Apple aiuta la Cina a tracciare gli utenti? No, però…

Ott 15, 2019 Marco Schiaffino Gestione dati, In evidenza, News, Privacy, RSS, Scenario 0

L'azienda di Tim Cook smentisce le voci riguardanti rischi per la privacy legati all'uso della navigazione sicura su Safari in Cina. Nessun tracciamento, ma c'è il rischio censura.

Ogni volta che si parla di **Apple** e della sua attività in **Cina**, spuntano puntualmente polemiche e accuse. L'azienda di Cupertino, in particolare, viene considerata da molti un po' troppo accondiscendente con le richieste del governo di Pechino.

Per rimanere solo ai casi più recenti, ad Apple viene rinfacciato per esempio di aver rimosso le app con servizi di VPN per gli utenti cinesi, di aver eliminato dal suo store l'applicazione usata dai manifestanti a **Hong Kong** per tracciare i movimenti della polizia e di aver assecondato l'eliminazione di ogni riferimento a **Taiwan** (come l'emoticon la bandiera taiwanese) sui suoi dispositivi.

L'ultima polemica in ordine di tempo riguarda **Safari** e la funzionalità di navigazione sicura, che sul browser Apple è impostata come opzione predefinita.

Si tratta di una funzione presente in tutte le versioni di Safari e che ha come scopo quello di bloccare la navigazione e inviare una segnalazione all'utente quando si sta per collegare a un sito Internet potenzialmente pericoloso.

Nel resto del mondo, Apple utilizza a questo scopo un database gestito da **Google**. In Cina, dove Google è bloccato, utilizza però il servizio di **Tencent**, azienda cinese molto “vicina” al governo di Pechino.

L’accusa, ripresa da molti siti di news generalisti, è che in questo modo Apple permetta alle autorità cinesi di tracciare la navigazione degli utenti Apple sul territorio della Repubblica Popolare.

L’azienda di Tim Cook, però, respinge ogni accusa. La funzione di navigazione sicura (nelle impostazioni è indicata come “Avvisi siti web fraudolenti”) funzionerebbe infatti attraverso un meccanismo che non comporta la condivisione di alcuna informazione con il soggetto che gestisce il database dei siti considerati pericolosi.

La lista degli indirizzi a rischio, infatti, verrebbe invece inviata al browser sotto forma di hash e confrontata in locale con quelli che l’utente visita. **Insomma: in questo caso**

Tencent non avrebbe alcun modo per tracciare la navigazione degli utenti su iOS o macOS.

“Apple tutela la privacy degli utenti e protegge i dati con Avvisi siti web fraudolenti, una funzione di sicurezza che individua i siti Web noti per essere pericolosi” spiegano dalle parti di Cupertino con un comunicato.

“Quando la funzione è attiva, Safari controlla l’URL del sito confrontandola con un lista di siti Internet conosciuti e visualizza un avviso se l’indirizzo corrisponde a una pagina che può contenere contenuti fraudolenti. Per farlo, Safari riceve una lista da Google e, per i dispositivi che risultano essere in Cina, da Tencent. L’URL non viene mai condivisa con il soggetto che fornisce la lista e la funzione”.

Resta, naturalmente, il problema della possibile censura di siti Internet che vengono indicati come pericolosi quando la loro colpa è solo quella di proporre contenuti sgraditi al governo. Nell’ecosistema dell’Internet cinese, però, non si tratta certo di una novità e, come ricorda la stessa Apple nel comunicato, la funzione di navigazione sicura può essere disabilitata dalle impostazioni di Safari.

Insomma: se i problemi legati alla presenza di Apple in Cina rimangono, per questa volta si è trattato della classica tempesta in un bicchier d’acqua.

Condividi l’articolo

Per l’Italia Simjacker è un problema

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/15/apple-aiuta-la-cina-a-tracciare-gli-utenti-no-pero/

Per l'Italia Simjacker è un problema

Ott 14, 2019 Marco Schiaffino Attacchi, In evidenza, News, Privacy, Vulnerabilità 0

Nuovo rapporto sulla vulnerabilità che permette di spiare i telefoni attraverso la SIM. I paesi interessati sono solo 29 e l'Italia è tra questi.

Buone notizie (per il mondo) sulla vicenda **Simjacker**. Stando a un nuovo report di **AdaptiveMobile Security**, infatti, la vulnerabilità individuata lo scorso settembre dai ricercatori della società di sicurezza impatterebbe solo 61 operatori mobile in 29 paesi. **La cattiva notizia (per l'Italia) è che il nostro paese rientra nell'elenco**.

