# UHD Blu-ray: una minaccia alla libertà degli utenti

Il sistema UHD Blu-ray è stato progettato per limitare la libertà degli utenti. Impedisce la riproduzione di dischi su dispositivi non autorizzati e limita la copia dei contenuti. Questo sistema rappresenta un esempio di come le tecnologie proprietarie possano essere utilizzate per limitare le libertà fondamentali degli utenti.

https://www.gnu.org/proprietary/all.html

# UEFI: una falla di sicurezza che espone i computer a minacce persistenti

UEFI, un’interfaccia firmware presente in molti computer moderni, introduce vulnerabilità che possono essere sfruttate per installare minacce persistenti difficili da rilevare. La natura proprietaria dell’UEFI impedisce agli utenti di esaminare e correggere autonomamente queste vulnerabilità, rendendo i loro sistemi esposti a rischi significativi.

https://www.gnu.org/proprietary/all.html

# Spotify abbandona il suo dispositivo musicale, condannando gli utenti al rifiuto elettronico

Spotify ha interrotto il supporto per il suo dispositivo musicale proprietario, rendendolo inutilizzabile. Gli utenti non possono più aggiornare o riparare il dispositivo a causa della sua natura proprietaria. Hanno chiesto a Spotify di rilasciare il software come software libero, ma la richiesta è stata respinta.

https://www.gnu.org/proprietary/all.html

# Microsoft adotta tattiche aggressive per promuovere Edge e Bing a spese

Microsoft sta utilizzando tattiche aggressive e scorrette per convincere gli utenti a passare al suo browser web Edge e al motore di ricerca Bing. Tra le pratiche contestate, l’iniezione di pubblicità pop-up invasive nel browser Chrome e l’importazione dei dati di navigazione degli utenti senza il loro esplicito consenso.

https://www.gnu.org/proprietary/all.html

# GM: la spia a quattro ruote che monitora gli automobilisti e vende i loro dati alle assicurazioni

GM raccoglie dati di guida dettagliati dai suoi veicoli, tra cui velocità, posizione e frenate, e li condivide con le compagnie assicurative tramite data broker. Queste informazioni vengono utilizzate per aumentare i premi assicurativi in base al comportamento di guida.

https://www.gnu.org/proprietary/all.html

# Telecamere di sorveglianza: quando la sicurezza si trasforma in strumento di controllo per governi terzi

Le telecamere di sorveglianza installate da un governo potrebbero essere utilizzate per la sorveglianza da parte di altri governi se il software che le controlla è non libero. La mancanza di trasparenza e di controllo sul codice sorgente del software proprietario crea un rischio concreto di accesso e utilizzo non autorizzato dei dati raccolti.

https://www.gnu.org/proprietary/all.html

# Microsoft: OneDrive, il software che obbliga gli utenti a giustificarsi per chiuderlo

Microsoft ha introdotto in OneDrive, il suo servizio di archiviazione cloud, un messaggio che obbligava gli utenti a fornire una motivazione per la chiusura del programma. La funzione, percepita da molti come invadente e irrispettosa della libertà degli utenti, è stata rimossa solo dopo numerose proteste. Questo episodio evidenzia come le aziende produttrici di software proprietario tendano a esercitare un controllo eccessivo sui propri utenti, limitando la loro libertà di scelta e di azione.

https://www.gnu.org/proprietary/all.html

# Newag: DRM sui treni, quando la tecnologia blocca la riparazione e limita la libertà

Newag, un produttore di treni polacco, utilizza il DRM (Digital Rights Management) per impedire le riparazioni da parte di terzi sui suoi treni. Il software del treno blocca il funzionamento se rileva la presenza di riparatori non autorizzati o se il treno è fermo per un certo periodo di tempo. Il sistema limita la libertà di riparare e modificare i beni.

https://www.gnu.org/proprietary/all.html

# LogoFAIL: una falla di sicurezza che mette a rischio i computer con UEFI

I computer dotati di UEFI (Unified Extensible Firmware Interface) sono vulnerabili a LogoFAIL, un difetto di progettazione che consente di sostituire il logo del BIOS con codice dannoso. Gli utenti non possono risolvere il problema a causa del firmware UEFI non libero, che impedisce loro di accedere al codice sorgente e di implementare autonomamente le necessarie misure di sicurezza.

https://www.gnu.org/proprietary/all.html

# Smartphone connessi alle auto: una minaccia alla privacy degli automobilisti

Le auto moderne consentono agli utenti di connettere i propri smartphone, ma questa funzione, spesso presentata come un vantaggio per la comodità e l'intrattenimento, cela un lato oscuro: la spia di chiamate e messaggi, con i dati inviati al produttore dell'auto e, potenzialmente, anche alle autorità governative.

https://www.gnu.org/proprietary/all.html

# Clash Royale: un gioco online studiato per creare dipendenza e spingere al consumo

Clash Royale, un popolare gioco online, utilizza un sistema di “gacha” ottimizzato per creare dipendenza nei giocatori e spingerli a spendere denaro per ottenere vantaggi virtuali. Il sistema, basato su meccanismi di ricompensa casuale e sulla pressione sociale, può portare a comportamenti compulsivi e a spese incontrollate, soprattutto tra i più giovani.

