

Privacy ed i giganti del web

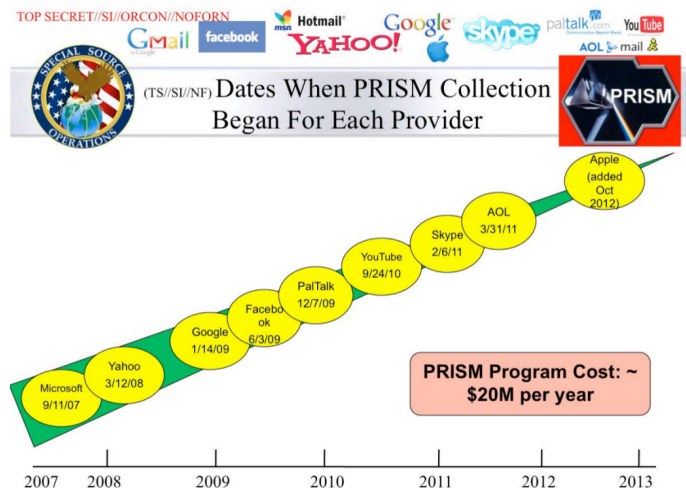
Paolo Vecchi – Omnis Cloud (Luxembourg)

#libreitaliaconf2020 – 19 dicembre 2020



Breve introduzione alla mancanza di privacy ed alla situazione legale post Privacy Shield

Introduzione alle problematiche



EU 'may take action' against Google over privacy policy

EU watchdogs plan to take action against Google by this summer over the web giant's current privacy policy, French privacy regulator CNIL has said.

Since March, Google has been combining data from across its sites to potentially better target adverts - which regulators see as "high risk" to people's privacy.



Hundreds of US companies make false data protection claims

08.10.13 @ 09:02

RELATED > EU questions decade-old US data agreement > Snowden to EU: Whistleblowers need protection > EU-wide whistleblower protection law rejected

BY NIKOLAJ NIELSEN

STRASBOURG - Hundreds of US-based companies handling EU citizens'

MEPs copy-pasting amendments from US lobbyists

12.02.13 @ 09:10

RELATED > EU data protection rules 'on schedule' despite delay > Euro-deputies weaken data protection law > Belgian MEP blames assistant for industry-scripted amendments

BY NIKOLAJ NIELSEN

BRUSSELS - A handful of MEPs have copy-pasted amendments made by giant US-based IT companies directly into the EU's new data protection law.



Congratulations, @MaxSchrems. You've changed the world for the better. webfoundation.org/2015/10/privac...

Übersetzung anzeigen



Alcuni considerano i dati come il petrolio



NSA's arsenal of Windows hacking tools has leaked

The NSA used the Windows hacking tools to target several banks.

By Zack Whittaker for Zero Day | April 14, 2017 -- 14:59 GMT (15:59 BST) | Topic: Security



US cell carriers are selling access to your real-time phone location data

The company embroiled in a privacy row has 'direct connections' to all major US wireless carriers, including AT&T, Verizon, T-Mobile, and Sprint -- and Canadian cell networks, too.

By Zack Whittaker for Zero Day | May 14, 2018 -- 19:00 GMT (20:00 BST) | Topic: Security

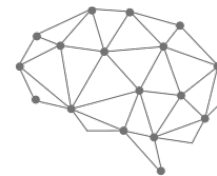


15B devices worldwide



Data firm leaks 48 million user profiles it scraped from Facebook, LinkedIn, others

Exclusive: Profile data was scraped without user consent or knowledge to 'build a three-dimensional picture' on millions of people.



Cambridge Analytica

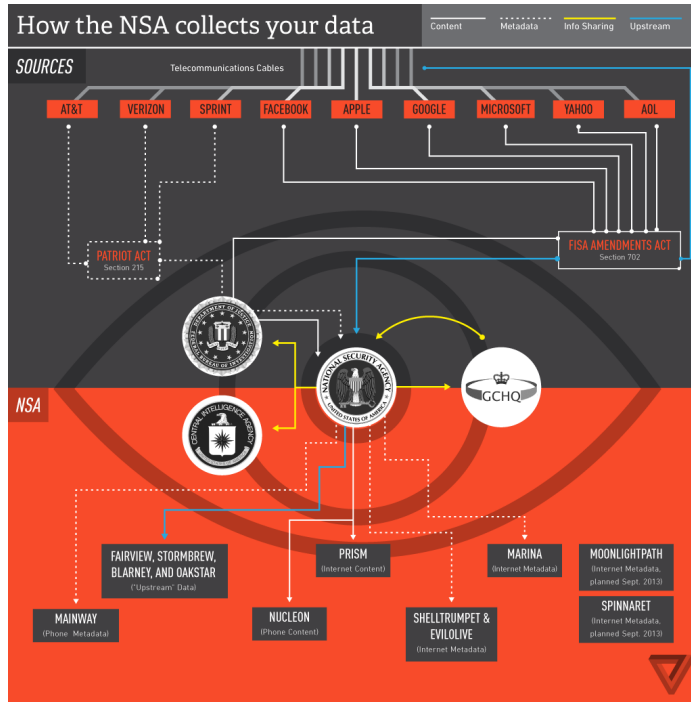
TECHNOLOGY NEWS JANUARY 21, 2020 / 1:07 PM / UPDATED 10 MONTHS AGO

Exclusive: Apple dropped plan for encrypting backups after FBI complained - sources

