto Pianon (Array)

Come funziona: certificazione → target → selettori (2)

2. Target (scelti dagli analisti)

- Persone o entità **non statunitensi, all'estero**, che si ritiene possano comunicare informazioni su quei temi
- **Non serve essere sospettati** di alcun illecito
- Scelta interna alle agenzie, controllata **solo a posteriori**

3. Selettori

- Identificativi concreti del target: **email, numero di telefono, account**
- Non parole chiave
- Inviati ai provider, che devono consegnare le comunicazioni collegate

© 2026 Alberto Pianon (Array)

FISA Sec 702: Le criticità per i cittadini europei (1)

Grandi volumi di dati

- Circa **350.000 target** stranieri nel solo 2025 (stima ufficiale)
- Si raccolgono anche le comunicazioni di **chiunque parli con un target** (“raccolta incidentale”): anche chi non è sorvegliato può finire nei database
- I dati raccolti possono essere **interrogati in seguito**; le tutele rafforzate valgono solo per i cittadini USA

© 2026 Alberto Pianon (Array)

FISA Sec 702: Le criticità per i cittadini europei (2)

Mancanza di un ricorso indipendente

- Le persone sorvegliate **non vengono mai informate**
- Un europeo **non può rivolgersi alla FISA Court**
- Un europeo **non può invocare il quarto emendamento**
- Eventuali rimedi giurisdizionali sono di fatto impraticabili per chi non è cittadino americano
- E l'Unione Europea non fa nulla? Sì, ma… (lo vedremo fra poco)

© 2026 Alberto Pianon (Array)

Non c'è solo il FISA Sec 702: l'EO 12333 (1)

Executive Order 12333 (1981)

- **Ordine presidenziale**, non una legge del Congresso: il Presidente può modificarlo o revocarlo da solo
- Regola la **raccolta di intelligence all'estero**: intercettazione di cavi e satelliti, accesso a reti straniere, attacchi informatici, collaborazione con servizi alleati
- **Nessun obbligo per i provider** e **nessun giudice**: le agenzie raccolgono i dati con mezzi propri
- Consente la **raccolta massiva** ("bulk"), oggi limitata a sei finalità dall'Executive Order 14086 del 2022

© 2026 Alberto Pianon (Array)

Non c'è solo il FISA Sec 702: l'EO 12333 (2)

- **Nessuna scadenza** e **nessun obbligo di trasparenza** paragonabile alla Section 702
- È la base giuridica della **maggior parte** dell'attività di intelligence dei segnali (SIGINT) americana

Perché conta per noi

- Tenere i dati **in Europa** riduce l'esposizione alla 702, non a questo strumento
- Non è toccato dalla **decadenza della 702** (giugno 2026)
- Unica tutela pratica: la **cifratura**
- Anche qui, l'Unione Europea non fa nulla? Ci arriviamo subito…

© 2026 Alberto Pianon (Array)

Le rivelazioni di Snowden (2013)



Credits: By https://www.youtube.com/user/TheWikiLeaksChannel - Derived from: File:Edward Snowden speaks about government transparency at Sam Adams award presentation in Moscow.webm @20s, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=28971285

Cosa è emerso

- **PRISM**: raccolta tramite i grandi provider USA (Google, Microsoft, Facebook, Apple, Yahoo…) in base alla Section 702
- **Raccolta "upstream"**: intercettazione direttamente sui cavi Internet
- **Metadati telefonici** di milioni di americani raccolti in blocco
- **Intercettazioni all'estero** anche dei collegamenti interni dei provider (EO 12333)
- **Migliaia di violazioni** delle regole interne ogni anno, poco visibili ai controllori

© 2026 Alberto Pianon (Array)

Snowden: le conseguenze

- Le aziende ottengono di pubblicare **dati aggregati** sulle richieste ricevute
- Riforme USA: stop alla **raccolta massiva** dei metadati telefonici (2015)
- In EU: ricorso di **Max Schrems** → annullamento del **Safe Harbor** (2015)

© 2026 Alberto Pianon (Array)

La sentenza Schrems I (2015) e la fine del Safe Harbor (1)

Cos'era il Safe Harbor (2000)

- Decisione della Commissione europea che dichiarava **"adeguato"** il trasferimento di dati verso le aziende USA aderenti
- Le aziende **si auto-certificavano**, impegnandosi a rispettare principi di privacy fissati dal governo USA
- Circa **3.200 aziende** aderenti nel 2013, tra cui i grandi provider

© 2026 Alberto Pianon (Array)