Come abbiamo spiegato in questo articolo, Simjacker è una falla di sicurezza che fa leva su un'applicazione integrate nelle SIM che non riceve alcun aggiornamento dal 2009 e può essere sfruttata per inviare comandi tramite degli SMS contenenti un particolare codice.

I messaggi, la cui ricezione non viene notificata in alcun modo al proprietario del telefono, permettono di eseguire numerose operazioni, come "estrarre" la posizione del telefono

attraverso il GPS, avviare telefonate o aprire collegamenti nel browser.

In altre parole, Simjacker può essere usato per monitorare gli spostamenti di una persona, mettere a segno truffe telefoniche "forzando" chiamate verso numeri a pagamento o **installare un malware attraverso una pagina Web infetta**.

L'approfondimento dei ricercatori si è concentrato sulla mappatura degli operatori telefonici mobili che usano ancora **S@T Browser**, l'applicazione che consente l'invio dei comandi in remoto. Il risultato è piuttosto sorprendente.

I 29 paesi a rischio, infatti, sono per la maggior parte in Sud America, mentre sono esclusi Stati Uniti e la stragrande maggioranza dei paesi europei. **Nel vecchio continente le nazioni a rischio sono solo tre: Bulgaria, Cipro e Italia**.

Il report di AdaptiveMobile Security non specifica quali siano le compagnie telefoniche interessate, ma fa una stima complessiva sul numero di SIM vulnerabili all'attacco. **I**

ricercatori parlano di un numero variabile tra i 500 e gli oltre 800 milioni di SIM.

L'approssimazione è dovuta al fatto che anche gli operatori che usano S@T Browser, in molti casi lo hanno dismesso e, di conseguenza, il problema potrebbe essere presente soltanto sulle vecchie SIM.

Per il momento, nessuno ha registrato ondate di attacchi che sfruttano Simjacker. Gli unici episodi si sarebbero verificati in Messico, Colombia e Perù.

Condividi l'articolo

Apple aiuta la Cina a tracciare gli utenti? No, però… Red Team o Blue Team? Adesso c'è anche il Purple Team… ed è una macchina

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/10/14/per-litalia-simjacker-e-un-problema/

Analisi UE dei rischi legati al 5G, ma l'obiettivo è

Huawei

Ott 10, 2019 Marco Schiaffino Gestione dati, In evidenza, Mercato, News, Privacy, RSS, Scenario, Tecnologia, Vulnerabilità 0

Il report congiunto evidenzia le criticità legate alla nuova tecnologia. E si parla di rischio elevato nel caso in cui si utilizzino infrastrutture fornite da un unico produttore…

Fino a oggi la crociata dell'amministrazione USA contro **Huawei** aveva incontrato una certa freddezza da parte dei paesi dell'Unione Europea. Anzi: come abbiamo spiegato in questo articolo, le poche voci che si erano levate sembravano puntare a smorzare le polemiche sulla scelta del fornitore per le infrastrutture 5G.

Adesso, però, l'aria è decisamente cambiata. Nella giornata di ieri, infatti, il commissario europeo per l'Unione della sicurezza **Julian King** (una dicitura curiosa, ma è quella riportata dalla versione italiana del sito della Commissione Europea – ndr) ha presentato un report sulla valutazione dei rischi legati al network 5G.

Nel dettaglio, il comunicato stampa della Commissione Europea evidenzia come il report sottolinei una serie di criticità, tra cui **una maggiore esposizione agli attacchi e un maggior numero di punti di accesso potenziali per attacchi informatici** provocata dalla "dipendenza" dai software per la gestione della rete. Il rischio, in pratica, è che ogni bug software si traduca in una nuova vulnerabilità con conseguenze sulla sicurezza.

Proseguendo nella lettura, però, cominciano a emergere elementi che sembrano puntare direttamente a "minare" i

progetti di Huawei. Ad esempio quando il report evidenzia come le nuove caratteristiche della rete 5G comportino il fatto che alcuni componenti diventeranno più "sensibili", o quando si fa riferimento a **una maggiore "dipendenza" da parte degli operatori mobile nei confronti dei fornitori di tecnologia**.