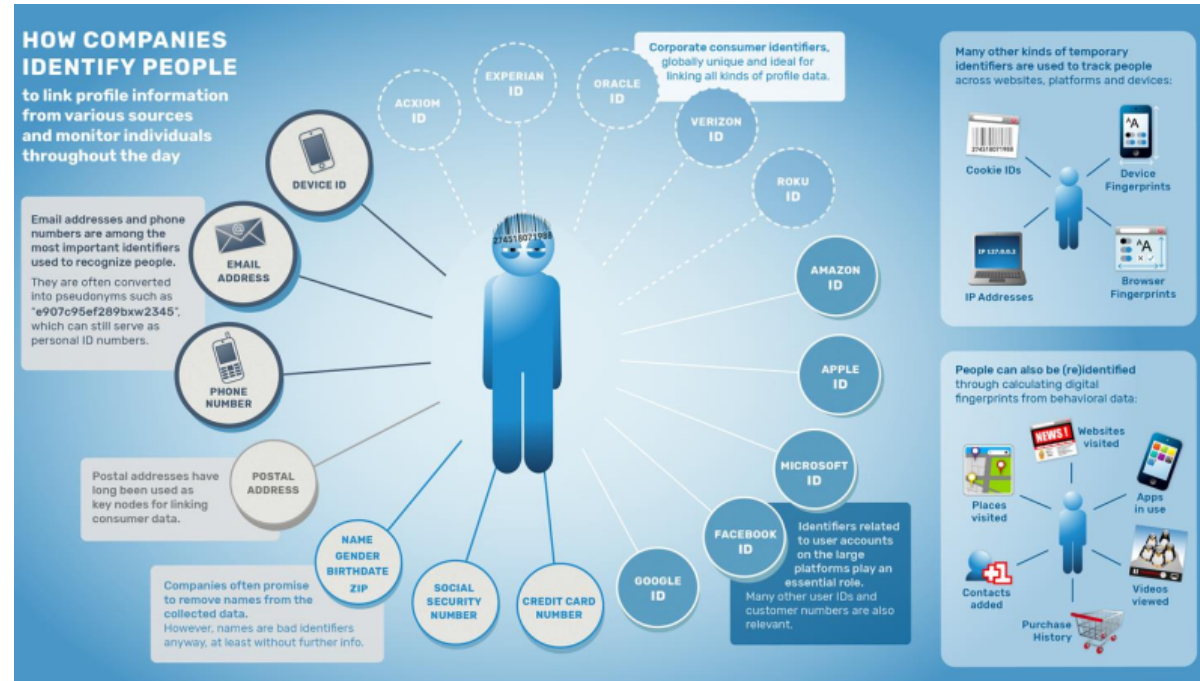
... ed il petrolio inquinata.

Due delle problematiche principali

Sorveglianza di massa



Capitalismo della sorveglianza



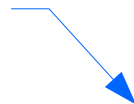
Antiterrorismo ma anche "interessi nazionali"
Echelon Affair docet

Real time bidding pubblicitario e prezzi "personalizzati",
manipolazione economica e sociale

“Prendiamo la vostra privacy, seriamente”

Email come comunicazione privata?

Ho inviato questo



BTW regarding your MS Office issue just download LibreOffice from here: <https://www.libreoffice.org/dow>

Download LibreOffice | LibreOffice - Free Office Suite ...

www.libreoffice.org

Download free office suite - download LibreOffice for Windows, macOS (Mac OS X), Linux. Originally OpenOffice.org.

“Loro” hanno aggiunto questo



Tracciamento su ogni sito visitato



Paolo Vecchi @Vecchi_Paolo · Apr 19

Maybe @teamdigitaleIT could look into it to remove Google Analytics and Google Fonts to respect citizens Privacy?
Implementing @matomo_org across government's site is easy & will show you care about #Privacy and #GDPR.