# Google Nest: la sorveglianza domestica 24/7 a pagamento

Le telecamere di sorveglianza Google Nest sono sempre connesse ai server di Google, registrano video 24 ore su 24, 7 giorni su 7 e richiedono un abbonamento per l'archiviazione dei dati. Questo sistema solleva preoccupazioni sulla privacy degli utenti, in quanto Google ha accesso a un flusso continuo di immagini e informazioni provenienti dalle loro abitazioni.

https://www.gnu.org/proprietary/all.html

# Apple: il “parts pairing” che blocca le riparazioni e costringe gli utenti a rivolgersi all’azienda

Apple utilizza il “parts pairing” per bloccare le riparazioni non autorizzate sui suoi dispositivi. I numeri di serie dei componenti sono codificati nel software del dispositivo, causando malfunzionamenti se sostituiti con parti di altri dispositivi, anche dello stesso modello. Questo sistema obbliga gli utenti a rivolgersi ad Apple per qualsiasi riparazione.

https://www.gnu.org/proprietary/all.html

# Samsung Push Service: l’app che bombarda gli utenti con pubblicità indesiderate

L’app proprietaria Samsung Push Service invia notifiche agli utenti riguardanti gli aggiornamenti delle app Samsung, ma spesso si tratta di pubblicità per giochi. L’app, considerata da molti invadente e fastidiosa, non può essere disattivata in modo permanente, limitando il controllo degli utenti sui propri dispositivi.

https://www.gnu.org/proprietary/all.html

# Chamberlain Group: l’azienda che blocca l’utilizzo di software libero con i suoi apriporta per garage

Chamberlain Group impedisce agli utenti di utilizzare software di terze parti, inclusi quelli liberi, con i suoi apriporta per garage, promuovendo l’uso esclusivo del suo software proprietario. L’app mobile ufficiale, oltre a essere chiusa e non controllabile dagli utenti, è infestata da pubblicità invasive che promuovono i servizi e i dispositivi dell’azienda.

https://www.gnu.org/proprietary/all.html

# Australia: la “maledizione” dei dispositivi “intelligenti” se manca internet

In Australia, i dispositivi “intelligenti” sono spesso progettati per essere sempre connessi a internet. In caso di interruzione della connessione anziché funzionare autonomamente o con funzionalità ridotte, diventano completamente inutilizzabili. Questa dipendenza da internet limita la libertà degli utenti e li rende vulnerabili ai problemi di connettività.

https://www.gnu.org/proprietary/all.html

# Stampanti 3D: quando un malfunzionamento del server scatena stampe incontrollate

Alcune stampanti 3D, connesse a un server remoto per il controllo, hanno iniziato a stampare senza il consenso dell’utente a causa di un malfunzionamento del server stesso. L’episodio, che ha causato danni significativi agli utenti, evidenzia i rischi connessi alla dipendenza da server remoti.

---

https://www.gnu.org/proprietary/all.html

# Yandex: i dati delle corse in taxi consegnati ai servizi segreti russi

Yandex, una società russa che offre servizi di trasporto tramite l’app Yango, ha iniziato a condividere i dati delle corse in taxi con il Servizio di sicurezza federale russo (FSB). Le informazioni condivise, che includono dati personali dei passeggeri e dei conducenti, come posizione, ora e destinazione delle corse, sollevano preoccupazioni sulla privacy degli utenti.

# Case automobilistiche bocciate ai test sulla privacy

Mozilla ha condotto un’indagine sulla privacy delle case automobilistiche, scoprendo che tutte le marche analizzate hanno fallito i test. Alcune case automobilistiche raccolgono dati sensibili, tra cui “attività sessuali” e “informazioni genetiche”. La mancanza di trasparenza e di controllo sulla raccolta e l’utilizzo di questi dati solleva serie preoccupazioni sulla tutela della privacy degli automobilisti.

https://www.gnu.org/proprietary/all.html

# Windows 11: installazione solo con internet e account Microsoft, la privacy degli utenti a rischio

Windows 11 Home e Pro richiedono una connessione internet e un account Microsoft per completare l'installazione, eliminando la possibilità di creare un account locale. Questa pratica solleva preoccupazioni sulla privacy degli utenti e limita la libertà di utilizzare il sistema operativo in modo anonimo e offline.

https://www.gnu.org/proprietary/all.html

# “Fattorie di trascrizione”: le aziende tecnologiche ascoltano le nostre conversazioni

Le aziende tecnologiche che aggiungono microfoni a prodotti come frigoriferi, assistenti vocali e veicoli stanno creando “fattorie di trascrizione” in cui i dipendenti ascoltano le conversazioni degli utenti per migliorare gli algoritmi di riconoscimento vocale. Questa pratica solleva preoccupazioni sulla privacy e sulla possibilità di accesso e utilizzo improprio di informazioni personali e conversazioni private.

