Pannolini smart, un chip per notificare ai genitori la pipì. La violazione della privacy dei neonati è totale

Se tuo figlio fa la pipì, popò o dorme arriva la notifica sullo smartphone, così aumenta il tempo trascorso dai genitori attaccati ai telefonini, perché occupati a fare selfie con i figli neonati per condividerli sui social, bypassando la privacy dei bambini per un pugno di like e perdendo di vista ciò che si sta facendo, soprattutto se il fare è affettivo, come osserva la psicoterapeuta **Barbara Volpi**, nella sua rubrica ***Bambini Digitali*** su *Key4biz*.

Ma i pannolini smart in arrivo negli Usa rappresentano soprattutto un rischio privacy per i dati dei più piccoli. Perché? Il sistema di crittografia, che raccoglie le informazioni sui neonati, non prevede l'autenticazione a due fattori: lo standard minimo di sicurezza. E secondo gli esperti, citati dal *Washington Post*, questa vulnerabilità è la porta per *"l'accesso non autorizzato ai sistemi".*

In più i dati finiranno a **Google**, che insieme a **Procter & Gamble**, la società proprietaria di Pampers, ha ideato **Lumi**, la tecnologia IoT infilata nei pannolini.

Google, che proprio in queste ore sta finalizzando con la Federal Trade Commission (**Ftc**) un accordo nell'ambito delle indagini su Youtube per la violazione della legge federale sulla privacy dei bambini. Lo scrive il *Washington Post*, citando due fonti a conoscenza del dossier. Si prevede che Big G paghi una multa multi milionaria ma l'ammontare esatto non è chiaro. La palla ora passa al ministero della giustizia, che raramente capovolge una decisione della Ftc.

Fame degli Ott di dati dei neonati e calo del fatturato, ecco perché nasce il pannolino smart

Il pannolino smart è già sperimentato da un anno in Corea. Nasce per due esigenze:

- Con le nascite in calo, l'unico modo di aumentare il fatturato è quello di vendere pannolini di maggior valore, anche se meno numerosi.
- Il secondo motivo è la fame di dati dei neonati da parte degli Over the top. Il mercato baby tech è in forte crescita: di solito per i figli appena nati i genitori non badano a spese, se poi si aggiunge anche la componente digitale lo stimolo all'acquisto del prodotto smart è accentuato. Ma da neogenitore ci penserei mille volte prima di infilare un chip nel pannolino di mio figlio. Il rischio privacy è altissimo, e in questo modo la violazione è totale perché potrebbe avvenire sui dati sensibili. Meglio toccare il pannolino con la mano per vedere se il bambino ha fatto la pipì o sentire con il naso la popò. Qui l'unico rischio è sentire un cattivo odore. Ma almeno la privacy di tuo figlio è al sicuro.

Pannolini smart, un chip per notificare ai genitori la pipì. La violazione della privacy dei neonati è totale

Quali dati abbiamo diffuso in Rete? Ecco come scoprirlo

Lug 19, 2019 Marco Schiaffino In evidenza, News, Privacy, Prodotto, RSS, Scenario 0

Da F-Secure un sito che permette di collegarsi rapidamente ai servizi di aziende e social network per verificare quali sono i nostri dati che conservano.

Tutela della privacy, gestione responsabile dei dati, diritto all'oblio… teoricamente abbiamo in mano tutti gli strumenti per mantenere il controllo di ciò che condividiamo online e che viene registrato dai vari fornitori di servizio.

Nella pratica, però, il numero di persone che utilizzano davvero tutti questi strumenti è piuttosto esiguo. Il motivo? Oltre alla solita "scarsa sensibilità" sul tema, c'è anche il fatto che l'accesso alle funzionalità di questo tipo non sono sempre intuitive.

Se volessimo usare con un pizzico di malizia, potremmo dire che a concorrere a questa situazione c'è anche il fatto che i giganti del Web non hanno un grande interesse a incentivarne l'uso.

A cercare di sparigliare le carte ci ha pensato **F-Secure**. La società di sicurezza finlandese ha infatti inaugurato un nuovo servizio online chiamato **Data Discovery Portal** e accessibile a questo indirizzo.

Si tratta, in pratica, di un HUB che ci consente di raggiungere con un clic le sezioni dedicate alla gestione dei dati di diversi servizi: da **Google** ad **Apple**, da **Facebook** a **Snapchat**, fino a **Twitter** e **Alexa**.

Attenzione però: non ci troveremo di fronte a un sistema diverso da quello a cui potremmo comunque accedere normalmente. **Semplicemente possiamo farlo in maniera decisamente più rapida**.

La scelta di fare riferimento alle funzioni dei servizi stessi non è dettata da una forma di pigrizia, ma da una impostazione ben precisa. "*Ciò che accade con la raccolta dei dati è una questione che riguarda interamente te e il servizio*" spiega **Erka Koivunen**, Chief Information Security Officer di F-Secure. "*Non vediamo – né vogliamo vedere – le tue impostazioni o i tuoi dati. Il nostro unico scopo è aiutarti a scoprire quanto delle tue informazioni è là fuori*."

Molte persone, infatti, tendono a sottovalutare la portata del

fenomeno. “*Spesso senti dire, ‘se non stai pagando, il prodotto sei tu.’ Ma i tuoi dati sono un asset per qualsiasi azienda, sia che tu stia pagando per un prodotto oppure no*,” precisa Koivunen. “*I dati permettono alle aziende tecnologiche di vendere miliardi in pubblicità e prodotti, alimentando quello che viene considerato come il più grande business nella storia del denaro*.”

L’azienda cita un’indagine che ha condotto, dalla quale emerge che il 54% degli utenti Internet sopra i 25 anni teme che qualcuno violi i propri account social media. Bene, ma non benissimo.

La logica dell’operazione, spiegano dalle parti di F-Secure, è quella di fare in modo che aumenti la consapevolezza riguardo l’importanza di proteggere in maniera adeguata gli account di questi servizi.

“*Sebbene gli utenti forniscano volontariamente queste informazioni, dovrebbero comprendere quali sono le implicazioni sulla privacy e la sicurezza che si generano col creare account che posseggono più dettagli sulla nostra identità di quanti potremmo condividere con la nostra famiglia*,”conclude Koivunen. “*Tutte queste informazioni potrebbero finire nelle mani di un hacker con una violazione o una compromissione di un account*.”

Condividi l’articolo

Protezione dei minori? Sì, ma tutelando la privacy

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/07/19/quali-dati-abbiamo-diffuso-in-rete-ecco-come-scoprirlo/

Protezione dei minori? Sì, ma tutelando la privacy

Lug 18, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia 0

La nuova edizione dell'antivirus Bitdefender introduce nuove funzionalità di parental control. Nel mirino il fenomeno del cyber-bullismo.

Il concetto di sicurezza informatica si sta allargando progressivamente: dal semplice rilevamento (ed eliminazione) dei malware, si è progressivamente passati a strumenti di protezione che comprendono aspetti molto differenti della dimensione digitale della nostra vita.

La conferma arriva da **Bitdefender**, che oggi ha lanciato sul mercato le nuove versioni dei suoi software di sicurezza per il 2020. Tra le novità, una funzione di parental control "evoluta" e tanta attenzione per la privacy.

A partire, per esempio, da **una funzione dedicata al blocco del tracciamento della navigazione tramite browser**, che molti utenti cominciano a sentire come una priorità per tutelare la loro privacy.

La vera novità riguarda però l'introduzione di un nuovo sistema di parental control che, oltre a funzioni "standard"

come la limitazione dei tempi di navigazione e il blocco di applicazioni e contenuti inappropriati, introduce funzioni avanzate come gli strumenti per bloccare contatti “indesiderati” e nuovi mezzi di contrasto del cyber-bullismo.

Ma di cosa si tratta in pratica? **Parental Control Premium** introduce una serie di sistemi di controllo basati sull’Intelligenza Artificiale (AI) che consentono di rilevare richieste o scambi di foto inappropriate, inviti ad appuntamenti da parte di sconosciuti e divulgazione di informazioni personali come l’indirizzo di casa o i dati della carta di credito.