1



6



Google Fonts

@googlefonts

Follow

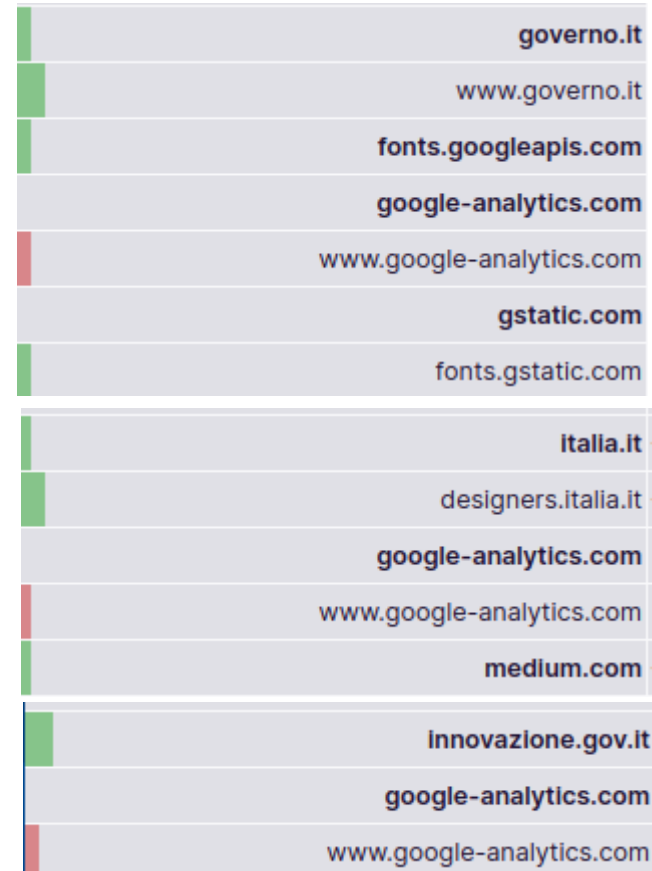
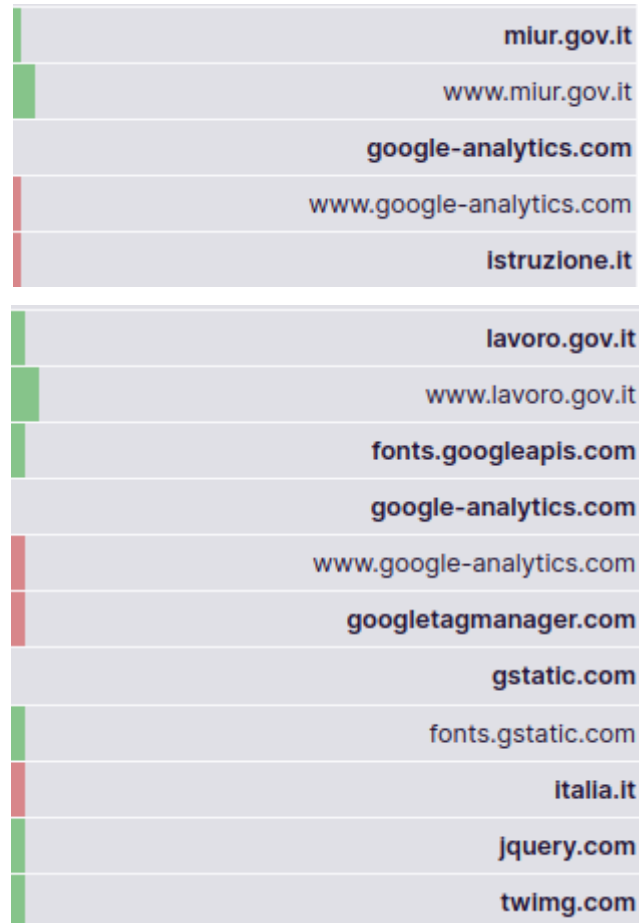
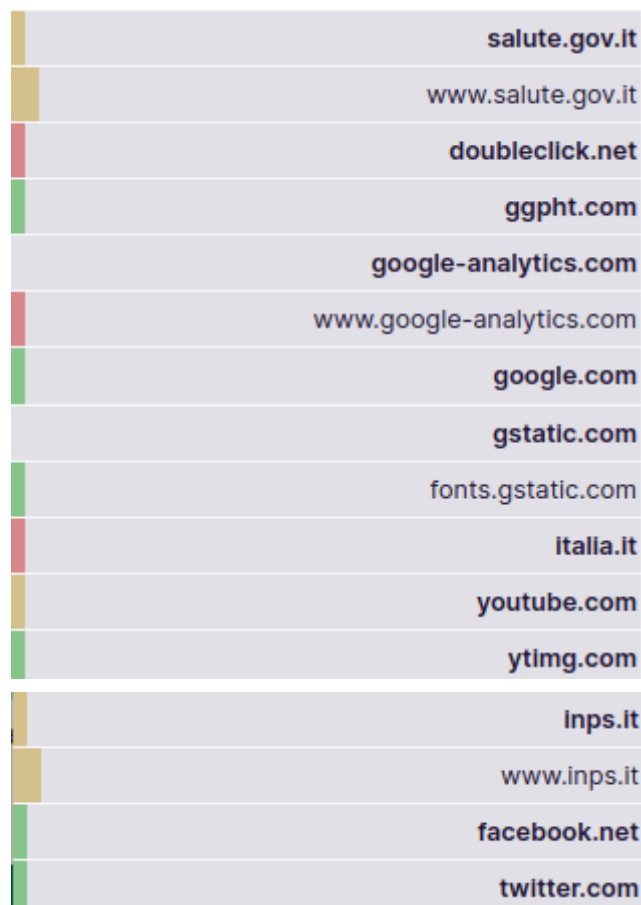
Replying to @Vecchi_Paolo @gchampeau and 2 others

Google Fonts acts as a "data controller" for any personal data that Google processes in connection with your use of Google Fonts web and Android APIs.

7:05 pm - 25 May 2018

E quando avrei fornito il mio consenso?

