Connaissez-vous le réseau plus anonyme et rapide que Tor ?

	Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Le Massachusetts Institute of technology (MIT), aux États-Unis, et l'École polytechnique fédérale de Lausanne (EPFL), en Suisse, annoncent la création d'un nouveau réseau anonyme sur Internet, baptisé Riffle, encore plus rapide et sécurisé que Tor, la référence en la matière.

A l'image de Tor, le plus célèbre des réseaux de ce type, Riffle permet de surfer et de communiquer en théorie en parfait anonymat en s'appuyant sur le protocole de chiffrement "en oignon". Cela signifie qu'il est composé d'une multitude de couches de routeurs, autant de "noeuds" par lesquels transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. Les données personnelles de l'internaute (adresse IP, pays) ne peuvent ainsi plus être localisées par les sites visités. Cette alternative serait toutefois selon ses créateurs bien plus sécurisée et fiable que Tor et consorts.
Selon le MIT, l'avantage de Riffle repose sur ses serveurs, capables de permuter l'ordre de réception des messages rendant l'analyse du trafic encore plus complexe et favorisant donc l'anonymat des utilisateurs. Si, par exemple, les messages provenant d'expéditeurs Alice, Bob et Carol atteignent le premier serveur dans l'ordre A, B, C, ils peuvent être renvoyés dans un ordre complètement différent au serveur suivant, et ainsi de suite. Les utilisateurs du réseau deviennent alors en théorie parfaitement impossibles à identifier.
Dernier point non négligeable, Riffle proposerait une meilleure bande passante, garantissant une navigation plus fluide et des échanges de fichiers accélérés.
Cette annonce intervient alors que la sécurité de Tor a récemment été mise à mal par des chercheurs de la Northeastern University de Boston (États-Unis) qui a découvert plus d'une centaine de "nœuds-espions", en réalité des serveurs, capables d'identifier des services cachés et éventuellement de les pirater.
Davantage de détails sur Riffle, toujours en phase de développement, seront communiqués lors de sa présentation officielle à la conférence Privacy Enhancing Technologies Symposium (PETS), qui se déroulera du 19 au 22 Juillet à Darmstadt (Allemagne).
Article original de Etienne Froment

Réagissez à cet article

Original de l'article mis en page : Riffle, le nouveau réseau garanti plus anonyme et rapide que Tor | geeko

Google met en avant ses succès contre le piratage

Google met en avant ses succès contre le piratage

Google combat le piratage, et cherche de plus en plus à le faire savoir. En plus de son filtrage qui limite l'utilisation de Google pour trouver des contenus piratés, Google a reversé 2 milliards de dollars aux ayants droits dont les contenus ont été mis en ligne sur YouTube. Difficile, toutefois, de savoir si c'est beaucoup… ou très peu.

Depuis plusieurs années, Google aime à s'afficher comme défenseur des droits d'auteur, alors que le moteur de recherche a souvent été vilipendé par des ayants droit qui lui reprochaient de donner trop facilement accès à des sites pirates. La firme de Mountain View, qui doit soigner des partenaires commerciaux pour YouTube et pour ses services de distributions de contenus sur Google Play, publie même désormais un document de 62 pages pour expliquer « Comment Google combat le piratage ».

Sur son blog dédié aux politiques publiques, Google précise certains points qui ont été mis à jour dans ce document, lequel était inimaginable quand les recherches avec des mots clés comme « torrents », « mp4 » ou « streaming » renvoyaient encore le plus souvent vers des pages de sites pirates.

NOS ALGORITHMES DE CLASSEMENT DES RECHERCHES RÉTROGRADENT CE SITE DANS LES FUTURS RÉSULTATS DE RECHERCHE

Aujourd'hui, « la grande majorité des requêtes liées à des médias que les utilisateurs soumettent chaque jour retournent des résultats qui incluent seulement des liens vers des sites légitimes », se félicite le géant de la recherche. Et lorsque l'utilisateur cherche à forcer la recherche avant des mots clés spécifiques au streaming gratuit ou au téléchargement sur BitTorrent, « nos systèmes de traitement des demandes de suppressions pour violation du droit d'auteur gèrent des millions d'URL chaque jour », qui font qu'en cas d'infractions répétées sur un site, « nos algorithmes de classement des recherches rétrogradent ce site dans les futurs résultats de recherche ».