Il fiore all’occhiello del nuovo strumento è però il sistema di **contrasto al cyber-bullismo**. Il software analizza infatti le comunicazioni (le nuove funzionalità sono disponibili per il momento solo per gli utenti di lingua inglese) per individuare messaggi o indizi di vario genere che possono corrispondere a dinamiche legate al cyber-bullismo.

Anche in questo ambito, però, gli sviluppatori di Bitdefender si sono preoccupati di tutelare la privacy, anche nei confronti dei genitori. Il controllo delle immagini (che

individua nudità ma anche documenti o carte di credito) per esempio, viene eseguito in locale senza coinvolgere i server della società di sicurezza.

Anche i messaggi (**Facebook, Whatsapp e Instagram**), che vengono dati in pasto a un algoritmo dedicato che non opera per parole chiave ma analizza il contesto per capire cosa stia succedendo, **vengono cancellati immediatamente dopo l'analisi in modo che non si aprano spazi che possano ledere la riservatezza della sfera privata**.

L'attenzione per la privacy, però, è anche (e soprattutto) confermata nelle procedure previste in caso di pericolo. Nell'eventualità in cui vengano rilevati indizi che possono far pensare a una vessazione da parte di cyber-culli, i genitori ricevono una segnalazione che **non comprende i messaggi scambiati**.

Questo per evitare che il sistema di parental control si trasformi in una sorta di "grande fratello" che il minore vivrebbe come uno strumento di controllo invasivo.

La procedura, messa a punto con la collaborazione di psicologi e professionisti del settore pedagogico, prevede anche la visualizzazione di suggerimenti su come affrontare il tema con il bambino.

Insomma: la nuova interpretazione del parental control abbandona la logica del semplice "controllo" per approdare a una concezione in cui l'uso dell'intelligenza artificiale consente di segnalare potenziali pericoli mantenendo quegli "spazi privati" che anche un bambino o un ragazzo ha diritto di avere.

Condividi l'articolo

Quali dati abbiamo diffuso in Rete? Ecco come scoprirlo Bug

nei NAS Iomega. Milioni di file esposti su Internet

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/18/protezione-dei-minori-si-ma-tutelando-la-privacy/

More on DataSpii: How extensions hide their data grabs—and how they’re discovered

Enlarge / You can trust us!
Irakli Kalandarishvili / EyeEm / Getty

reader comments

9 with 9 posters participating

Share this story

In our 5,000 word piece on “DataSpii,” we explained how researcher Sam Jadali spent tens of thousands of dollars investigating the murky Internet ecosystem of browser extensions that collect and share your Web history. Those

histories could end up at sites like Nacho Analytics, where they can reveal personal or corporate data.

Here, we want to offer more detail for the technically curious reader on exactly how these browser extensions work—and how they were discovered.

Obscurity

Discovering which browser extensions were responsible for siphoning up this data was a months-long task. Why was it so difficult? In part because the browser extensions appeared to obscure exactly what they were doing. Both Hover Zoom and SpeakIt!, for instance, waited more than three weeks after installation on Jadali's computers to begin collection. Then, once collection started, it was carried out by code that was separate from the extensions themselves.

One example: immediately after an installation on February 5, 2019, both extensions contacted developer-designated servers and reported their installation time, installation version, current version, and unique extension ID. On February 15, the extensions received an automatic update, but they still didn't collect any browsing history. Then, on March 1, both extensions received a second automatic update.

Almost immediately, the extensions again contacted developer-controlled servers and reported the unique ID of the extension, installation time, and current version. About one second later, the extensions received a 156KB payload, with 150KB of this being stored not in the extension folder, but in the Chrome browser system profile (in Jadali's case, the file was located at C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\File System\002\p\00\00000000).

The Hover Zoom extension can be seen downloading the 156KB payload in request 2103 of the following packet capture:

Enlarge / Hover Zoom’s response to GET request #2103. The contents of this response were saved in C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\File System\002\p\00\00000000.
Sam Jadali
This payload contained a minified JavaScript file that was responsible for collecting a user’s browsing data and sending it to a developer-controlled server. The contents of the file are shown in the figure below:

Enlarge / Contents of the JavaScript file 00000000 that’s downloaded by Hover Zoom.
Sam Jadali

The JavaScript file downloaded by the SpeakIt! Extension looked substantially the same; it also mentions the same cr-b.hvrzm.com host name found in the Hover Zoom file. These JavaScript files, because they’re stored in the Chrome profile and don’t update the actual extension that downloaded them, make it substantially harder for investigators—both inside and outside of Google—to detect the data collection.

“If people examine the extension itself, they’re not going to see that data collection instruction set,” Jadali told Ars. “It’s in an entirely different place.”

“We repeated this experiment six times, under numerous scenarios,” Jadali wrote in a detailed report. “Each time we

obtained the same result. In the past, similar [delaying] tactics have been used to avoid data collection” by other browser extensions.

Other tactics

The eight extensions that Jadali identified concealed their collection in other ways. All used base64 encoding and data compression that obfuscated the data being uploaded. The image immediately below shows what data uploaded by Hover Zoom looked like to the naked eye; the second image below shows its contents after being decoded.

Sam Jadali

Enlarge / The same collected data after it is uncompressed and decoded.
Sam Jadali
These screenshots also show Hover Zoom collecting hyperlinks and image locations of visited pages, even when these are

inside a private network. SpeakIt! performed almost identical data collection. As noted in the main article, the collection of hyperlinks and resources is serious because it can give outsiders a birds-eye view of an organization's private network. Jadali's research shows this data was being sent to pnldsk.adclarity.com. Adclarity.com is the homepage for AdClarity, maker of a marketing intelligence tool for people in the online advertising industry, which told Ars that it had purchased the data for a trial project but has already stopped using it. There is no evidence of Nacho Analytics publishing or even accessing any of the hyperlink data.

Jadali also observed both Hover Zoom and SpeakIt! sending other browsing data to p.ymnx.co. It remains unclear what this subdomain is or what happened to the data it received.

The data collection was also hard to detect because it continually morphed over the seven months that Jadali tracked it. Some of the extensions, for instance, regularly tweaked the encoding and compression used before uploading user data.

The data collection was hard to track for other reasons. Four of the extensions uploaded visited URLs and page titles in batches ranging from 10 to 50, and the batch size changed regularly over the seven-month span of Jadali's research. What's more, websites for three of the extensions used a robots.txt file to prevent search engines from indexing their terms of service and privacy policies.

Watching the watchers

Jadali used browsers with all of the suspect extensions installed to visit a total of more than two-dozen unique URLs on a domain that he hosted. For tracking purposes, the unique URLs he visited contained long strings that specified the time of the visit and the operating system, browser, and extension being used. One such URL was this:
[REDACTED-

DOMAIN]/samtesting.html?&os=mac&brow=crmium&v=74.0.3684.0&ext=SZ&date=mar112019&time=149pmpst&socsec=123004567&customerssn=123004567&lastname=doe&first=john&last=doe&password=mypass&p=anotherpass&apikey=XYZ
Except for the visit by his lab browser using one of the extensions, Jadali was careful to keep the two dozen unique URLs private. Within about an hour of each visit, however, Nacho Analytics published each link. Because Jadali controlled the domain that was hosting each of the URLs, he was able to track any follow-on visits the links received. Within three hours of being published on Nacho Analytics, a third-party IP address also visited each one of the URLs.

Jadali's logs show the above link receiving the following Web request:
184.72.115.35 - - [12/Mar/2019:01:03:45 +0000] "GET /samtesting.html?&os=mac&brow=crmium&v=74.0.3684.0&ext=SZ&date=mar112019&time=149pmpst&socsec=123004567&customerssn=123004567&lastname=doe&first=john&last=doe&password=mypass&p=anotherpass&apikey=XYZ HTTP/1.1" 200 198 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/600.1.25 (KHTML, like Gecko) Version/8.0 Safari/600.1.25"

Who was behind this further collection? Jadali said that one of the five following IP addresses visited each of his test URLs:

- 54.209.60.63
- 54.175.74.27
- 54.86.66.252
- 52.71.155.178
- 184.72.115.35

Not only did the IP addresses visit the URLs for Jadali's domain, in many cases they also actively downloaded an SQL database hosted by the pages. The download happened on pages hosting databases with sizes of 1.6KB, 9KB, 425KB, and 4.2MB. An 8.4MB database, however, wasn't downloaded, leading Jadali

to speculate that it passed an unknown size threshold designated by the person or script controlling the page visits.