La sentenza Schrems I (2015) e la fine del Safe Harbor (2)

La sentenza (Corte di giustizia UE, 6 ottobre 2015)

- Le **autorità privacy nazionali** possono esaminare i reclami anche in presenza di una decisione di adeguatezza; e la Corte può annullarla
- "Adeguato" significa **"sostanzialmente equivalente"** alla tutela garantita nell'UE
- Il Safe Harbor vincolava **solo le aziende, non le autorità USA**, e cedeva sempre davanti alle esigenze di **sicurezza nazionale**
- La Commissione **non aveva verificato** che il diritto USA garantisse davvero tale tutela
- **Risultato: Safe Harbor annullato**

© 2026 Alberto Pianon (Array)

La sentenza Schrems I (2015) e la fine del Safe Harbor (3)

I principi fissati

- L’accesso generalizzato delle autorità al **contenuto** delle comunicazioni lede l’**essenza** del diritto alla vita privata (Art. 7 CDFUE)
- L’assenza di **qualsiasi rimedio** per l’interessato lede l’**essenza** del diritto a una tutela giurisdizionale effettiva (Art. 47 CDFUE)

© 2026 Alberto Pianon (Array)

La sentenza Schrems II (2020) e la fine del Privacy Shield (1)

Cos'era il Privacy Shield (2016)

- Successore del Safe Harbor, adottato **nove mesi dopo** Schrems I
- Stesso meccanismo di **auto-certificazione** delle aziende USA, con regole più severe e revisioni annuali
- Novità: un **Ombudsperson** presso il Dipartimento di Stato USA per i reclami degli europei sulla sorveglianza

© 2026 Alberto Pianon (Array)

La sentenza Schrems II (2020) e la fine del Privacy Shield (2)

La sentenza (Corte di giustizia UE, 16 luglio 2020)

- Il caso nasce dalle **clausole contrattuali standard** usate da Facebook; la Corte esamina anche il Privacy Shield, adottato nel frattempo
- La sorveglianza USA (**Section 702** ed **EO 12333**) **non è limitata allo stretto necessario**
- La FISA Court approva i **programmi**, ma non verifica che i **singoli target** siano scelti correttamente
- Gli europei **non hanno diritti azionabili** davanti a un giudice
- L'**Ombudsperson** dipende dal governo e non può imporre nulla alle agenzie
- **Risultato: Privacy Shield dichiarato invalido**, con effetto immediato e senza periodo transitorio

© 2026 Alberto Pianon (Array)

La sentenza Schrems II (2020) e la fine del Privacy Shield (3)

Le clausole contrattuali standard (SCC)

- Restano **valide**, ma chi esporta i dati deve verificare caso per caso la legge del Paese di destinazione
- Se serve, deve adottare **misure supplementari**; altrimenti il trasferimento va sospeso
- In mancanza, è l'**autorità di controllo** che **deve** sospenderlo o vietarlo

© 2026 Alberto Pianon (Array)

Provaci ancora, Sam – Il Data Privacy Framework (2023) e i suoi punti deboli (1)

Come funziona

- Decisione di adeguatezza della Commissione del **10 luglio 2023**
- Aziende USA **auto-certificate** presso il Dipartimento del Commercio, con controlli affidati a **FTC** e Dipartimento dei Trasporti
- Base sul fronte sorveglianza: **Executive Order 14086** (2022)
  - **necessità e proporzionalità** dell'intelligence
  - **12 finalità** ammesse; la raccolta massiva è limitata a 6
  - nuovo ricorso: **Data Protection Review Court**, attivabile tramite il garante privacy
- Le garanzie dell'EO 14086 valgono anche per i trasferimenti basati su **clausole standard**

© 2026 Alberto Pianon (Array)

Provaci ancora, Sam – Il Data Privacy Framework (2023) e i suoi punti deboli (2)

Le criticità

- La DPRC è un **organo del governo**, non un tribunale; dà una **risposta standard** e non è appellabile
- Tutto poggia su un **ordine presidenziale**, revocabile con una firma
- La raccolta massiva avviene **senza autorizzazione preventiva indipendente**
- Restano fuori dall'EO 14086 gli **acquisti di dati dai data broker**

© 2026 Alberto Pianon (Array)

Provaci ancora, Sam – Il Data Privacy Framework (2023) e i suoi punti deboli (3)

Novità 2024–2026:

- definizione **più ampia** dei soggetti obbligati dalla 702
- **PCLOB** (l'organo di controllo indipendente) senza quorum dal 2025
- **decadenza della 702** a giugno 2026
- sentenza Trump v. Slaughter (29 giugno 2026): la **FTC** perde la sua indipendenza

© 2026 Alberto Pianon (Array)

Il caso Latombe (2023–....)