2 MILLIARDS DE DOLLARS REVERSÉS PAR YOUTUBE AUX AYANTS DROITS

Sur YouTube, la chasse au piratage et aux utilisations non autorisées d'extraits de vidéos ou de musique est fortement automatisée, avec Content ID qui détecte les empreintes des contenus et permet aux ayants droit de choisir, soit la suppression des exploitations illégales, soit de recevoir les revenus publicitaires attachés à cette exploitation – ce qui n'est pas sans poser régulièrement quelques problèmes de retraits abusifs ou de détournement de revenus par des ayants droits qui s'accaparent toute œuvre dérivée.

Ainsi selon Google, 98 % des problèmes de droits d'auteur sur YouTube sont désormais gérés directement avec Content ID, ce qui ne laisse que 2 % de demandes de suppression envoyées par formulaire. ***Dans 90 % des cas les ayants droit choisissent de percevoir une rémunération*** *plutôt que demander le retrait des vidéos mises en cause.*

Google dit ainsi avoir versé 2 milliards de dollars de droits grâce à Content ID depuis son lancement, ce qui est beaucoup et peu à la fois. Il ne dit pas à combien de visionnages cela correspond, ce qui ne permet pas de calculer le gain par vidéo vue. La page officielle des statistiques de YouTube, dont la mise à jour ne semble pas récente, indique que « depuis juillet 2015, plus de 8 000 partenaires (parmi lesquels de nombreux grands groupes audiovisuels, studios de cinéma et maisons de disques) ont revendiqué plus de 400 millions de vidéos via Content ID ».

Le système est aujourd'hui capable de détecter 50 millions d'œuvres, réattribuées à leurs propriétaires respectifs en cas de réclamation.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Google met en avant ses succès contre le piratage – Politique – Numerama

---

Les géants d’internet contrôlent de plus en plus l’information

Les géants d’internet contrôlent de plus en plus l’information

---

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont*« désormais directement impliqués dans tous les aspects du journalisme »*, fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.

« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. *« L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles »*, considère l'institut Pew.

Désormais, les géants d'internet *« supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) »*, affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. *« Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures »*, prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

Une étude réalisée par Nic Newman du Reuters Institute a fait état de*« préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents »*, selon le blog de son auteur. Mais *« les jeunes préfèrent les algorithmes aux éditeurs »* qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.

« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. *« Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles »*, a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, *« parce que sans cela, tous les jours à midi, le déjeuner serait une tendance »*. Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors,*« des questions quant à la transparence »* de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. *« Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit »*, estime l'universitaire, pour qui *« il faut réfléchir à des normes de transparence ».*

Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. *« Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme »*, reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. *« D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient »* en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr

---

Facebook regarde dans quels magasins vous faites vos courses

Facebook regarde dans quels magasins vous faites vos courses

Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.

Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d'un carrousel – pour indiquer à l'internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s'inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d'afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s'y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l'occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu'environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n'a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n'est d'ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Moutain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l'utilisateur et de sa géolocalisation.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

---

La double authentification de

Google contournée par des hackers

	La double authentification de Google contournée par des hackers

Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !

La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

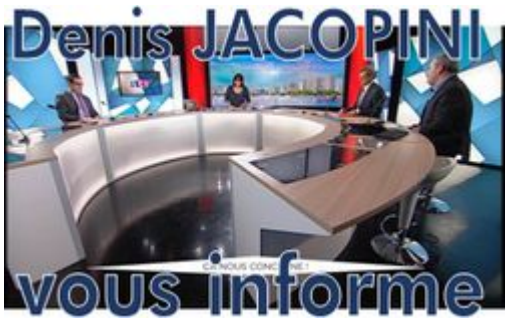
Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient. Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