Jadali used both forward and reverse DNS records to trace all five of the IP addresses to kontera.com. The URL http://kontera.com/ redirects browsers to the website of Amobee. A division of Singaporean telecommunications company Singtel, Amobee is an advertising company that bought analytics company Kontera in 2014 for a reported $150 million.

Amobee representatives didn’t respond to messages asking how they obtained the links Jadali observed the Kontera IP addresses visiting or what the company did with the downloaded SQL files.

Jadali said that if these IP addresses visited obscure URLs he had created only a few hours earlier, it’s a reasonable bet they visited many, many others.

“It’s possible they could be analyzing those pages for advertising or marketing purposes,” he told Ars. “Perhaps they use the page content data to deliver advertisements related to the content. However, as DataSpii shows, how do we really know what companies do with our data?”

https://arstechnica.com/?p=1533185

My browser, the spy: How extensions slurped up

browsing histories from 4M users

Aurich Lawson / Getty

reader comments

32 with 29 posters participating

Share this story

When we use browsers to make medical appointments, share tax returns with accountants, or access corporate intranets, we usually trust that the pages we access will remain private. DataSpii, a newly documented privacy issue in which millions of people's browsing histories have been collected and exposed, shows just how much about us is revealed when that assumption is turned on its head.

DataSpii begins with browser extensions—available mostly for Chrome but in more limited cases for Firefox as well—that, by Google's account, had as many as 4.1 million users. These extensions collected the URLs, webpage titles, and in some cases the embedded hyperlinks of every page that the browser user visited. Most of these collected Web histories were then published by a fee-based service called Nacho Analytics, which markets itself as "God mode for the Internet" and uses the tag line "See Anyone's Analytics Account."

Web histories may not sound especially sensitive, but a subset of the published links led to pages that are not protected by passwords—but only by a hard-to-guess sequence of characters (called tokens) included in the URL. Thus, the published links could allow viewers to access the content at these pages.

(Security practitioners have long discouraged the publishing of sensitive information on pages that aren't password protected, but the practice remains widespread.)

According to the researcher who discovered and extensively documented the problem, this non-stop flow of sensitive data over the past seven months has resulted in the publication of links to:

- Home and business surveillance videos hosted on Nest and other security services
- Tax returns, billing invoices, business documents, and presentation slides posted to, or hosted on, Microsoft OneDrive, Intuit.com, and other online services
- Vehicle identification numbers of recently bought automobiles, along with the names and addresses of the buyers
- Patient names, the doctors they visited, and other details listed by DrChrono, a patient care cloud platform that contracts with medical services
- Travel itineraries hosted on Priceline, Booking.com, and airline websites
- Facebook Messenger attachments and Facebook photos, even when the photos were set to be private.

In other cases, the published URLs wouldn't open a page unless the person following them supplied an account password or had access to the private network that hosted the content. But *even in these cases*, the combination of the full URL and the corresponding page name sometimes divulged sensitive internal information. DataSpii is known to have affected 50 companies, but that number was limited only by the time and money required to find more. Examples include:

- URLs referencing teslamotors.com subdomains that aren't reachable by the outside Internet. When combined with corresponding page titles, these URLs showed employees troubleshooting a "pump motorstall fault," a "Raven

front Drivetrain vibration," and other problems. Sometimes, the URLs or page titles included vehicle identification numbers of specific cars that were experiencing issues—or they discussed Tesla products or features that had not yet been made public. (See image below)
- Internal URLs for pharmaceutical companies Amgen, Merck, Pfizer, and Roche; health providers AthenaHealth and Epic Systems; and security companies FireEye, Symantec, Palo Alto Networks, and Trend Micro. Like the internal URLs for Tesla, these links routinely revealed internal development or product details. A page title captured from an Apple subdomain read: "Issue where [REDACTED] and [REDACTED] field are getting updated in response of story and collection update APIs by [REDACTED]"
- URLs for JIRA, a project management service provided by Atlassian, that showed Blue Origin, Jeff Bezos' aerospace manufacturer and sub-orbital spaceflight services company, discussing a competitor and the failure of speed sensors, calibration equipment, and manifolds. Other JIRA customers exposed included security company FireEye, BuzzFeed, NBCdigital, AlienVault, CardinalHealth, TMobile, Reddit, and UnderArmour.

Clearly, this is not good. But how did it happen?

- DataSpii revealing Raven in late March, about a week before it became widely known as a Tesla code name.
- The history of Tesla pages being opened.
- Trend Micro project management issues from a non-public domain.
- Symantec was exposed by DataSpii as well.
- Project management issues from a non-public FireEye domain.
- Browsing data published for Blue Origin showing project management items and non-public subdomains.

- Atlassian domains.
- One of thousands of mailers showing the names and addresses of car buyers, along with how many more payments they had left and the identification numbers of their vehicles.
- Travel itineraries containing passengers’ full names and email addresses are a common DataSpii occurrence.

The data spy

The term DataSpii was coined by Sam Jadali, the researcher who discovered—or more accurately *re*-discovered—the browser extension privacy issue. Jadali intended for the DataSpii name to capture the unseen collection of both internal corporate data and personally identifiable information (PII). (Ars has more technical details about DataSpii here.)

As the founder of Internet hosting service Host Duplex, Jadali first looked into Nacho Analytics late last year after it published a series of links that listed one of his client domains. Jadali said he was concerned because those URLs led to private forum conversations—and only the senders and recipients of the links would have known of the URLs or would have the credentials needed to access the discussion. So how had they ended up on Nacho Analytics?

Enlarge / An ad for Nacho Analytics.

Jadali suspected that the links were collected by one or more extensions installed on the browsers of people viewing the specialized URLs. He forensically tested more than 200 different extensions, including one called “Hover Zoom”—and found several that uploaded a user’s browsing behavior to developer-designated servers. But none of the extensions sent the specific links that would later be published by Nacho Analytics.

Enlarge / Sam Jadali

Donald Carlton

Still curious how Nacho Analytics was obtaining these URLs from his client’s domain, Jadali tracked down three people who had initial access to the published links. He correlated time

stamps posted by Nacho Analytics with the time stamps in his own server logs, which were monitoring the client's domain. That's when Jadali got the first indication he was on to something; two of his three users told him they had viewed the leaked forum pages with a browser that used Hover Zoom.

Web searches such as this one have reported the extension's earlier history of data collection. Suspicious that Hover Zoom might be doing the same thing again, Jadali set out to more rigorously test the extension.

He set up a fresh installation of Windows and Chrome, then used the Burp Suite security tool and the FoxyProxy Chrome extension to observe how Hover Zoom behaved. This time, though, he found no initial sign of data collection, so he remained patient. Then, he said, after more than three weeks of lying dormant, the extension uploaded its first batch of visited URLs. Within a couple of hours, he said, the visited links, which referenced domains controlled by Jadali, were published on Nacho Analytics. Soon after, each URL was visited by a third party that often went on to download the page contents.

Jadali eventually tested browser extensions for Firefox and also set up test machines running both macOS and the Ubuntu operating system. In the end, he said, the extensions that he found to have collected browsing histories that later appeared on Nacho Analytics include:

- Fairshare Unlock, a Chrome extension for accessing premium content for free. (A Firefox version of the extension, available here, collects the same browsing data.)
- SpeakIt!, a text-to-speech extension for Chrome.
- Hover Zoom, a Chrome extension for enlarging images.
- PanelMeasurement, a Chrome extension for finding market research surveys
- Super Zoom, another image extension for both Chrome and

Firefox. Google and Mozilla removed Super Zoom from their add-ons stores in February or March, after Jadali reported its data collection behavior. Even after that removal, the extension continued to collect browsing behavior on the researcher's lab computer weeks later.

- SaveFrom.net Helper a Firefox extension that promises to make Internet downloading easier. Jadali observed the data collection only in an extension version downloaded from the developer. He did not observe the behavior in the version that was previously available from Mozilla's add-ons store.
- Branded Surveys, which offers chances to receive cash and other prizes in return for completing online surveys.
- Panel Community Surveys, another app that offers rewards for answering online surveys.