Anche il governo contribuisce al problema



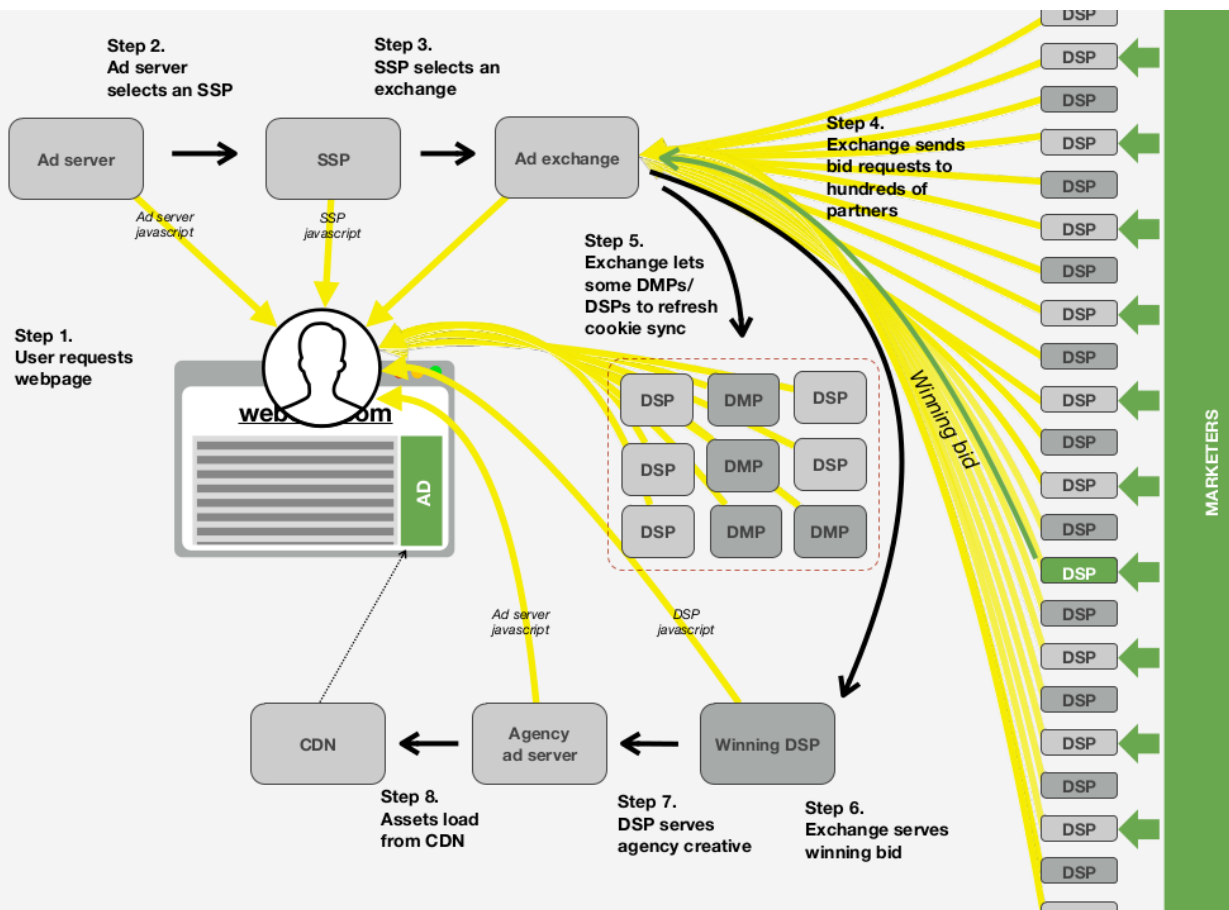
Cosa succede dietro le quinte

DATA LEAKAGE IN ONLINE ADVERTISING

This is the current process of real-time bidding that is used in online behavioural advertising.