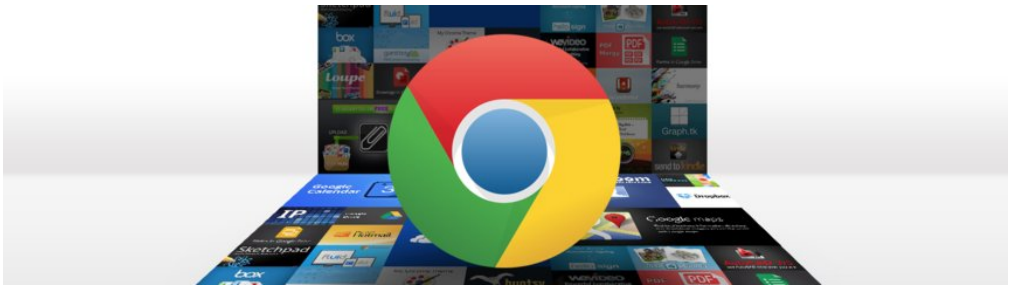
Réagissez à cet article

Original de l'article mis en page : La double authentification de Google contournée par des hackers

Google Chrome v51 corrige 42 failles de sécurité

	Google Chrome v51 corrige 42 failles de sécurité

Google vient de publier une nouvelle mouture stable de son navigateur Chrome, en version 51.



Chrome 51 est disponible au téléchargement pour Windows, OS X et Linux. Cette mouture intègre les interfaces de programmation Credential Management. Avec ces dernières, les sites Internet peuvent directement communiquer avec le gestionnaire de mots de passe mais aussi avec Google Smartlock ou les autorisations liées à un compte Facebook. Le processus de connexion s'en trouve simplifié, notamment sur smartphones.

L'équipe a en outre procédé à des optimisations du chargement des pages, notamment en ne récupérant pas les éléments non visibles à l'écran. Il en résulterait une meilleure gestion de la batterie avec un navigateur 30% moins gourmand.

Coté sécurité, les ingénieurs ont comblé 42 failles de sécurité en reversant au total 65 000 dollars aux experts ayant partagé leurs recherches. Retrouvez davantage d'informations sur cette page.

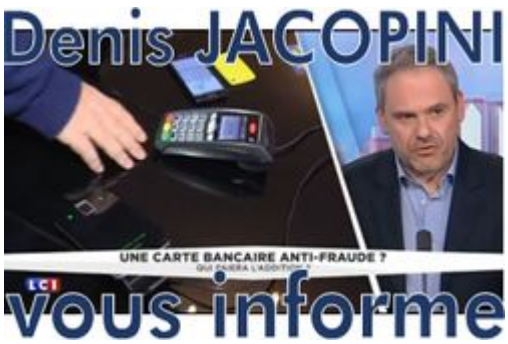
- Téléchargez Google Chrome 51 pour Windows
- Téléchargez Google Chrome 51 pour OS X
- Téléchargez Google Chrome 51 pour Linux

Article de Guillaume Belfiore

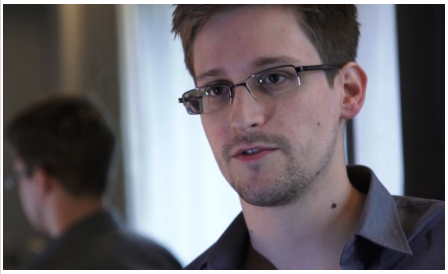
Réagissez à cet article

Source : *Chrome 51 : Google corrige 42 failles de sécurité*

Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

	Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google

Le lanceur d'alerte à l'origine du scandale de la surveillance de la NSA et des spécialistes en sécurité informatique mettent en cause la politique de chiffrement mise en place par Google pour sa nouvelle messagerie.



Haro sur Allo. La nouvelle application de messagerie instantanée de Google était l'une des principales annonces de la conférence Google I/O, mercredi 18 mai, au quartier général de l'entreprise à Mountain View. Fondée sur l'intelligence artificielle, elle est capable de comprendre le langage humain et affine son algorithme au fil des conversations afin de proposer des suggestions de plus en plus pertinentes. Disponible cet été sur Android et iOS, elle est déjà au coeur d'une controverse d'experts.
Allo possède des paramètres de sécurité renforcés. Un mode « incognito » permet de chiffrer de bout en bout les messages afin de les rendre illisibles pour une personne extérieure à la conversation. Seuls les participants à la discussion sont en mesure de les déchiffrer. Google lui-même ne peut pas y accéder et répondre à d'éventuelles requêtes judiciaires des autorités.
Cette option est basée sur le protocole open source Signal, développé par Open Whispers Systems. C'est le même protocole de chiffrement que WhatsApp, dont les discussions sont cryptées de bout en bout depuis le mois d'avril. Mais à l'inverse de WhatsApp et d'autres messageries sécurisées actuelles (Viber, Signal, iMessage) le chiffrement des conversations n'est pas activé par défaut sur Allo. C'est aux utilisateurs d'effectuer la démarche.