While Jadali can't be certain *how* Nacho Analytics obtained URLs for pages that can only be accessed by people authorized by companies like Apple, Tesla, Blue Origin, or Symantec, the most likely explanation is that one or more of them had a browser with an affected extension. Jadali has confirmed with four affected companies that employees did, in fact, have one or more of the extensions installed. Palo Alto Networks also confirmed to Ars that browsers inside its network used an affected extension. All five companies have since removed the extensions. Google, citing violations to its terms of service, has also removed the six extensions it hosted in its Chrome Web Store.

Ars contacted a small sample of affected companies, including Apple, Symantec, FireEye, Palo Alto Networks, Trend Micro, Tesla, and Blue Origin. Symantec, Trend Micro, and Palo Alto Networks were the only ones who provided a comment.

Symantec's statement read: "We want to thank the researcher for alerting us to this issue and sharing his findings. We have taken immediate steps to remediate this issue." Trend

Micro officials said: “Trend Micro appreciates being made aware of this and has remedied the issue.” A Palo Alto Networks representative wrote: “On the day we were notified of the issue, Palo Alto Networks deleted the browser extensions and blocked the outbound traffic associated with the add-on extensions to prevent any further potential impact.”

Investigating DataSpii over the past six months has eclipsed Jadali’s full-time job and much of his personal life.

Jadali said the new vocation has so far cost him nearly $30,000 in personal expenses, since the research is not tied to his responsibilities at Host Duplex. Jadali estimates that about 60% of the cost has been in fees from Nacho Analytics. The rest has been for travel and for various consultants.

“It became my number one priority,” he said. “Almost as if it was out of my control.”

Reading the fine print

Principals with both Nacho Analytics and the browser extensions say that any data collection is strictly “opt in.” They also insist that links are anonymized and scrubbed of sensitive data before being published. Ars, however, saw numerous cases where names, locations, and other sensitive data appeared directly in URLs, in page titles, or by clicking on the links.

The privacy policies for the browser extensions do give fair warning that some sort of data collection will occur. The Fairshare Unlock policy, for example, says that the extension “collects your digital behavior data and shares it with 3rd parties to enable better survey targeting and other market research activities.” (This and other policies mentioned in this article were recently taken down.)

The collected information expressly includes “URLs visited,

data from URLs loaded and pages viewed, search queries entered, social connections, profile properties, contact details, usage data, and other behavioral, software, and hardware information." At the same time, the policy promises that Fairshare will take steps to anonymize the data.

"For our primary use-case of research, PII scrubbers attempt to remove all personally identifiable information before analysis and archiving," the Fairshare Unlock policy states. "Individual users are regularly re-assigned randomly generated identifiers which, when combined with PII scrubbing, provides anonymity."

Privacy policies for SpeakIt!, PanelMeasurement, Hover Zoom, Panel Community Surveys, and Branded Surveys contain language that's largely identical to that cited above. Savefrom.net's policy also makes clear it will collect the "URL of the particular Web page you visited." (The policy for Super Zoom is no longer available.) Below are images that some of the extensions display when being installed:

- Fairshare Unlock permissions.
- Hover Zoom permissions.
- Speak It! permissions.
- PanelMeasurement permissions.
- The opt-in page for PanelMeasurement.

Nacho Analytics, for its part, has this to say in a YouTube promotion, which starts out asking "Is this legal?"

"We are gathering data from millions of opt-in users, individuals from around the world that agreed to share their browsing data anonymously. Nacho analytics scrubs this data so all personal information is deleted and so it's GDPR compliant." (This is a reference to the strict Government Data Protection Regulation that went into effect in the European Union 26 months ago.)

Jadali's research found that Fairshare Unlock, PanelMeasurement, SpeakIt!, Hover Zoom, Branded Surveys, and Panel Community Surveys did redact some information on end users' computers before sending it to the developer-designated servers. But he said that an examination of data packets sent to the servers and links published on Nacho Analytics makes it clear that not all types of sensitive information were removed. Redaction seemed to happen only when Web developers use certain query string parameters in their URLs.

Enlarge / When a URL designated a surname with the parameter "lastname," extensions replaced the name with asterisks. This redaction failed when URLs used less standard parameter names such as "passengerLastname."
Sam Jadali
As the image above shows, strings that used "lastname=x" seemed to successfully cause last names to be replaced with asterisks. Strings that used "passengerLastName=y," however, were not removed. None of Jadali's research shows that Super Zoom or SaveFrom.net Helper performed any redactions at all.

What's more, some links published by Nacho Analytics contain what appear to be the personal information of real people. Examples of such personal information included passenger names in links from airline Southwest.com, pick-up and drop-off locations of people using the Uber.com website (but not the phone app) to hail rides, and email addresses from Apple's password reset service. While Jadali redacted sensitive information from the following screenshots, none of it was removed from the links published by Nacho Analytics.

- Sam Jadali
- Sam Jadali
- Sam Jadali

What's more, even when the URLs published by Nacho Analytics removed names, social security numbers, or other sensitive

information, clicking on the links often led to pages that revealed the same redacted information.

Meet the DataSpii players

DDMR

Google's Chrome Web Store lists the developer of PanelMeasurement as DDMR.com with a mailing address in Walnut, California. The store doesn't identify the developer of Fairshare Unlock, Hover Zoom, SpeakIt!, or Super Zoom, but the privacy policy for Fairshare Unlock also lists DDMR.com and the same Walnut, California, mailing address in a Contact Us section. The policies for Hover Zoom, SpeakIt!, and Panel Community Surveys also contain language and organization almost identical to those for the PanelMeasurement and Fairshare Unlock extensions.

Another link to DDMR: domains that received browsing data from all eight of the extensions resolved to the same two IP addresses—54.160.162.145 and 52.54.192.223. This page from SSL Labs, a research project by security firm Qualys, shows that 54.160.162.145 is tied to a security certificate belonging to DDMR domain ddmr.com (viewers first must click the "click here to expand" for certificate #2).

This LinkedIn profile lists Christian Rodriguez as the founder and CEO of DDMR. A 2015 article—reporting an earlier round of data collection by Chrome extensions—identifies Rodriguez as working in business development for Fairshare Labs. Fairshare Labs' contact page lists the same Walnut, California, mailing list.

Rodriguez told me that Fairshare Labs is an abandoned project and that Fairshare Unlock is no longer actively developed (although he said it does continue to receive security and GDPR compliance updates). He pointed to the bottom of this

page, which he said provides “very clear, pre-installation disclosure to users.”

Rodriguez described DDMR as a “passive metering technology company” that provides market research companies with “passive metering browser extensions that they distribute to their research panelists.” He went on to write in an email:

> *Our customers are responsible for recruiting end-users into their panels and directing them to our landing pages.*
>
> *It is our responsibility to (1) ensure that we provide end-users with clear disclosure of what data is collected and how it is used, and (2) receive appropriate consent. Once consent is given, we collect the behavioral data, scrub it for sensitive information like phone numbers, social security numbers, credit card numbers, and email addresses, and then make it available to market researchers to use in their research.*
>
> *If it is brought to our attention that sensitive information is leaking, we immediately take action to improve our filters and eliminate that data from our dataset.*
>
> *Responsible use of behavioral data allows market researchers and the companies they serve to build better products and experiences for consumers, but it is necessary to recognize the value of this data in the context of its potentially sensitive nature.*

He declined to say if Nacho Analytics was a customer, business partner, or had any other relationship with DDMR.

Nacho Analytics

Nacho Analytics, meanwhile, promises to let people “see anyone’s analytics account” and to provide “Real-Time Web Analytics For Any Website.” The company charges $49 per month,

per domain, to monitor any of the top 5,000 most widely trafficked websites, although certain domains—including those for Google, YouTube, Facebook, and others—aren't available for monitoring. For sites below this premium threshold, it costs $49 per month to monitor one domain, $99 per month for up to five domains, and $149 per month for up to 10 domains.