Legend

- Channel of data leakage
- Money

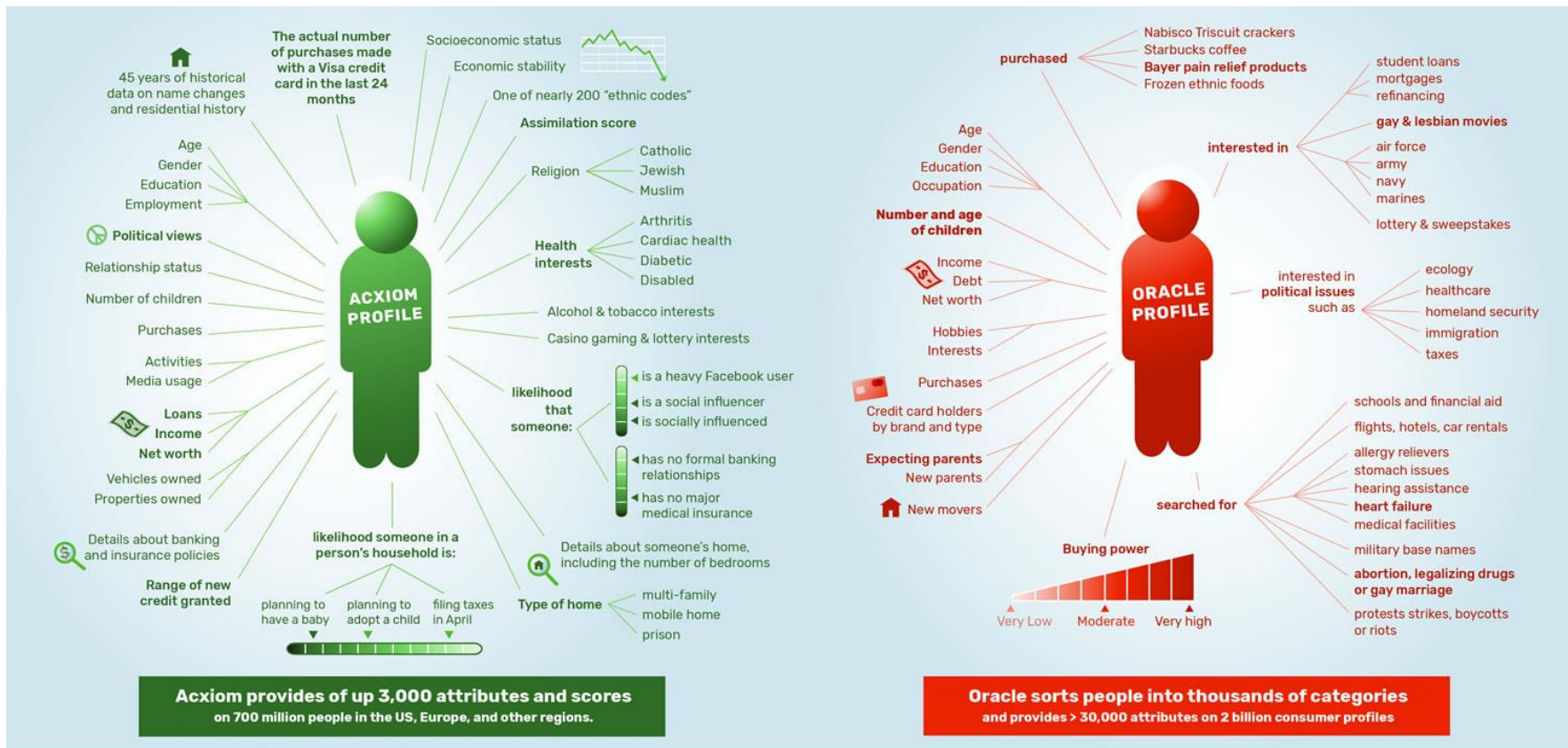


Piccola selezione degli attori visibili

Piccola selezione degli attori visibili



La privacy lede chi non ce l'ha



© Cracked Labs CC BY-SA 4.0. April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Acxiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs), Oracle press release, help center website, audience playbook, taxonomy updates for January, 2017 (Excel document). For details about the sources see the report "Corporate Surveillance in Everyday Life".

Vi fidate di queste aziende?!



December 16, 2020 | Press Release

AG Paxton Leads Multistate Coalition in Lawsuit Against Google for Anticompetitive Practices and Deceptive Misrepresentations

Texas Accuses Google and Facebook of an Illegal Conspiracy

A new antitrust case against Google alleges that the two companies made a deal to reduce competition in online advertising.

Big Tech Goes on Shopping Spree, Brushing Off Antitrust Scrutiny

FOCUS-Microsoft quietly prepares to avoid spotlight under Biden

“It’s the classic case of shiny objects,” said Andrew Gavil, a professor at Howard University School of Law. “Microsoft has succeeded in making sure the attention stays on everybody else even when they continue to be dominant in many areas they operate.”

Facebook will move UK users to US terms, avoiding EU privacy laws

Amazon sought to water down EU privacy rules, document shows

Company pushed for laxer rules around using data by pitting EU institutions against each other.

Italy antitrust opens inquiry into Google, Apple, Dropbox on cloud computing

Microsoft may face EU antitrust probe after Slack complaint on tying practice

French watchdog fines Google, Amazon for breaching cookies rules

noyb files complaints against Apple's tracking code "IDFA"

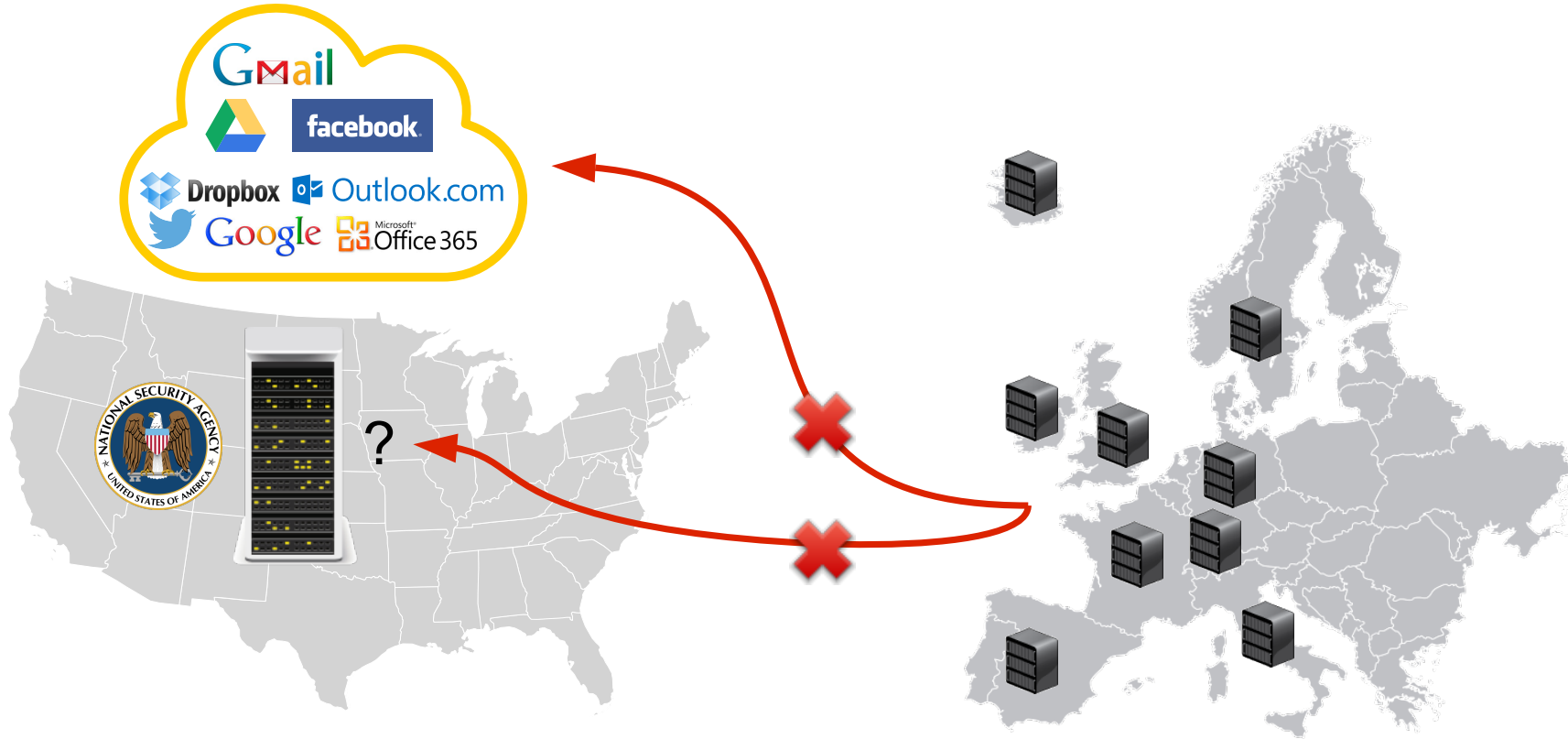
Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services