Les experts en sécurité déconseillent Allo

Des experts en cybersécurité s'interrogent déjà sur la pertinence d'une telle fonction, arguant que de nombreux utilisateurs ne feront pas la démarche de l'activer. « La décision de Google de désactiver par défaut le chiffrement de bout en bout dans la nouvelle application de discussion instantanée Allo est dangereuse et la rend risquée. Évitez-la pour l'instant », a conseillé Edward Snowden sur Twitter.
Le lanceur d'alerte à l'origine du scandale des programmes de surveillance de la NSA en 2013 n'est pas le seul à critiquer le choix de Google. Nate Cardozo, représentant de l'EFF, une association américaine de défense des libertés numériques, a estimé pour sa part que « présenter la nouvelle application de Google comme étant sécurisée n'est pas juste. L'absence de sécurité par défaut est l'absence de sécurité tout court ».
« Rendre le chiffrement optionnel est une décision prise par les équipes commerciales et juridiques. Elle permet à Google d'exploiter les conversations et de ne pas agacer les autorités », a encore indiqué Christopher Soghoian, membre de l'Association américaine pour les liberté civiles.

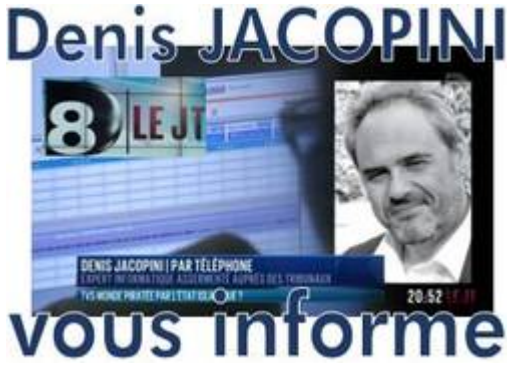
L'intelligence artificielle, priorité de Google

Après avoir pris fait et cause pour Apple dans le bras de fer qui l'a opposé au FBI sur le déblocage de l'iPhone chiffré d'un des terroristes de San Bernardino, Google n'est donc pas allé aussi loin que WhatsApp en généralisant le chiffrement des discussions. Un ingénieur en sécurité de Google a expliqué sur son blog comment la société avait dû arbitrer entre la sécurité des utilisateurs et les services d'intelligence artificielle d'Allo.
Pour profiter pleinement des capacités de Google Assistant implémentées dans Allo, les algorithmes doivent être en mesure d'analyser les conversations, ce qui n'est possible qu'en clair. « Dans le mode normal, une intelligence artificielle lit vos messages et utilise l'apprentissage automatique pour les analyser, comprendre ce que vous voulez faire et vous donner des suggestions opportunes et utiles », explique Thaï Duong.
Ce parti pris pourrait évoluer d'ici la sortie de l'application cet été. Le site américain TechCrunch a publié des paragraphes que l'ingénieur avait publié dans son article avant de les supprimer. Il affirme qu'il est en train de « plaider en faveur d'un réglage avec lequel les usagers peuvent choisir de discuter avec des messages en clair », pour interagir avec l'intelligence artificielle en l'invoquant spécifiquement, sans renoncer à la vie privée. En somme, proposer « le meilleur des deux mondes »… [Lire la suite]