La vera mazzata arriva però quando si parla di una "particolare importanza" nel p**rofilo di rischio collegato ai singoli fornitori**, in particolare riguardo "la possibilità che il fornitore sia soggetto a interferenze da parte di un governo esterno alla UE."

E ancora, come "la dipendenza da un singolo fornitore" possa creare problemi sia sotto il profilo dei rischi di un fallimento a livello commerciale, sia a livello dell'impatto generalizzato di eventuali vulnerabilità nei suoi sistemi.

Insomma, il messaggio inviato dalla Commissione Europea è chiaro: **Huawei non può pensare di essere l'unico fornitore tecnologico per la nuova rete 5G**.

La chiusa di questo elenco, poi, non lascia molto spazio a

interpretazioni: “*Le minacce alla disponibilità e all’integrità delle reti diventeranno importanti problemi di sicurezza: oltre alle minacce alla riservatezza e alla privacy, in una situazione in cui le reti 5G che dovrebbero diventare la spina dorsale di molte applicazioni IT critiche l’integrità e la disponibilità di tali reti diventeranno i principali problemi di sicurezza nazionale e una priorità in termini di sicurezza per l’Unione Europea*”.

Dalle parti di Huawei non l’hanno presa benissimo, ma la società ha reagito adottando la tradizionale linea ispirata alla prudenza, cercando di mantenere la vicenda all’interno di confini quanto più possibile “neutri”. In un comunicato stampa, l’azienda di Shenzhen dice di essere “contenta” del fatto che il rapporto si concentri su aspetti oggettivi e **non faccia riferimento esplicitamente a singole nazioni e governi**. Auspica poi che questo approccio “basato sui fatti” ispiri anche le future attività in questo settore.

Tra le righe, però, c’è anche una velata minaccia. Soprattutto quando si legge “*la forte e perdurante collaborazione con i nostri partner europei è un’opportunità unica per l’Europa per mantenere la sua leadership tecnologica*”. Il ragionamento è chiaro: senza di noi il 5G non lo fate.

Condividi l’articolo

Vittima del ransomware Muhstik reagisce hackerando i pirati

Articoli correlati

Altro in questa categoria

---

egati-al-5g-ma-lobiettivo-e-huawei/

Twitter transgression proves why its flawed 2FA system is such a privacy trap

reader comments

106 with 84 posters participating

Share this story

If ever there was a surefire way to sour users against a two-factor authentication system that was already highly flawed, Twitter has found it. On Tuesday, the social media site said that it used phone numbers and email addresses provided for 2FA protection to tailor ads to users.

Twitter requires users to provide a valid phone number to be eligible for 2FA protection. A working cell phone number is mandatory even when users’ 2FA protection is based solely on security keys or authenticator apps, which don’t rely on phone numbers to work. Deleting a phone number from a user’s Twitter settings immediately withdraws an account from Twitter 2FA, as I confirmed just prior to publishing this post.

Security and privacy advocates have long grumbled about this requirement, which isn’t a condition of using 2FA protection from Google, Github, and other top-ranked sites. On Tuesday, Twitter gave critics a new reason to complain. The site said it may have inadvertently used email addresses and phone numbers provided for 2FA and other security purposes to match users to marketing lists provided by advertisers. Twitter didn’t say if the number of users affected by the blunder was in the hundreds or the millions or how long the improper targeting lasted.

Company officials wrote:

> *We cannot say with certainty how many people were impacted by this, but in an effort to be transparent, we wanted to make everyone aware. No personal data was ever shared externally with our partners or any other third parties. As of September 17, we have addressed the issue that allowed this to occur and are no longer using phone numbers or email addresses collected for safety or security purposes for advertising.*

Security advocates, including Matt Green—a Johns Hopkins professor specializing in cryptography—wasted no time castigating Twitter for the gaffe.

“In all seriousness: whose idea was it to use a valuable advertising identifier as an input to a security system,” he wrote on Twitter. “This is like using raw meat to secure your tent against bears.”

> *In all seriousness: whose idea was it to use a valuable advertising identifier as an input to a security system. This is like using raw meat to secure your tent against bears.*
>
> *— Matthew Green (@matthew_d_green) October 8, 2019*

Not all 2FA was created equal

Two-factor authentication has emerged as the single-most effective means for protecting accounts against phishing and so-called credential-stuffing attacks (the latter uses passwords swept up in breaches on one site to guess passwords on unrelated sites). As the name suggests, 2FA requires a factor—for example, a security key or a fingerprint—in addition to a password to successfully log in from a device that has never accessed the account before.