Once someone signs up, Nacho Analytics uses a Google-provided programming interface to deliver data to a Google Analytics account designated by the user. Ars installed several extensions identified by Jadali, visited sites with long-pseudorandom strings in them, and then observed Nacho Analytics populating those unique URLs into the designated Google Analytics page.

- One booking.com page with a specific string in the URL
- A second one. Both are viewed using a browser that has four DataSpii extensions installed.
- Both pages are soon published.

The previously mentioned video promoting Nacho Analytics on YouTube says that the service is "100-percent legal and completely complies with Google's terms of service." The video also asserts that the Nacho Analytics service is "GDPR compliant."

In an interview, Nacho Analytics founder and CEO Mike Roberts reiterated that the service is fully GDPR compliant and that the millions of people whose data is collected have expressly agreed to this arrangement.

"You absolutely do" click an agree button, Roberts said of all users whose data is published. What's more, he said, "we spend quite a bit of time processing every URL that we see to remove all the personally identifiable information." Ars has confirmed that in many cases, the URLs published by Nacho Analytics have had names, Social Security numbers, and other personal information removed. However, Ars was also able to

find numerous instances of names and other personal information remaining in published URLs.

[embedded content]
A Nacho Analytics video called “FAQ: Is This Legal?”
Roberts said that he was unaware Nacho Analytics published links to webpages hosting tax returns, Nest Videos, car buyer information, and an extensive amount of other personally identifiable information. Nacho Analytics already excludes domains for Google, Facebook, YouTube, and many other services out of privacy concerns, he said, and may exclude others.

“Your report is personally disturbing to me—and [publishing sensitive data] is definitely not the purpose of Nacho Analytics,” he said. “We work hard to remove personally identifiable information from URLs and page titles, and exclude sites with serious security issues. When we learn of a new issue, we have a system to remove it immediately. We’ve stopped all new sign-ups for Nacho until we can get more information on this issue. If you give me a list of the sites that have these issues, we’ll immediately disable those sites and work on a permanent solution.”

He also pushed back on the idea that Nacho Analytics had ever been used by customers to harvest sensitive information. Jadali, he claimed, was the only one who had done so. (He also claimed that Jadali had violated Nacho Analytics’ terms of service in doing the research.)

“Jadali looked at hundreds of websites, only a tiny fraction of which any legitimate Nacho Analytics customer ever viewed,” he said. “In fact, none of the sites with the issues you’ve made me aware of have been viewed by any legitimate Nacho Analytics customer.”

But Roberts defended the basic practice of publishing links that, when clicked, lead to private data—so long as that data isn’t viewable in the URL itself as published by Nacho

Analytics.

He put it this way:

> *Those pages are available. It's just that you didn't know how to discover them. This is just something that you're now able to see that you weren't able to see before. But we're not creating a loophole. There's no backdoor or anything. We're just showing links that you didn't know about before and maybe weren't indexed, but they do exist…*
>
> *That link by obfuscation thing, I don't like it. I wish it didn't exist because I definitely don't want to be enabling anybody to do anything bad, only good. I'm trying to create good things in the world. And there's the opportunity there for some people to do some damage.*

Roberts said he was also unaware that Nacho Analytics was publishing links and page titles from the non-public, internal networks of companies. But, while he questioned the analytics value of this data, he didn't necessarily think publishing it was a bad thing.

"I don't think I personally see much value in it," he said. "But just because a company may want to keep it private, I'm not sure that's where the best value is."

He said he had never heard of any of the extensions that Jadali had identified as collecting data that later ended up on Nacho Analytics, but he declined to identify any software that collects end-user browsing data, nor would he name any companies that Nacho Analytics works with to obtain this data. (In a later email, he clarified that the data "comes from third-party data brokers. We certainly didn't invent the method of data collection.")

"Using Nacho to look at private information or to try to hack into websites is an explicit violation of our terms of use,"

Roberts added. “[Nacho is] a marketing product that puts small businesses and entrepreneurs on a level playing field with large corporations that have and will continue to have access to this type of data.”

“Honestly, I think you have the wrong villain here.”

On July 8, five days after Google remotely disabled the extensions Jadali had reported, Roberts said on Twitter that Nacho Analytics “had an upstream data outage.” A day later, Roberts said Nacho Analytics’ “data partner has ended operations.” Shortly after that, the Nacho Analytics front page said the service was “halting all access to any potentially sensitive data.”

Enlarge / One of many Nest.com URLs leaked by DataSpii. Ars has redacted faces, computer and video screens, and posters.
https://arstechnica.com/?p=1531629

FaceApp, i like preferiti alla privacy ceduta per sempre alla società russa (Che usa i volti come cavie per l'IA)

Un nuovo "gioco" sta contagiando oltre 80 milioni di utenti nel mondo e sta invadendo le bacheche dei social: invecchiare il proprio volto con **FaceApp**, un'applicazione disponibile su App Store e Google Play Store che grazie ad un'aggiornamento con le tecnologie di Intelligenza Artificiale offre una trasformazione digitale abbastanza realistica. Dopo aver scaricato l'app basta scattarsi una foto o prenderla dalla propria galleria di immagini e in pochi click è possibile modificare il volto, modificando l'acconciatura, invecchiando o ringiovanendo i tratti somatici, ma anche riuscendo a trasformarci in uomini o donne. Anche le celebrities sono state contagiate dal gioco, tanto che è diventato virale l'hashtag #FaceAppChallenge.

"Abbiamo sviluppato una nuova tecnologia che sfrutta le reti neurali per modificare in maniera realistica il volto nelle foto", ha spiegato al sito *TechCrunch* il fondatore e Ceo dell'app russa, **Yaroslav Goncharov.**

I rischi

All'aspetto ludico si uniscono però i tanti rischi sulla privacy. Alla perplessità di far circolare troppe immagini personali sulle piattaforme social, nella pagina dell'app dedicata all'uso delle informazioni si legge che *"potrebbe condividere i contenuti e le informazioni degli utenti con le aziende che fanno parte del gruppo di società di FaceApp".*

E questo è il primo allarme sulla protezione dei dati degli utenti, privacy che si cede totalmente e per sempre all'app russa. Infatti, fa notare **Guido Scorza**, uno dei candidati ad essere eletto dal Parlamento Garante per la protezione dei dati personali: "*La foto del nostro volto diventa, nella sostanza, di FaceApp che può farne quello che vuole perché la licenza – salvo non volersi avventurare in interminabili battaglie giudiziarie sulla validità delle relative clausole – è perpetua, irrevocabile, mondiale, cedibile e, naturalmente gratuita*".

I volti come cavie per l'IA

Si regala, dunque, per sempre il proprio volto alla società russa, che lo utilizzerà come cavia per addestrare le reti neurali e i sistemi di intelligenza artificiale su cui sta lavorando. Il tutto per avere solo un pugno di like sui social.

https://www.key4biz.it/faceapp-i-like-preferiti-alla-privacy-ceduta-per-sempre-alla-societa-russa-che-usa-i-volti-come-cavie-per-lia/265725/

GDPR e videosorveglianza, pubblicate le linee guida

EDPB. L’analisi punto per punto

Sono state rese note dall’*European Data Protection Board* (**EDPB**) le linee guida 3/2019 del 12 luglio 2019 sul trattamento dei dati personali in merito ai servizi di videosorveglianza.

Le linee guida in commento sono interessanti perché l’utilizzo intensivo dei sistemi di video sorveglianza ha modificato il comportamento dei cittadini che, sentendosi osservati, modificano il loro atteggiamento, diverso da quello che avrebbero avuto nel caso fossero rimasti anonimi.

Le linee guida si prefiggono lo scopo di fornire gli strumenti utili per evitare che la legittima acquisizione di video registrazioni scivoli poi in un trattamento illecito o non conforme al GDPR.

Di seguito una rielaborazione di quanto descritto nelle linee guida 3/2019.

1. **L’analisi del trattamento dati nei casi di Videosorveglianza a mente dell’Articolo 5 GDPR.**

Per identificare le finalità del trattamento si deve verificare quanto prescritto dall’Articolo 5 del GDPR.

Invero, le finalità possono cambiare a seconda che il **titolare** sia **pubblico** o **privato**, che la video sorveglianza abbia la finalità di migliorare la sicurezza, per fornire strumenti di pubblicità mirata.