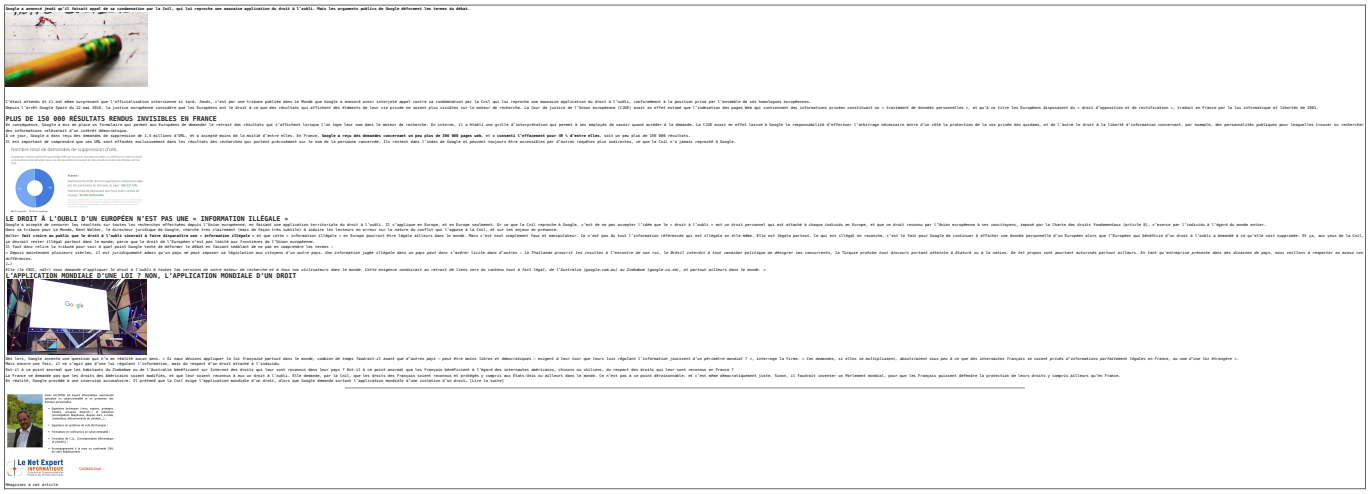
Réagissez à cet article

Source : *Pourquoi Edward Snowden déconseille Allo, la nouvelle messagerie de Google*

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

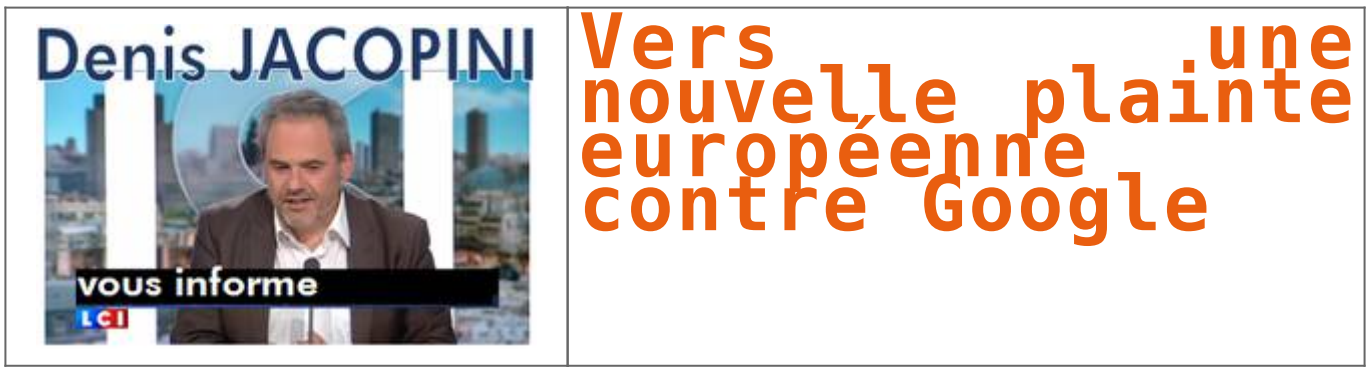


Google fait semblant de ne rien comprendre à ce qu'exige la Cnil



Source : *Droit à l'oubli : Comment Google feint de ne rien comprendre à ce qu'exige la Cnil – Politique – Numerama*

Vers une nouvelle plainte européenne contre Google



Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

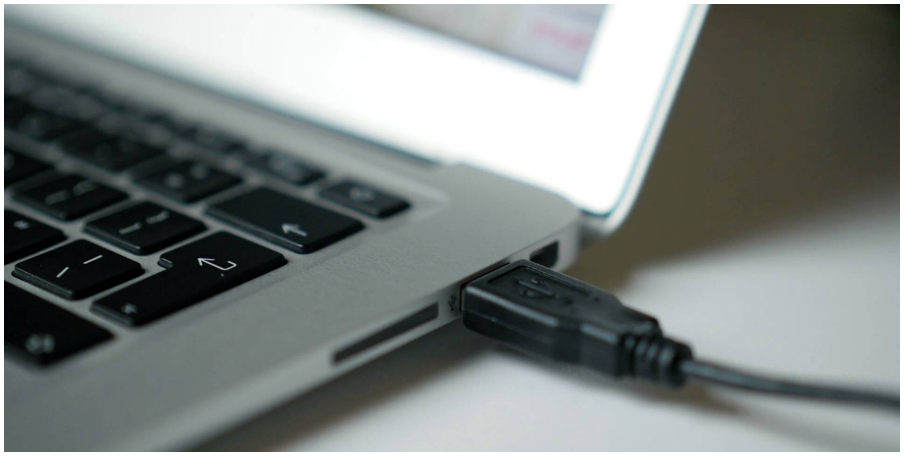
Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