Over the past few years, security practitioners have increasingly turned away from 2FA based on SMS text messages. The reasons: (1) attackers can take control of users’ phone numbers by impersonating the owners and getting the carrier to swap out the SIM card, and (2) SMS messages can be hijacked through weaknesses in the Signalling System No. 7 routing protocol that cellular carriers use to make their networks interoperable. Attackers have been known to actively exploit these weaknesses more than once. A far more effective means of 2FA relies on physical security keys that connect over USB or NFC interfaces or—less secure but still better than SMS—one-time passwords generated by authenticator apps. Twitter allows either form of 2FA. Both require a user to provide a phone number.

Twitter signals a change is coming

Twitter representatives declined to answer on the record why a phone number is required to use 2FA. A representative on background, however, said that the requirement is based on previous experiences in which users frequently lost access to other 2FA methods and were locked out of accounts with no way to recover. Twitter officials now recognize that tying 2FA to a phone number isn't ideal, and they are looking for ways to decouple the two in the future.

Last year, Facebook was outed for using 2FA-provided phone numbers to send notifications that weren't related to security. The social network said the behavior was the result of a bug.

While SMS-based 2FA isn't ideal, it's still better for most people than no 2FA at all—at least when services don't use phone numbers for marketing purposes.

https://arstechnica.com/?p=1582055

Senator proposes mandatory labeling for products with mics, cameras



Enlarge / A surveillance camera on display in Hamburg, Germany, in January 2019.

reader comments

131 with 69 posters participating

Share this story

Much in the same way that food labels are now required to disclose the potential presence of allergens such as peanuts, one Senator is proposing a law that would require tech companies to include a label on products disclosing the presence of recording devices.

The bill, dubbed the Protecting Privacy in our Homes Act, would mandate a new kind of labeling on goods that include Internet-connected microphones or cameras. The proposed law does not define what kind of labels would need to be appended but rather would order the Federal Trade Commission to put in place specific regulations “under which each covered

manufacturer shall be required to include on the packaging of each covered device manufactured by the covered manufacturer a notice that a camera or microphone is a component of the covered device."

Sen. Cory Gardner (R-Colo.) introduced the bill to the Senate. "Consumers face a number of challenges when it comes to their privacy, but they shouldn't have a challenge figuring out if a device they buy has a camera or microphone embedded into it," Gardner said. "This legislation is about consumer information, consumer empowerment, and making sure we're doing everything we can to protect consumer privacy."

Most products that ship with cameras or microphones included tout the inclusion of such recording devices as a selling point, which could make this kind of regulation feel redundant at best. That said, there's quite a difference between "most" and "all." A rule such as the regulation Gardner proposes would close the gap that, for example, led owners of Nest Secure devices to the unpleasant discovery earlier this year that the products had shipped with undisclosed microphones.

Gardner is a co-chair of the Senate Cybersecurity Caucus, along with Sen. Mark Warner (D-Va.). The two earlier this year led a bipartisan group of senators that co-sponsored the Internet of Things Cybersecurity Act of 2019, which would require existing regulators to develop security standards for connected devices.

The Senate, however, largely seems concerned with other events this year, and GovTrack.us gives the PPHA a 3% chance of actually becoming law.

https://arstechnica.com/?p=1581691

Inexpensive, unpatched phones put billions of users' privacy at risk



Enlarge / Cellphones charging in the Philippines at a station run by generator in 2013, while power was out in the wake of tyhpoon Haiyan.

reader comments

116 with 65 posters participating, including story author

Share this story

Privacy, it seems, is increasingly a luxury reserved for those who can afford it. "Free" services are rarely free, and in the 21st century, the adage seems to be that if you aren't paying with your money, you're paying with your personal data. But while a user at the higher ends of the income scale can afford

to be choosy with both their cash and their privacy, users of the cheap, mostly Android-based smartphones that dominate the market worldwide are bearing the burden.

Apple’s iPhone might be the single most popular device line among US consumers, but the iPhone’s high-end cachet comes with a matching price tag. Likewise, a premium flagship Android phone, such as a new Google Pixel or Samsung Galaxy device, runs in the $500 to $1000 range.