Sono tutti collusi

142. Google has also actively worked with Big Tech competitors to undermine government efforts to enhance users' privacy. For example, in preparation for a closed-door meeting on August 6, 2019 between the five Big Tech companies—Google, Facebook, Apple, Amazon, and Microsoft—Google [REDACTED]

[REDACTED]
[REDACTED] Google was particularly interested in coordinating with other Big Tech companies to delay privacy regulation because of its impact to Google's advertising business. Google presents a public image of caring about privacy, but behind the scenes Google coordinates closely with the Big Tech companies to lobby the government to delay or destroy measures that would actually protect users' privacy.

E' ora di ridurre il trasferimento dei dati



IANAL!

(I Am Not A Lawyer!)

Sono un semplice cesellatore di bytes

Quanto segue deriva dalla lettura di documenti pubblici ufficiali presentati in modo estremamente semplificato ma il cui messaggio di base può essere confermato da chiunque investa un po di tempo per leggere le fonti:

[Sentenza C-311/18](#), [FAQ di EDPB](#), [Clausole Contrattuali Tipo](#), [Modifiche della Commissione agli SCC](#),
[Raccomandazioni misure aggiuntive EDPB](#), [analisi pre-Schrems II](#), [situazione post-Schrems II](#),
[Risultato investigazione di EDPS su Microsoft](#)

Naturalmente questo è quello che tutti i DPO avrebbero dovuto fare!

Lo dice la legge (e/o il RGPD)



- Accordo tra EU/US invalidato
- Leggi statunitensi violano i nostri diritti fondamentali
- Clausole contrattuali standard non valide nel Cloud
- Nessuna base legale valida disponibile
- Pratiche commerciali ingannevoli
- Contratti al limite della truffa

Carta dei Diritti Fondamentali dell'UE

Articolo 7

Rispetto della vita privata e della vita familiare

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8

Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Articolo 47

Diritto a un ricorso effettivo e a un giudice imparziale

Ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo.

Ogni individuo ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni individuo ha la facoltà di farsi consigliare, difendere e rappresentare.

A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.



Interpretazioni della sentenza Schrems II

Domanda*: Le clausole contrattuali standard violano gli articoli 7, 8 e 47 della Carta?

Risposta: Di per se, no.

Continuare a garantire trasferimento di dati tra i Paesi:
l'impegno Microsoft

luglio 16, 2020

Oggi la Corte di Giustizia dell'Unione Europea ha emesso una sentenza relativa ad un Caso che esamina i trasferimenti di dati dall'UE.

Vogliamo chiarire l'impatto di questa decisione per i nostri Clienti.

Confermiamo che tutti i nostri Clienti possono continuare a utilizzare i servizi Microsoft, in pieno rispetto del diritto europeo. La sentenza della Corte non modifica la capacità di trasferire dati tra l'UE e gli Stati Uniti utilizzando il cloud Microsoft.

Per anni, Microsoft ha fornito ai Clienti livelli di protezione elevati sia per gli Standard Contractual Clauses (SCC) che per il Privacy Shield in merito a tutti i trasferimenti di dati. Anche se la sentenza odierna ha invalidato l'utilizzo di Privacy Shield, gli SCC rimangono validi. I nostri Clienti sono già protetti dalle SCC per l'utilizzo del cloud Microsoft e i relativi trasferimenti di dati.

Aggiornamento alle clausole contrattuali standard (agosto 2020)

A partire dal 12 agosto 2020, Google si baserà sulle clausole contrattuali standard della Commissione europea per i trasferimenti dei dati personali relativi alla pubblicità online e alla misurazione al di fuori dallo Spazio economico europeo, del Regno Unito o della Svizzera. Per i [Servizi del Responsabile del trattamento](#), Google sta aggiornando i [Termini per il trattamento dei dati di Google Ads](#) in modo da includere le [clausole contrattuali standard per i trasferimenti di dati personali ai responsabili del trattamento con sede in paesi terzi](#). Per i Servizi del titolare del trattamento, Google sta aggiornando i [Termini contrattuali sulla protezione dei dati applicabili al Titolare del trattamento di Google Ads](#) in modo da includere le [clausole contrattuali standard per i trasferimenti di dati personali ai titolari del trattamento con sede in paesi terzi](#). In caso di trasferimento pertinente di dati personali, verranno applicate le clausole contrattuali standard incorporate nel contratto tra il cliente e Google.

(Pubblicato ad agosto 2020)

Basandosi solo sull'articolo 149, ed ignorando il resto della sentenza, i Cloud provider statunitensi cercano di convincere i clienti che con le nuove Clausole tutto è a posto.

* semplificazione delle domande 7 e 11 e della risposta presente nella sentenza C-311/18

Ma non per Cloud provider statunitensi

- Art. 168 I programmi di sorveglianza di massa negli stati uniti non garantiscono i diritti fondamentali sanciti dalla Carta art. 7, 8 e 47
- Art. 199 Includendo i motivi di cui sopra e l'art 45 del RGPD invalida Privacy Shield
- Art 141 ricorda l'obbligo dell'esportatore e dell'importatore di verificare se le normative locali proteggono i diritti del singolo in modo equivalente alle norme presenti nello Stato membro dell'esportatore. Relativo a 2010/87/UE Clausola 1 e), 4 a) e 5 b)
- Art 145 L'importatore dovrebbe notificare il titolare che non è in grado di conformarsi con le normative Europee ed il titolare dovrebbe interrompere il trattamento/trasferimento o notificare il Garante se vuole continuare a farlo. 2010/87/UE Clausola 5 a) ed e)

Avete ricevuto notifiche in merito dal vostro Cloud provider?