A volte poi le tecniche di video sorveglianza hanno carattere

altamente intrusivo (es. tecnologie biometriche complesse) o meno intrusive (ad esempio semplici algoritmi di conteggio delle persone in un locale).

Sul punto l'EDPB fa notare come gli algoritmi spesso non siano totalmente affidabili e che i titolari e responsabili della videosorveglianza devono mantenere un grado minimo di affidabilità dei sistemi di video sorveglianza per evitare scelte giuridiche affidate a tali sistemi (come l'identificazione facciale o il riconoscimento) abbia risultati errati e quindi deleteri.

Inoltre l'EDPB afferma che la videosorveglianza non è l'unico strumento da adottare per alcune finalità perseguite dal titolare del trattamento.

2. L'area di applicazione del GDPR nel trattamento dei dati nella video sorveglianza.

2.1 I Dati personali raccolti

È di tutta evidenza che una volta entrato in un locale videosorvegliato, si raccolgono così tante immagini e video correlate ad un interessato.

La raccolta di tutte le informazioni relative alle persone monitorate consente l'elaborazione di dati personali riferibili alla presenza della persona in un determinato luogo e permette di valutarne il comportamento o estrapolarne dettagli che a prima vista non sarebbero percepibili ad occhio nudo.

L'abuso che potrebbe derivarne da tali informazioni è evidente.

Più è ampia la sorveglianza più è alto il rischio.

Sul punto basti evidenziare che l'articolo 35, paragrafo 3, lettera c) del GDPR prescrive la DPIA in caso di monitoraggio sistematico su larga scala di un'area accessibile al pubblico

(si veda il paragrafo 10 in calce).

Inoltre è degno di nota quanto prescritto all'articolo 37, paragrafo 1, lettera b) GDPR che in questi casi impone la nomina di un **DPO**.

Tuttavia, il GDPR non si applica quando la persona non è in alcun modo identificabile, direttamente o indirettamente.

Qui di seguito gli esempi forniti dall'EDPB in cui non si applica il GDPR:

1. **telecamere false** (cioè quelle che non registrano video o immagini) poiché non vengono elaborati dati personali;
2. **video registrazioni ad alta** quota (perché le immagini non possono essere agganciate ad un soggetto preciso);
3. **videocamera a bassa risoluzione**, non in grado di raccogliere alcuna informazione relativa ad una specifica persona fisica (come targhe o informazioni che potrebbero identificare i passanti).

2.2 Direttiva EU2 016/680

Ogni trattamento dei dati personali (anche da video registrazione) da parte delle autorità competenti ai fini della prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, non è disciplinato dal GDPR ma dalla Direttiva EU 2016/680

2.3 Eccezioni per fini domestici

Ai sensi dell'articolo 2, paragrafo 2, lettera c), il trattamento di dati personali da parte di una persona fisica nel corso di attività puramente personali o domestiche, che possono includere anche attività *online*, è da considerarsi fuori dal campo di applicazione del GDPR (si veda anche il considerando n.18).

Questa eccezione – specie nel contesto della videosorveglianza – deve essere interpretato restrittivamente.

Sul punto, la Corte di Giustizia (sentenza nella causa C-101/01, *caso Bodil Lindqvist* , 6 novembre 2003, paragrafo 47) afferma che tale eccezione si riferisce solo alle attività svolte nel corso della vita privata o familiare, e tale non può essere la condivisione su Internet di tali dati, che di conseguenza sono resi accessibili a un numero indefinito di persone.

Inoltre, se un sistema di videosorveglianza registra ed archivia immagini, anche parzialmente, di uno spazio pubblico, non può più essere considerata tale attività come privata o familiare (Corte di giustizia europea, sentenza nella causa C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů* , 11 dicembre 2014, par. 33.)

Esempio: un turista sta registrando un video sia attraverso il suo telefono cellulare che attraverso una videocamera per documentare le sue vacanze.

Mostra il filmato ad amici e parenti ma non lo rende accessibile ad un numero indefinito di persone. Questo ricadrebbe nell'eccezione richiamata.

Esempio: un *mountainbiker* vuole registrare la sua discesa con una *actioncam*. Le registrazioni verranno visionate per il suo intrattenimento. Anche questa circostanza ricade nell'eccezione.

Esempio: qualcuno ha installato un sistema di video sorveglianza nel proprio giardino.

La proprietà è recintata e solo il titolare stesso e la sua famiglia hanno accesso regolarmente nel giardino. Questo rientrerebbe nell'eccezione a condizione che la videosorveglianza non monitori, anche parzialmente, uno spazio pubblico o una proprietà altrui.

3 LEGITTIMITÀ DEL TRATTAMENTO

Prima di ogni trattamento effettuato con dispositivi video devono essere specificate nel dettaglio le sue finalità (Articolo 5, paragrafo 1, lettera b), GDPR).

Le finalità della video sorveglianza possono essere diverse:

- la protezione della proprietà e di altri beni;
- la raccolta di prove per il diritto di difesa nei processi civili.

Per questa ragione, le finalità devono

- essere documentate per iscritto (articolo 5, paragrafo 2, GDPR);
- essere specifiche per ogni sistema di video sorveglianza in uso (cioè raggruppate per scopi comuni);
- devono fornire informazioni agli interessati in modo da far comprendere le finalità e gli scopi del trattamento conformemente all'articolo 13 del GDPR.

Secondo l'EDPB la semplice finalità per fini di "sicurezza" non è sufficientemente specificata poiché non si aggancia alle diverse base giuridiche di cui all'art. 6.

3.1 Le basi giuridiche

Ad esempio, si applica l'articolo 6, paragrafo 1, lettera c), GDPR quando è la stessa legge a prevedere l'obbligo di video sorveglianza.

Comunque le basi giuridiche più comuni sono quelle fondate:

· sull'Articolo 6, paragrafo 1, lettera f), GDPR (**legittimo interesse**).

· sull'Articolo 6, paragrafo 1, lettera e), GDPR (necessità di svolgere un compito svolto **nell'interesse pubblico** o **nell'esercizio di autorità ufficiale**)

· sull'Articolo 6, paragrafo 1, lettera a), GDPR (**consenso**).

3.1.1 Legittimo interesse

La videosorveglianza è lecita se è necessaria a soddisfare la finalità per legittimo interesse perseguito da un titolare del trattamento o da terzi, a meno che tali interessi non mettano a rischio i diritti e libertà fondamentali dell'interessato (articolo 6, paragrafo 1, lettera f), GDPR).

Per legittimo interesse si intende un interesse:

1. **legale**;
2. **economico**;
3. **immateriale**.

Tuttavia, l'interessato può opporsi (ai sensi dell'art. 21 GDPR) al trattamento dei dati (anche per i sistemi di videosorveglianza) e ciononostante il titolare può procedere con la videosorveglianza laddove il legittimo interesse prevalga sugli interessi, i diritti e le libertà dell'interessato o per esercitare il diritto di difesa.

Invero, in una situazione realmente pericolosa, la finalità di proteggere la proprietà ad es. da un furto può costituire un legittimo interesse per giustificare la videosorveglianza.

Il legittimo interesse deve essere pertanto:

- **reale** (cioè non deve essere immaginario o speculativo); e,
- **attuale** (cioè non potenziale ma concreto, ad esempio una situazione di pericolo imminente può costituire una base giuridica da legittimo interesse; ad esempio le gioiellerie o le stazioni di benzina).

Del pari il legittimo interesse non può essere desunto in *re ipsa* ma deve essere valutato caso per caso e bilanciato con i diritti dell'interessato.

3.1.2 Necessità del trattamento.

I dati personali devono essere **adeguati**, **pertinenti** e **limitati** in relazione alle finalità per i quali sono trattati ("**minimizzazione dei dati**"), a mente dell'Articolo 5, paragrafo 1, lettera c), GDPR.

Prima di installare un sistema di videosorveglianza il titolare dovrebbe verificare che tale misura è proporzionata alla finalità perseguita.

Invero la videosorveglianza dovrebbe essere adottata come *extrema ratio*.