Connectivity, however, is happily not limited to just the global wealthy. Billions of users in both developing and mature economies to whom the price tag puts a high-end phone out of reach still have access to lower-spec devices. Nearly all of the lower-end phones available worldwide run Android, giving Google’s OS a greater than 80% market share globally.

Android is easily modifiable by device manufacturers and wireless carriers, and the cheaper the phone is, the more likely it is that someone, or multiple someones, has installed crapware or malware on it, Fast Company reports.

Fast Company highlights one example: the MYA2 MyPhone, sold in the Philippines. The phone as described is a privacy and security nightmare:

> *First, it comes with an outdated version of Android with known security vulnerabilities that can’t be updated or patched. The MYA2 also has apps that can’t be updated or deleted, and those apps contain multiple security and privacy flaws. One of those pre-installed apps that can’t be removed, Facebook Lite, gets default permission to track everywhere you go, upload all your contacts, and read your phone’s calendar.*

The wealth gap

According to data gathered by the Pew Research Center, about 17% of US adults use smartphones and *only* smartphones to connect to the Internet. The farther down the household-income ladder you go, the higher that percentage is. Among those whose household income falls between $50,000 and $75,000, about 10% of users are mobile-only. Among those whose household incomes fall below $30,000, the figure rises to 26%.

Fast Company points to a recently published study conducted by researchers at the University of Pennsylvania and Rutgers University. The study finds that many mobile-only, lower-income consumers were well aware that their privacy was regularly being violated, but they didn't feel they had a real choice.

"Nearly all study participants shared stories of relinquishing their data privacy, which the researchers consider to be a basic human right, in exchange for the ability to access online services and platforms," the researchers wrote. "Many people shared anecdotes about forgoing opportunities in an attempt to maintain data privacy."

The researchers concluded:

> *Because of the sheer ubiquity of digitized data compiled on individuals who rely on cell phones to access the Internet, the need for privacy should be elevated from a personal liberty and legal right to a matter of social justice… Data privacy is not a luxury for those who cannot afford to invest the time, resources, and effort required to actively protect one's digital assets.*

Global challenge

Fast Company notes that approximately 2 billion users, or just over half of all people now online, only access the Internet on their smartphones. That number is projected to be as high as 3.7 billion users by 2025, as mobile infrastructure solidifies a foothold and gains penetration in currently underserved regions.

The problem is not new, and it’s not limited to users in developing economies or low-GDP nations. In 2016, for example, 120,000 Android phones distributed inside the US by BLU Products were found to be sending users’ text messages and other highly sensitive data to China. The security hole was not a bug but a feature of the phones—the phones just weren’t meant to be distributed that way inside the United States.

(BLU reached a settlement with the Federal Trade Commission in April 2018.)

Dozens of other models of Android phones have been found in recent years to arrive pre-loaded with malware or boasting backdoors that should not be—particularly phones distributed by low-cost resellers.

And the trade-off isn’t always surreptitious. In 2016, for example, Amazon launched a program selling cheap, unlocked Android phones with “special offers” (i.e. advertisements) baked into the lock screen and certain pre-installed apps. The company dumped the program in 2018 after Google changed the terms of its developer policy.

https://arstechnica.com/?p=1581257

Why big ISPs aren’t happy about Google’s plans for encrypted DNS



reader comments

142 with 77 posters participating

Share this story

When you visit a new website, your computer probably submits a request to the domain name system (DNS) to translate the domain name (like arstechnica.com) to an IP address. Currently, most DNS queries are unencrypted, which raises privacy and security concerns. Google and Mozilla are trying to address these concerns by adding support in their browsers for sending DNS queries over the encrypted HTTPS

protocol.

But major Internet service providers have cried foul. In a September 19 letter to Congress, Big Cable and other telecom industry groups warned that Google's support for DNS over HTTPS (DOH) "could interfere on a mass scale with critical Internet functions, as well as raise data-competition issues."

On Sunday, the *Wall Street Journal* reported that the House Judiciary Committee is taking these concerns seriously. In a September 13 letter, the Judiciary Committee asked Google for details about its DOH plans—including whether Google plans to use data collected via the new protocol for commercial purposes.

But Google says that these concerns are groundless. Despite insinuations from telecom companies, Google says, the company has no plans to switch Chrome users to its own DNS servers. And while Google didn't mention it, the company has plenty of ways to monitor users' browsing patterns with or without access to their DNS queries.