Avete interrotto i trattamenti/trasferimenti o notificato il Garante?



Una volta era facile invalidare gli SCC

Articolo 4

1. Fatto salvo il potere di provvedere all'osservanza delle disposizioni nazionali adottate in attuazione dei capi II, III, V e VI della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei poteri loro attribuiti per vietare o sospendere i flussi di dati verso paesi terzi allo scopo di proteggere le persone con riguardo al trattamento dei dati personali, qualora:

- a) sia accertato che, in base alla legge ad esso applicabile, l'importatore o il subincaricato è tenuto ad applicare deroghe alla normativa sulla protezione dei dati che eccedono le restrizioni ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva 95/46/CE e pregiudicano significativamente le garanzie previste dalla normativa sulla protezione dei dati e dalle clausole contrattuali tipo;
- b) un'autorità competente abbia accertato che l'importatore o il subincaricato non ha rispettato le clausole contrattuali tipo riportate in allegato; oppure
- c) sia probabile che le clausole contrattuali tipo in allegato non vengano rispettate e che la prosecuzione del trasferimento determini un imminente rischio di gravi danni per le persone cui i dati si riferiscono.

Ma la [Commissione Europea nel 2016](#) dopo Schrems I (Invalidazione Safe Harbor) ha eliminato i punti dell'articolo 4 che avrebbero escluso l'uso degli SCC ed hanno addossato la responsabilità sui titolari del trattamento.

In termini ancora più semplici...

Come da FAQ dell EDPB:

Mi avvalgo di SCC con un importatore di dati negli Stati Uniti, cosa devo fare?

“La Corte ha rilevato che la normativa degli Stati Uniti (Art. 702 della FISA ed EO 12333) non garantisce un livello di protezione sostanzialmente equivalente.”

Step da seguire per i titolari del trattamento:

- 1) Data Protection Impact Assessment
- 2) Implementazione misure aggiuntive adeguate per proteggere la privacy
- 3) Interrompere il trattamento/trasferimento dei dati o informare il Garante

Se il titolare del trattamento usa responsabili del trattamento statunitensi e/o loro filiali Europee è estremamente probabile che non siano conformi con il RGPD!



Misure aggiuntive necessarie

Alcune raccomandazioni fornite da EDPB:

- Crittografare i dati prima di effettuare il trasferimento (Caso 1)
La chiave di crittografia non deve essere resa disponibile al responsabile del trattamento
- Esportazione dei dati in forma pseudonimizzata (Caso 2)
L'importatore non deve avere accesso a metodi o dati per ri-identificare gli interessati
- Trasferimento in chiaro dei dati personali (Caso 6)
Nessuna soluzione idonea è al momento disponibile

Se usate servizi come Microsoft 365 o G Suite dove i dati personali non sono crittografati alla fonte state violando i diritti fondamentali degli interessati e **non siete conformi con il RGPD...**



Stop!... lo dice chiaramente anche EDPB

Where you are not able to find or implement effective supplementary measures that ensure that the transferred personal data enjoys an essentially equivalent level of protection,⁵⁵ you must not start transferring personal data to the third country concerned on the basis of the Article 46 GDPR transfer tool you are relying on. If you are already conducting transfers, you are required to suspend or end the transfer of personal data.⁵⁶ Pursuant to the safeguards contained in the Article 46 GDPR transfer tool you are relying on, the data that you have already transferred to that third country and the copies thereof should be returned to you or destroyed in their entirety by the importer.⁵⁷

Example: the law of the third country prohibits the supplementary measures you have identified (e.g. prohibits the use of encryption) or otherwise prevents their effectiveness. You must not start transferring personal data to this country, or you must stop ongoing existing transfers to this country.

Vi hanno promesso che comunque i dati rimangono in Europa?

La nota 22 a pagina 8 delle raccomandazioni ci ricorda:

Anche l'accesso remoto da una nazione terza a dati localizzati nell'Area Economica Europea è da considerarsi un trasferimento

... e comunque se non è scritto nel contratto non ha alcun valore.

Un trattamento o un un trasferimento?

Come da FAQ di EDPB:

"Mi avvalgo di un responsabile del trattamento che tratta dati per mio conto, essendo io il titolare del trattamento. Come posso sapere se il mio responsabile del trattamento trasferisce i dati verso gli Stati Uniti o un altro paese terzo?

Il contratto stipulato con il responsabile in conformità dell'articolo 28, paragrafo 3, del RGPD deve stabilire se i trasferimenti siano o meno autorizzati (occorre tenere presente che costituisce un trasferimento anche l'accesso ai dati effettuato a partire da un paese terzo, ad esempio a fini amministrativi).

Occorre un'autorizzazione anche per consentire a un responsabile di affidare a sub-responsabili del trattamento il trasferimento di dati verso paesi terzi. È necessaria particolare attenzione perché numerose soluzioni informatiche possono comportare il trasferimento di dati personali verso un paese terzo (ad esempio, a fini di conservazione o manutenzione)."