Réagissez à cet article

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*

Des drivers USB dans le Cloud pour piloter à distance les périphériques



Piloter à distance des périphériques USB grace au Cloud, ca vous dit ?

Des ingénieurs de Google proposent une norme pour piloter à distance des périphériques USB, à travers un driver situé dans le Cloud, appelé uniquement lorsqu'il est nécessaire. Objectif : toujours mieux intégrer le Web et le hardware.

Deux ingénieurs de Google, Reilly Grant et Ken Rockot, proposent au World Wide Web Consortium (W3C) de travailler sur une nouvelle norme appelée WebUSB, qui permettrait de piloter à distance des périphériques USB sans avoir à installer de drivers sur son ordinateur. Le pilotage des appareils branchés au PC ou au Mac se ferait directement depuis le cloud.
L'idée est de faciliter l'utilisation des appareils USB qui sortent de l'ordinaire (par exemple un calibreur d'écran, une imprimante 3D, un circuit Arduino, un chauffe-tasse USB,…), et d'offrir aux services en ligne une API sécurisée qui permettrait de les configurer et de les exploiter quelle que soit la machine de l'utilisateur.

USB-plug

Puisqu'il n'y a plus de drivers à installer et que tout le pilotage se fait à distance par internet, les périphériques seraient fonctionnels aussi bien sous Windows que sous Mac OS, Linux… ou même Chrome OS ou Android. On voit donc bien l'intérêt pour Google d'une telle norme, qui accélérerait la « terminalisation » des ordinateurs, de plus en plus réduits à assurer l'affichage, alors que le stockage et la puissance de calcul sont déportés sur le cloud.
En pratique, la norme proposée prévoit que les constructeurs d'appareils USB puissent définir dans le firmware un ou plusieurs domaines (par exemple chauffe-tasse.numerama.com) qui sont autorisés à piloter ou à mettre à jour l'appareil. Seules les connexions sécurisées vers ces domaines seraient permises. Les autres sites internet qui veulent exploiter les possibilités d'un périphérique devraient alors intégrer le support du driver à travers une iframe, qui appelle le pilotage à travers une interface autorisée.

EN CONTREPARTIE, LES UTILISATEURS PERDENT ENCORE UN PEU PLUS LE CONTRÔLE DE LEURS APPAREILS

Grant et Rockot assurent que leur technique est même plus sûre que les drivers USB traditionnels, qui peuvent être piratés pour obtenir, par exemple, le contrôle à distance d'une webcam.
Pour défendre leur idée, les ingénieurs prennent l'exemple d'une imprimante 3D et d'un service de modèles 3D à télécharger, comme Thingiverse. Actuellement les utilisateurs sont obligés de télécharger un driver pour leur imprimante, ainsi qu'un logiciel d'impression. Ils doivent télécharger les fichiers STL des modèles 3D, et les ouvrir avec le logiciel d'impression. Mais avec leur idée, Thingiverse pourrait appeler l'API de l'imprimante de l'utilisateur (qui pourrait être déclarée au site par le navigateur), et offrir lui-même une application de calibrage et d'impression des modèles.
L'idée est loin d'être idiote, et c'est certainement une voie d'avenir. Mais elle signifie aussi, en contrepartie, que les utilisateurs perdent encore un peu plus le contrôle de leurs appareils. Ils n'auraient plus vraiment le choix des drivers à installer, ni la possibilité de les modifier pour installer d'autres drivers officieux.
.. [Lire la suite]

Réagissez à cet article

Source : *Des drivers USB dans le Cloud pour piloter à distance les périphériques – Tech – Numerama*