The telecom industry letter is confusing because it mashes together two different criticisms of Google's DOH plans. One concern is that switching to encrypted DNS would prevent ISPs and others from spying on their users. The other is that, in the process of enabling DOH, Google will switch millions of users over to Google's own DNS servers, leading to a dangerous concentration of control over DNS.

Understanding the debate is easier if we consider each of these concerns separately.

Google says it isn't planning to switch users to its DNS

Let's start with the second concern: that Google will switch Chrome users to its own DNS servers, giving Google

concentrated power over DNS. Google's response here is simple.

"Google has no plans to centralize or change people's DNS providers to Google by default," the company said in an email to Ars Technica. "Any claim that we are trying to become the centralized encrypted DNS provider is inaccurate."

Google laid out its plans in detail in a September 10 blog post. Starting with version 78, Chrome will begin experimenting with the new DOH feature. Under the experiment, Chrome will "check if the user's current DNS provider is among a list of DoH-compatible providers, and upgrade to the equivalent DoH service from the same provider," Google wrote. "If the DNS provider isn't in the list, Chrome will continue to operate as it does today."

One possible reason for confusion on this point is that Mozilla is planning a more aggressive rollout of the technology. The company is planning to gradually shift all of its users to DOH—whether or not their existing DNS provider supports it. The shift will make Cloudflare the default DNS provider for many Firefox users, regardless of the DNS settings of the underlying OS.

Mozilla has more latitude to do this because most surveys show Firefox with single-digit market share—and Firefox isn't a major DNS provider in its own right. So there'd be little basis for antitrust scrutiny if Mozilla shifts its users over to a new DNS provider. The same move could raise antitrust concerns if Google started switching Chrome users over to its own DNS. But Google says it has no plans to do that.

DNS over HTTPS means ISPs can't spy on their users



Enlarge / Google CEO Sundar Pichai.
Simon Dawson/Bloomberg via Getty Images

Telecom companies also raised a second concern that applies even if Google doesn't shift anyone to its own DNS servers. Put simply: the lack of DNS encryption is convenient for ISPs.

ISPs sometimes find it useful to monitor their customers' Internet traffic. For example, queries to malware-associated domains can be a signal that a customer's computer is infected with malware. In some cases, ISPs also modify customers DNS queries in-flight. For example, an easy way to block children from accessing adult materials is with an ISP-level filter that re-writes DNS queries for banned domains. Some public Wi-Fi networks use modified DNS queries as a way to redirect users to a network sign-on page.

Some ISPs also use DNS snooping for more controversial purposes—like ad targeting or policing their networks for copyright infringement.

Widespread adoption of DOH would limit ISPs' ability to both monitor and modify customer queries. It wouldn't necessarily

eliminate this ability, since ISPs could still use these techniques for customers who use the ISP's own DNS servers. But if customers switched to third-party DNS servers—either from Google or one of its various competitors—then ISPs would no longer have an easy way to tell which sites customers were accessing.

ISPs could still see which IP addresses a customer had accessed, which would give them some information—this can be an effective way to detect malware infections, for example. But this is a cruder way to monitor Internet traffic. Multiple domains can share a single IP address, and domains can change IP addresses over time. So ISPs would wind up with reduced visibility into their customers' browsing habits.

What would a switch mean?

But a switch to DOH would clearly mean ISPs had less ability to monitor and manipulate their customers' browsing activity. Indeed, for advocates that's the point. They believe users, not their ISPs, should be in charge.

Mozilla, which is pushing DOH more aggressively than Google, has taken steps to avoid creating too much chaos in the process. In July, Mozilla said that it wouldn't enable DOH by default in the UK, where ISPs are planning to use DNS to implement legally mandated porn filtering.

Before enabling DOH, Firefox will check if a computer has parental control software installed. In enterprise settings, Mozilla will try to figure out if a switch to DOH will break corporate Intranet features that depend on using specific DNS servers. Firefox will continue using the existing DNS servers in these cases.

So far, Google is only enabling DOH for a selected number of whitelisted DNS providers, so the switch shouldn't cause too many problems. If the company goes beyond that, we can expect

it to take measures similar to those Mozilla has taken.