Ad esempio, l'EDPB suggerisce che se la finalità è quella di prevenire i reati connessi alla proprietà, invece di installare un sistema di videosorveglianza, il titolare potrebbe anche adottare misure di sicurezza alternative come sistemi di sorveglianza quali assumere personale di sicurezza.

Esempio: il proprietario di un negozio desidera aprire un nuovo esercizio commerciale e desidera installare una sistema di videosorveglianza. A base del legittimo interesse, egli può riferirsi alle statistiche di atti di vandalismo in quel quartiere o riferirsi ad esperienze dei locali commerciali dei negozi vicini.

Tuttavia, non è sufficiente per giustificare un legittimo interesse basarsi su statistiche nazionali o generali senza analizzare l'area in questione o i pericoli specifici inerenti il negozio.

Inoltre, secondo l'EDPB, prima di installare un sistema di video sorveglianza il titolare è obbligato a valutare dove e quando le telecamere di sorveglianza sono strettamente necessarie (per esempio di notte e situate nel perimetro della proprietà).

Esempio: una libreria vuole proteggere i suoi locali contro atti di vandalismo.

In generale, le fotocamere dovrebbero solo filmare i locali interni perché non è necessario installare telecamere nei luoghi attigui o aree pubbliche nelle vicinanze.

Pertanto, per minimizzare i dati e per evitare una eccessiva raccolta, viene spesso utilizzato il *black box* in cui il filmato viene automaticamente eliminato dopo un certo periodo di archiviazione e accessibile solo in caso di incidente.

3.1.3 Bilanciamento degli interessi

Dando per assodato che la videosorveglianza sia necessaria per proteggere i legittimi interessi di un titolare, come detto è necessario sempre **bilanciare gli interessi** contrapposti dell'interessato.

In particolare, il titolare deve considerare:

1. in che misura il monitoraggio incide sugli interessi, diritti fondamentali e le libertà degli individui; e
2. se ciò provochi violazioni o conseguenze negative sui diritti dell'interessato.

Tale bilanciamento di interessi è obbligatorio:

da una parte, i diritti fondamentali e libertà dell'interessato; dall'altra, gli interessi legittimi del titolare.

Esempio: una società di parcheggi ha documentato il ripetersi di episodi di furto delle macchine parcheggiate. L'area di parcheggio è uno spazio aperto e può essere facilmente accessibile da chiunque, seppur debitamente segnalato con cartelli che circondano il perimetro.

Il legittimo interesse è prevenire i furti delle auto dei clienti.

Dall'altro gli interessati hanno diritto a non essere monitorati, nonostante che la videoregistrazione avvenga per

la prevenzione dei furti e sia effettuata anche a loro vantaggio. Quindi il monitoraggio è limitato solo alla sorveglianza delle auto ma non alla sorveglianza degli stessi clienti.

Esempio: un ristorante decide di installare delle videocamere nei servizi igienici per controllare la loro pulizia. In questo caso i diritti degli interessati hanno chiaramente la precedenza sul legittimo interesse del titolare, quindi le telecamere non possono essere installate nei servizi igienici.

3.1.3.1 Bilanciamento case-by-case

Seguendo l'impostazione data dall'Articolo 6, paragrafo 1, lettera f), GDPR, il bilanciamento degli interessi è obbligatorio e deve essere concreto ed attuale (quindi non formale).

Il titolare, ad esempio, deve valutare il peso (numero dei dati e delle persone o le dimensioni dell'area monitorata) ed i rischi dei diritti e delle libertà degli interessati coinvolti; nonché la possibilità di disporre di valide alternative alla videosorveglianza.

Esempio: se viene installata una *dash cam* (ad es. per raccogliere eventualmente prove nel caso di un incidente), è importante assicurarsi che anche questa telecamera non stia registrando costantemente le persone presenti sulla strada. Altrimenti la finalità andrebbe fuori dal perimetro del legittimo interesse alla video registrazione e cioè si trasformerebbe nella finalità di monitorare i dati di terzi in generale.

3.1.3.2 Ragionevoli aspettative degli interessati

Secondo il considerando 47 del GDPR, l'esistenza di un legittimo interesse richiede un'attenta valutazione anche delle aspettative degli interessati, per tale intendendosi l'aspettativa dell'interessato ad essere tutelato dal titolare

nella valutazione del caso concreto.

Ad esempio, un dipendente sul posto di lavoro nella maggior parte dei casi non si aspetta che sia monitorato dal suo datore di lavoro.

Allo stesso modo, non è ragionevole aspettarsi di essere monitorati in strutture sanitarie o altre aree che per definizione sono riconosciute come zone private.

Esempio: nei servizi igienici ci si aspetta di non essere monitorati.

Di contro, il cliente di una banca potrebbe aspettarsi che venga monitorato all'interno della stessa banca.

L'aspettativa di essere monitorati può esserci anche nei luoghi pubblici, dove il legittimo interesse è declinazione **dell'Articolo 6, paragrafo 1, lettera e), GDPR**, per svolgere quelle attività nell'interesse pubblico (come salute e sicurezza per la protezione di dipendenti e visitatori).

3.3 Base giuridica tramite consenso ai sensi dell'Articolo 6, paragrafo 1, lettera a), GDPR.

Come noto il consenso deve essere

1. **libero**;
2. **specifico**;
3. **informato**;
4. **attuale**;
5. **revocabile**.

Tali presupposti si applicano anche alla videosorveglianza, con la precisazione che il consenso può costituire valida base giuridica solo in casi eccezionali a mente dell'Articolo7 GDPR (cfr. considerando 43).

Infatti, per sua natura la videosorveglianza consente di monitorare contemporaneamente un numero sconosciuto di

persone.

Il titolare difficilmente sarà in grado di provare che l'interessato abbia dato il proprio consenso prima del trattamento dei propri dati personali (Articolo 7, paragrafo 1, GDPR).

Come del resto sarebbe difficile che in caso di revoca del consenso, il titolare sia in grado di non trattare più quei dati riferibili a quel singolo interessato (Articolo 7, paragrafo 3, GDPR).

Tuttavia, se il titolare intende giovarsi della base giuridica del consenso, è suo dovere assicurarsi che ogni persona interessata conferisca il suo esplicito consenso (per esempio quando si attraversa un'area particolare come un corridoio o un cancello specifico per entrare in un luogo monitorato).

Oppure, nel caso di videosorveglianza nei luoghi di lavoro, ove dato lo squilibrio di potere tra datore di lavoro e dipendenti, nella maggior parte dei casi i datori di lavoro dovrebbero non fare affidamento sul consenso, in quanto è improbabile che venga dato liberamente (sul punto si rimanda a quanto previsto dall'art. 4 dello Statuto dei lavoratori).

Esempio: gli atleti possono richiedere di essere monitorati durante le singole esercitazioni per analizzarne le proprie tecniche e prestazioni. Tuttavia, se un *club* sportivo prende l'iniziativa di monitorare un'intera squadra per la medesima finalità, il consenso spesso non è valido poiché il singolo atleta o gli atleti possono sentirsi costretti a dare il consenso per evitare che il loro rifiuto possa influire negativamente, anche sugli stessi compagni di squadra.

4 Divulgazione di filmati a terzi

In linea di principio, il GDPR disciplina i casi di divulgazione di registrazioni video a terzi.

4.1 Divulgazione di riprese video a terzi in generale

La divulgazione come "trattamento dati" è definita all'articolo 4, paragrafo 2, GDPR, come trasmissione (ad es. comunicazione individuale), diffusione (ad esempio, la pubblicazione online) o la messa a disposizione in altro modo.

I terzi sono definiti all'articolo 4, paragrafo 10, GDPR (inoltre, il WP Group 29 ha adottato delle specifiche linee guida al riguardo).

Ad ogni modo, qualsiasi divulgazione di filmati contenenti dati personali deve avere una specifica base giuridica (Articolo 6, paragrafo 4, GDPR).

Esempio: un titolare che desideri caricare una registrazione su Internet deve fare affidamento su una base giuridica per tale trattamento, ad esempio ottenendo il consenso dell'interessato secondo Articolo 6, paragrafo 1, lettera a), GDPR.