https://www.gnu.org/proprietary/all.html

# Philips Hue: la “luce intelligente” che obbliga gli utenti a cedere i propri dati per accendere una lampadina

Philips Hue, un popolare sistema di automazione domestica, sta pianificando di obbligare gli utenti ad accedere al server dell’app per controllare le lampadine e utilizzare altre funzionalità. Questa mossa solleva preoccupazioni sulla privacy degli utenti, in quanto l’accesso al server permetterà a Philips Hue di raccogliere dati sulle loro abitudini di utilizzo.

https://www.gnu.org/proprietary/all.html

# Auto a guida autonoma: telecamere sempre attive, la sorveglianza stradale a 360 gradi

Le auto a guida autonoma utilizzano telecamere interne ed esterne per registrare video costantemente. I governi hanno già raccolto questi video segretamente, sollevando preoccupazioni sulla privacy dei cittadini e sulla possibilità di utilizzo improprio di queste informazioni. La proliferazione di telecamere sui veicoli autonomi crea una rete di sorveglianza capillare che potrebbe essere sfruttata per monitorare gli individui.

https://www.gnu.org/proprietary/all.html

# “Bossware”: il software spia che trasforma il lavoro a distanza in un incubo di sorveglianza

Alcuni datori di lavoro stanno costringendo i dipendenti a utilizzare software di monitoraggio sui propri computer, anche durante il lavoro a distanza. Questi programmi proprietari, definiti “bossware”, possono acquisire screenshot, registrare i tasti premuti, registrare audio e video, violando la privacy dei dipendenti e creando un clima di ansia e controllo.

https://www.gnu.org/proprietary/all.html

# Microsoft Edge: il browser che invia le immagini visualizzate ai server di Microsoft

Per impostazione predefinita, Microsoft Edge invia gli URL delle immagini visualizzate dagli utenti ai server di Microsoft per “migliorarle”. Questa pratica, non sempre chiara agli utenti, solleva preoccupazioni sulla privacy, in quanto le immagini potrebbero finire sui server della NSA o di altre agenzie governative, senza il consenso esplicito degli utenti.

https://www.gnu.org/proprietary/all.html

# Termostati Honeywell: quando la “casa intelligente” diventa inaffidabile e vulnerabile

I termostati Honeywell, progettati per essere controllati da remoto tramite un’app, si sono dimostrati inaffidabili a causa di problemi di connessione ricorrenti con il server a cui sono connessi. Questa dipendenza da un server esterno rende i termostati vulnerabili ai problemi di connettività e limita il controllo degli utenti sulla propria abitazione.

https://www.gnu.org/proprietary/all.html

# HP: la stampante che si auto-sabota per bloccare le cartucce non originali

HP ha utilizzato una backdoor nei suoi software per installare malware sulle stampanti, impedendo l'utilizzo di cartucce d'inchiostro non HP e costringendo gli utenti ad acquistare solo prodotti originali, spesso a prezzi maggiorati. Questa pratica, definita "dynamic security" da HP, è in realtà un sistema di DRM che limita la libertà degli utenti e li danneggia economicamente.

https://www.gnu.org/proprietary/all.html

# Microsoft: la fine forzata di Internet Explorer e l’imposizione di Edge

Microsoft sta disabilitando Internet Explorer da remoto, reindirizzando forzatamente gli utenti a Microsoft Edge. Questa pratica, che limita la libertà di scelta degli utenti e li obbliga a utilizzare un browser che potrebbe non preferire, solleva preoccupazioni sul potere eccessivo delle aziende produttrici di software proprietario.

https://www.gnu.org/proprietary/all.html

# Microsoft: l’aggiornamento che installa segretamente un programma di sorveglianza

Microsoft ha rilasciato un aggiornamento che installa segretamente un programma di sorveglianza sui computer degli utenti per raccogliere dati sui programmi installati. Questo programma, che opera in background senza il consenso esplicito degli utenti, viola la loro privacy e solleva preoccupazioni sulla trasparenza e sull’affidabilità di Microsoft.

https://www.gnu.org/proprietary/all.html

# Volkswagen: la tracciabilità costante degli automobilisti e la vendita dei loro dati

Volkswagen traccia la posizione di tutti i conducenti dei suoi veicoli e vende i dati a terzi, ma si rifiuta di utilizzare i dati per implementare funzionalità a vantaggio dei clienti a meno che non paghino un extra. Questa pratica, che viola la privacy degli automobilisti e li sfrutta economicamente, evidenzia come le aziende automobilistiche stiano trasformando i veicoli in strumenti di sorveglianza e di profitto.

https://www.gnu.org/proprietary/all.html