In any event, it’s hard to see a policy problem here. ISPs’ ability to eavesdrop on their customers’ DNS queries is little more than an historical accident. In recent years, websites across the Internet have adopted SSL encryption for the contents of their sites. The encryption of DNS is the natural next step toward a more secure Internet. It may require some painful adjustments by ISPs, but that hardly seems like a reason for policymakers to block the change.

https://arstechnica.com/?p=1576941

Gdpr, conforme solo il 21% delle imprese italiane. Cloud principale abilitatore

In tutto il mondo meno di un terzo delle imprese si può dichiarare conforme al regolamento generale europeo sul trattamento dei dati o **Gdpr** (acronimo inglese per *General data protection regulation*). Appena il **28% delle aziende** è riuscito a soddisfare pienamente quanto richiesto dalla normativa.

Tuttavia, le aziende stanno scoprendo i vantaggi derivanti dalla conformità al regolamento: **l’81% di coloro che sono in linea con il GDPR afferma di aver avuto un impatto positivo in termini di reputazione e brand image**.

È quanto emerso dallo studio pubblicato dal **Capgemini Research Institute** dal titolo “**Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century**”, in cui si è indagato ed esaminato il grado di adozione della

normativa Gdpr da parte delle organizzazioni a più di un anno dall'entrata in vigore.

In Italia solo il 21% delle imprese può dirsi conforme al Gdpr. Stessa percentuale in Spagna, ancora meno in Svezia (18%), molto meglio negli Stati Uniti (35%), Regno Unito e Germania (entrambe con il 33%).

Per i dirigenti, le sfide sono legate all'allineamento dei sistemi IT legacy (38%), dalla complessità dei requisiti del regolamento (36%) e dai costi proibitivi che vanno sostenuti per essere in linea con gli stessi (33%).

In termini economici, le aziende dichiarano di effettuare investimenti significativi per coprire i costi relativi all'aumento delle commissioni professionali legate alla conformità con il **Gdpr: il 40% stima che, nel 2020, spenderà oltre un milione di dollari per spese legali**, mentre il 44% ritiene che questa sarà la cifra da investire per effettuare aggiornamenti in ambito tecnologico.

L'innovazione tecnologica sembra avere un ruolo abilitatore nell'adozione del regolamento.
Le aziende conformi, si legge nello studio, hanno maggiori probabilità di utilizzare piattaforme ***cloud*** (84% rispetto al 73% di quelle non conformi), **crittografia** dei dati (70% vs. 55%), ***Robotic Process Automation*** (35% vs. 27%) e **conservazione dei dati** industrializzati (20% vs. 15%).

Gdpr, inoltre, non vuol dire solo spese da sostenere e regole da rispettare, perché i vantaggi sono numerosi.
La stragrande maggioranza dei dirigenti delle aziende conformi al regolamento ha dichiarato di aver assistito a un **impatto positivo sulla fiducia dei clienti** (84%), sulla *brand image* (81%) e sul morale dei dipendenti (79%).
Gli stessi manager hanno identificato gli **effetti positivi** secondari dell'implementazione del Gdpr tra cui miglioramenti

nei sistemi IT (87% rispetto al 62% del 2018), nelle pratiche di ***cybersecurity*** (91% vs. 57%) e in cambiamenti e trasformazioni a livello di organizzazione (89% vs. 56%).

https://www.key4biz.it/gdpr-conforme-solo-il-21-delle-imprese-italiane-cloud-principale-abilitatore/272648/

Vimeo collected detailed facial scans without consent, lawsuit alleges



reader comments

27 with 23 posters participating

Share this story

Vimeo is collecting and storing thousands of people’s facial biometrics without their permission or knowledge, a recently filed lawsuit alleges.

The “highly detailed geometric” facial maps, according to a complaint, are being collected and stored in violation of the Illinois Biometric Information Privacy ACT, or BIPA, according to a complaint filed last week in Illinois state court. The law bars companies from obtaining or possessing an individuals’ biometric identifiers or information unless the company (1) informs the person in writing of its plans to do so, (2) states in writing the purpose and length of term for the collection and storage, (3) receives written permission from the user, and (4) publishes retention schedules and guidelines for destroying the biometric identifiers and information.

The complaint alleges Vimeo is violating the law by collecting, storing, and using the facial biometrics of thousands of unwitting individuals throughout the United States whose faces appear in photos or videos uploaded to the Magisto video-editor application. Vimeo acquired Magisto in April and claimed the editor had more than 100 million users.

“Vimeo has created, collected, and stored, in conjunction with its cloud-based Magisto service, thousands of ‘face templates’ (or ‘face prints’)—highly detailed geometric maps of the face—from thousands of Magisto users,” the complaint alleged.