La stessa valutazione deve essere effettuata dal destinatario che, in particolare, dovrà identificare la sua base giuridica ai sensi dell'Articolo 6 (ad esempio la ricezione del materiale).

Esempio: il sistema di videosorveglianza posto su una barriera all'ingresso di un parcheggio è stata installata con lo scopo di risolvere eventuali richieste di risarcimento danni. Si verifica un danno e la registrazione viene trasferita ad un avvocato per seguirne il caso.

In questo caso la finalità della registrazione è il trasferimento del dato personale contenuto nella registrazione.

Laddove nella medesima situazione, però, la registrazione venisse pubblicata *online* per puro divertimento, in questo caso la finalità sarebbe diversa e non sarebbe compatibile con

la finalità iniziale. Inoltre sarebbe problematico identificare una base giuridica per tale trattamento (pubblicazione) e si potrebbe immaginare il consenso dell'interessato.

4.2 Divulgazione di filmati alle forze dell'ordine

Anche la divulgazione di registrazioni video verso le forze dell'ordine è un trattamento separato che richiede una base giuridica diversa ai sensi dell'Articolo 6, paragrafo 1, lettera c), GDPR, per esempio per cooperare durante le indagini.

Esempio: un proprietario del negozio registra filmati al suo ingresso. Registra una persona che ruba un portafoglio. La polizia chiede al titolare di consegnare il materiale per finalità di indagine ai sensi dell'Articolo 6, paragrafo 1, lettera c), GDPR.

Esempio: una telecamera è installata in un negozio per motivi di sicurezza. Il proprietario del negozio crede di aver registrato qualcosa di sospetto e decide di inviare il materiale alla polizia (senza alcuna indicazione di una qualsivoglia indagine in corso). In questo caso il proprietario del negozio deve valutare se le condizioni di cui all'Articolo 6, paragrafo 1, lettera f), GDPR sono soddisfatte.

Ricordiamo che il trattamento dei dati personali da parte delle forze dell'ordine è disciplinato dalla direttiva EU 2016/680.

Per scaricare le linee guida complete e tradotteclicca qui. (pdf)

https://www.key4biz.it/gdpr-e-videosorveglianza-pubblicate-le-linee-guida-edpb-lanalisi-punto-per-punto/265510/

La protezione dei dati personali in Italia

- Di Giusella Finocchiaro
- Zanichelli editore
- ISBN: 9788808820433
- Pagine: 1048
- Prezzo: € 189,00

L’opera nasce a seguito della recente entrata in vigore del Regolamento UE n. 679/2016 sulla protezione dei dati personali, nonché del d.lgs. 101/2018 che ha operato un coordinamento della normativa europea con quella italiana. Il volume costituisce un importante supporto per i giuristi e i professionisti che devono misurarsi con l’applicazione della nuova disciplina sulla privacy. Il nuovo Regolamento, infatti, muta la disciplina del trattamento dei dati personali e della privacy ed è direttamente applicabile in tutti i Paesi membri dell’Unione europea dal 25 maggio 2018. Il decreto ha rivisto il quadro normativo vigente, abrogando espressamente alcune disposizioni del d.lgs. 196/2003, c.d. Codice Privacy.

Il volume tratta tutti i temi del Regolamento, fornendo una lettura inedita delle novità introdotte dal legislatore europeo e da quello italiano. In particolare, e per citare soltanto le novità di maggior respiro, il nuovo principio di accountability e il mutato regime di responsabilità dei soggetti coinvolti nel trattamento dei dati personali; l'introduzione della figura del data protection officer; il nuovo obbligo della data breach notification e il mutato, più severo, regime sanzionatorio.

All'esame delle norme del Regolamento si affianca la valutazione del relativo impatto sulla disciplina nazionale e un confronto con la Direttiva 95/46/CE.

Giusella Finocchiaro, avvocato, ordinario di diritto privato e diritto di Internet presso l'Università di Bologna, Presidente della Commissione Uncitral sul commercio elettronico nonché Presidente della Commissione istituita presso il Ministero della Giustizia che ha redatto la proposta di coordinamento fra il Regolamento europeo e il Codice Privacy. E' già autrice, tra le molte pubblicazioni, del commentario al Codice Privacy edito da questa stessa casa editrice.

https://www.key4biz.it/la-protezione-dei-dati-personali-in-italia/265198/

Facebook, Libra spaventa la

Fed. Powell: ‘Rischio privacy e stabilità finanziaria’

La valuta digitale che **Facebook** intende lanciare nel 2020 solleva “*molte preoccupazioni serie*” legate alla privacy e alla stabilità finanziaria. Lo ha detto **Jerome Powell**, governatore della **Federal Reserve**, nel corso della sua testimonianza semestrale al Congresso Usa.

Su **Libra** Powell ha dichiarato: “*Ci sono molte preoccupazioni dovute alla privacy, riciclaggio di denaro, protezione dei consumatori e stabilità della struttura finanziaria globale. Il processo per affrontare queste preoccupazioni dovrebbe essere lento e accurato, non deve essere fatto di fretta. Per questo motivo la Fed ha creato un gruppo di lavoro per un coordinamento con altri regolatori per studiare approfonditamente la criptovaluta di Facebook*“.

Powell ha anche confermato di aver incontrato i rappresentanti di Facebook nei mesi precedenti l’annuncio del progetto ma di non esserne uscito soddisfatto dell’esito dei colloqui.

Le preoccupazioni

Le preoccupazioni di Powell arrivano sulla scia di commenti simili da parte dei maggiori regolatori in Europa e in Asia. Domenica scorsa, **Benoît Cœuré,** dirigente della Banca centrale europea, ha definito Libra come un “*campanello d’allarme*” per i regolatori, dicendo che non può operare in un ‘vuoto normativo’ al di fuori della struttura tipica delle banche centrali.



Il vice direttore dei pagamenti del Banca Popolare Cinese **Mu Changchun** ha affermato che Facebook deve ancora spiegare come gestirà la privacy degli utenti, il riciclaggio di denaro o preoccupazioni per il terrorismo e ha dichiarato che la criptovaluta deve essere regolata dalle autorità monetarie.

La stessa presidente della Financial Services House **Maxine Waters** ieri ha ribadito che lo sviluppo di Libra dovrebbe essere congelato fino a quando non saranno affrontate le crescenti preoccupazioni sul suo impatto.

Secondo la **CNBC** infatti, il crescente calo ha portato a un elevato scetticismo dell'industria secondo cui il progetto **Libra** sarà spostato dalla data di lancio prevista per la prima metà del 2020.

https://www.key4biz.it/facebook-libra-spaventa-la-fed-powell-rischio-privacy-e-stabilita-finanziaria/264926/

Silent Mac update nukes

dangerous webserver installed by Zoom



reader comments

79 with 47 posters participating

Share this story

Apple said it has pushed a silent macOS update that removes the undocumented webserver that was installed by the Zoom conferencing app for Mac.

The webserver accepts connections from any device connected to the same local network, a security researcher disclosed on Monday. The server continues to run even when a Mac user uninstalls Zoom. The researcher showed how the webserver can be abused by people on the same network to force Macs to reinstall the conferencing app. Zoom issued an emergency patch

on Tuesday in response to blistering criticism from security researchers and end users.

Apple on Wednesday issued an update of its own, a company representative speaking on background told Ars. The update ensures the webserver is removed—even if users have uninstalled Zoom or haven't installed Tuesday's update. Apple delivered the silent update automatically, meaning there was no notification or action required of end users. The update was first reported by TechCrunch.

Apple's update causes Zoom users who click on a conference link to receive a prompt requiring them to confirm they want to join. Previously, clicking on a link—or even encountering a link hidden in a malicious website—automatically opened Zoom and put them into the conference. Zoom developers came under criticism for this behavior as well, because it had the potential to catch users off-guard and expose them to hackers.

Apple occasionally issues silent updates to block malware that's actively circulating on the Internet. It's less common for the company to issue silent updates that block or remove something installed by an app users installed by choice. The Apple representative said company took this action to protect users against risks posed by the webserver. The Zoom app is installed on about 4 million Macs, researcher Jonathan Leitschuh estimated.

Representatives from Zoom didn't respond to an email seeking comment for this post.

https://arstechnica.com/?p=1534287