- Ricorso di **Philippe Latombe**, deputato francese, per l'annullamento del DPF (causa T-553/23)
- **Tribunale UE, 3 settembre 2025: ricorso respinto**
  - la DPRC offre **garanzie sufficienti** di indipendenza, anche se non è stata creata per legge
  - per la raccolta massiva basta un **controllo successivo** (quello della DPRC); non serve un'autorizzazione preventiva
  - valutazione riferita alla situazione **al momento dell'adozione** (2023)
- **Appello alla Corte di giustizia** (C-703/25 P, ottobre 2025): **pendente**

© 2026 Alberto Pianon (Array)

Verso Schrems III – La Vendetta?

- **30 giugno 2026**: noyb (Max Schrems) chiede alla Commissione un **ritiro ordinato** del DPF e annuncia un'azione legale
- **31 luglio 2026**: l'**EDPB** chiede alla Commissione di valutare l'impatto di *Trump v. Slaughter*
- A quanto risulta, **nessuna nuova causa** è ancora stata depositata
- Scenari possibili:
  - decisione della Corte sull'**appello Latombe**
  - nuovo caso tramite un **reclamo** a un'autorità privacy e un **rinvio pregiudiziale**
  - **sospensione o revisione** da parte della Commissione
- **Oggi il DPF è pienamente valido**, ma strutturalmente esposto

© 2026 Alberto Pianon (Array)

E poi c'è il CLOUD Act (1)

Cos'è (2018)

- Legge USA per le **indagini penali**, non per l'intelligence
- Le autorità USA possono ordinare ai **provider americani** di consegnare i dati che controllano, **ovunque siano conservati**, anche in data center europei
- Accordi bilaterali per consentire ad altri Paesi richieste dirette ai provider USA: oggi solo **Regno Unito** e **Australia**; UE e Canada in trattativa

© 2026 Alberto Pianon (Array)

E poi c'è il CLOUD Act (2)

Le differenze con FISA 702 ed EO 12333

- **Finalità**: perseguire reati, non raccogliere intelligence
- **Controllo**: richieste legate a un **singolo procedimento**, di regola autorizzate da un giudice, non programmi approvati in blocco
- **Bersaglio**: chiunque sia coinvolto in un'indagine, **anche cittadini europei**

Il rapporto con Schrems I e II

- Le sentenze hanno riguardato la **sorveglianza per sicurezza nazionale**: il CLOUD Act **non è stato toccato**
- Non è coperto dall'**EO 14086** né dalla **Data Protection Review Court**
- Resta il conflitto con l'**art. 48 GDPR**, che riconosce gli ordini di Paesi terzi solo sulla base di un accordo internazionale

© 2026 Alberto Pianon (Array)

Last but not least: il “data broker loophole” (1)

Il problema

- Le agenzie USA possono **comprare** dati invece di chiederli con un ordine
- Sul mercato: **posizione degli smartphone**, profili pubblicitari, dati delle app
- Sono dati raccolti ogni giorno anche su **cittadini europei**, tramite app e circuiti pubblicitari

© 2026 Alberto Pianon (Array)

Last but not least: il “data broker loophole” (2)

Perché è una scappatoia

- L’acquisto **non è sorveglianza** in senso giuridico: niente FISA, niente giudice
- È **fuori dall’EO 14086**: niente necessità e proporzionalità, niente ricorso alla DPRC
- Le regole interne dell’intelligence (2024) non prevedono rimedi e non è chiaro se tutelino i non statunitensi
- La **FTC** può colpire i venditori, ma i suoi provvedimenti hanno **esentato** le vendite per sicurezza nazionale
- Il progetto di legge per vietare questi acquisti si è fermato al **Congresso** (2024)
- Secondo l’EDPB, è un modo per **aggirare** le garanzie del DPF

© 2026 Alberto Pianon (Array)

...il cerchio si chiude

- There’s no cloud, just other people’s computers…
- Se non stai pagando per un prodotto, allora il prodotto sei tu…
- Da un grande potere derivano grandi responsabilità… o no?

© 2026 Alberto Pianon (Array)

Grazie per l'attenzione!



This work is licensed under a Creative Commons - Attribution - ShareAlike 4.0
Presentation made using Reveal.js and a Markdown workflow with reveal-md

© 2026 Alberto Pianon (Array)