The complaint adds:

> *Vimeo creates these templates using sophisticated facial-recognition technology that extracts and analyzes data from*

> *the points and contours of faces that appear in photos and videos taken on mobile devices and uploaded to the Magisto app. Each face template that Vimeo extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person.*

The complaint referred to this page that says that Magisto uses "artificial intelligence engines" to analyze videos users upload. The analysis includes "face detection."

The complaint continued:

> *Unbeknownst to the average consumer, and in direct violation of § 15(b)(1) of the BIPA, plaintiff is informed and believes that Magisto's facial recognition technology scans each and every video and photo uploaded to Magisto for faces, extracts geometric data relating to the unique points and contours (i.e., biometric identifiers) of each face, and then uses that data to create and store a template of each face—all without ever informing anyone of this practice.*
>
> *The Magisto service uses these face templates to organize and group together videos based upon the particular individuals appearing in the videos. This technology works by comparing the face templates of individuals who appear in newly-uploaded videos or photos with the facial templates already saved in Magisto's face database. Specifically, when a Magisto user uploads a new video or photo, Magisto's sophisticated facial recognition technology creates a template for each face depicted therein, and then compares each template against Magisto's face template database. If there is a match, then the Magisto service groups the video from which the newly-uploaded face template was derived with the previously uploaded videos depicting that individual.*

Besides using face templates to identify individuals, the service also uses the biometrics to determine the individuals'

gender, age, and location.

The complaint was filed on behalf of Illinois resident Bradley Acaley, who subscribed to Magisto for one year, starting in December 2017, at a cost of $120. He regularly uploaded videos of himself and his family, including his minor children. He would then edit the uploaded videos or create videos from uploaded photos or videos.

Vimeo analyzed Acaley's videos and photos "by automatically locating and scanning plaintiff's face and by extracting geometric data relating to the contours of his face and the distances between his eyes, nose, and ears—data which Vimeo then used to create a unique template of plaintiff's face," the complaint alleged. Vimeo also used the data to recognize Acaley's gender, age, race, and location.

The complaint said that Acaley never received notice of this collection or storage of his biometrics and that he never provided his consent.

Attempts to reach Vimeo representatives for comment were unsuccessful. The company didn't own Magisto at the time Acaley used it, but Vimeo possibly assumed all legal liabilities when it acquired the video-editing service. If that question ever gets sorted out, it will be interesting to see how the court treats the issue of cloud services using facial-recognition analysis to analyze images and videos users willingly uploaded.

https://arstechnica.com/?p=1575655

Microsoft: Customers are entitled to know about federal data requests



David Ryder/Bloomberg via Getty Images

reader comments

52 with 38 posters participating

Share this story

Microsoft revealed on Wednesday that it is fighting in court for the right to tell one of its large enterprise customers about a federal request for data hosted on Microsoft's cloud services. The data request came with an order prohibiting Microsoft from notifying its customer about the request, and Microsoft views the gag order as inappropriate.

“On Sept. 5, 2018, Microsoft challenged a secrecy order issued by a federal magistrate judge in Brooklyn, New York in connection with a federal national security investigation,” wrote Microsoft general counsel Dev Stahlkopf. “Based on the limited information available to us in this case, we feel the secrecy order was too broadly drawn and is inconsistent with the U.S. government’s policy that secrecy orders be narrowly tailored.”

The Microsoft customer in question has thousands of employees. Microsoft argues that the feds should be able to identify someone at the company who can be notified without jeopardizing the investigation. However, a judge rejected Microsoft’s request and left the secrecy requirement in place.

“We have challenged that order in the lower court, and we will pursue an appeal in the appellate court if necessary.”

This appears to be the case Microsoft is referring to. While the case’s docket is available through the court’s PACER system, most of the substantive filings are sealed.

Microsoft has waged a long-and-determined battle against over-broad government secrecy orders. Microsoft successfully fended off an FBI secrecy order in 2014 relating to a customer of Office 365. In 2016, Microsoft sued the Department of Justice over its repeated use of over-broad secrecy orders. In October 2017, the government settled the case by agreeing to limit its use of gag orders.

“As a cloud services provider, Microsoft has an important role in forcing governments to go before impartial judges to justify their conduct,” Stahlkopf wrote in his Wednesday post. “Our thorough review of law enforcement demands helps ensure that governments are respecting the rights of internet users around the world.”

https://arstechnica.com/?p=1575337