Come continuare ad usare quelle piattaforme

Se volete continuare ad utilizzare piattaforme Cloud non conformi potete:

- Chiedere il consenso informato agli interessati mettendoli al corrente del fatto che verranno trasferiti e trattati da responsabili del trattamento che, a causa delle leggi a cui sono soggetti, probabilmente violeranno i loro diritti fondamentali.
- Notificare il Garante della vostra intenzione di continuare ad utilizzare tali piattaforme
- Attendere che il Garante dia il benestare o confermi che dovete interrompere il trattamento
- Opzionalmente potete provare a convincere il Governo statunitense a non violare i diritti fondamentali dei cittadini europei



Avete per caso letto i contratti? Un'esempio

Nota: solo per questioni di brevità presentiamo il caso di un provider ma simili problematiche contrattuali si applicano a un gran numero di provider diversi.

Microsoft Online Services DPA:

“Trasferimenti dei Dati (Pagina 10)

....Tenendo conto di tali misure di sicurezza, la **Società chiede a Microsoft di trasferire i Dati della Società e i Dati Personali negli Stati Uniti o in qualunque altro paese** in cui Microsoft o gli Altri suoi Responsabili del Trattamento sono presenti e di archiviare e trattare i Dati della Società e i Dati Personali per erogare i Servizi Online, fatto salvo quanto descritto in altri Articoli delle Condizioni dell'Addendum.

Tutti i trasferimenti dei Dati della Società e dei Dati Personali fuori dall'Unione Europea, dallo Spazio Economico Europeo, dal Regno Unito e dalla Svizzera per erogare i Servizi Online verranno disciplinati dalle Clausole Contrattuali Tipo contenute nell'Allegato 2.”

**Strano che in tanti continuino a dire che sono conformi perché i dati sono sempre in Europa.
(anche ignorando che l'accesso da paese terzo equivale ad un trasferimento)**

E se il titolare è una scuola?

Microsoft Online Services DPA:

“Istituti scolastici (Pagina 11)

....La Società comprende che Microsoft potrebbe non avere a disposizione alcuna informazione di contatto o avere solo informazioni limitate relativamente agli studenti della Società e ai loro genitori. Di conseguenza, **la Società avrà la responsabilità di ottenere l'autorizzazione dei genitori** per l'eventuale utilizzo del Servizio Online da parte degli utenti finali in conformità alla legge applicabile e di presentare per conto di Microsoft agli studenti (**o, nel caso di uno studente di età inferiore ai 18 anni e che non frequenti un istituto di studi superiori, al genitore dello studente**) l'eventuale ordine di comparizione in tribunale o ordinanza legalmente emanata che richieda la divulgazione dei Dati della Società in possesso di Microsoft in conformità alla legge applicabile.”

Quanti genitori hanno ricevuto una richiesta di autorizzazione o di consenso informato dove le implicazioni relative al trattamento e trasferimento di dati sono state chiaramente(!) spiegate?

Il titolare dichiara di essere il colpevole

Microsoft Online Services DPA:

“Clausola 4. Obbligazioni dell’esportatore (Pagina 21 – SCC non valide)

L’esportatore dichiara e garantisce:

(a) che il trattamento, compreso **il trasferimento, dei dati personali, è stato e continuerà a essere effettuato in conformità a tutte le disposizioni pertinenti della normativa applicabile sulla protezione dei dati personali** (e, a seconda dei casi, è stato comunicato alle autorità competenti dello Stato Membro in cui ha sede l’esportatore) e nel pieno rispetto delle disposizioni specifiche di quello Stato;

(f) che, qualora il trasferimento riguardi categorie particolari di dati, **gli interessati sono stati o saranno informati prima del trasferimento**, o immediatamente dopo, che i dati che li riguardano potrebbero essere trasmessi **a un paese terzo che non garantisce una protezione adeguata** ai sensi della Direttiva 95/46/CE; ”

Il titolare ha sicuramente fatto una DPIA, ha sicuramente valutato se il trattamento viene fatto seguendo tutte le normative vigenti e naturalmente ha informato gli interessati che i loro dati particolari/speciali verranno trasferiti dove non viene garantita una protezione adeguata. Vero?

EDPS Public Paper on

**Outcome of own-initiative
investigation into EU
institutions' use of Microsoft
products and services**

Anche i DPO non aiutano molto

Diverse risposte a richieste dimostrano:

- Scarsa conoscenza del RGPD
- Non al corrente di Schrems II
- Non seguono raccomandazioni di EDPB
- Non intendono disturbare lo status quo
- Non formano il personale correttamente



Alcuni elementi di base

- Sovranità tecnologica
 - Open Source
 - Public money, public code
- Open Data per il bene pubblico
- Interoperabilità per “aprire” il mercato (es. ODF)

“Ma così fan tutti... e non ci sono alternative”

Invece di dire che non potete farci nulla, iniziate ad implementare alternative



Gli strumenti necessari sono già disponibili



Grazie!

Paolo Vecchi
Omnis Cloud (Luxembourg)



Quest'opera è distribuita con Licenza Creative Commons
Attribuzione/Condividi allo stesso modo 4.0 Internazionale.

About this presentation

Presentation created with:



Broadcasted using:



Disclaimer:

The information included in this presentation may not be complete and could be misinterpreted as more information and explanation was provided during the event.

If you think some of the data is incorrect or depict your organisation in a way you don't like, we are happy to discuss your concerns at our next public event.

Images used are believed not to be covered by copyright or any restriction when used in public presentation. If you believe any of the content should not be used in this presentation please let us know and we'll act on your request promptly.

Logos, names and trademarks are proprieties of their respective owners.

No computers or other electronic devices have been subjected to cruelties and/or the use of Microsoft products to create this presentation.