Enquête sur les indiscrétions de Google, Facebook, Apple, Amazon...

Tout ce que les géants du Web savent de vous

Jamais notre vie privée n'a été autant exposée. Chaque jour, sans vous en rendre compte, vous laissez sur Internet des infos personnelles qui sont ensuite stockées et commercialisées à des fins publicitaires. Enquête sur ces pratiques à la Big Brother, fascinantes mais qui commencent à faire peur.

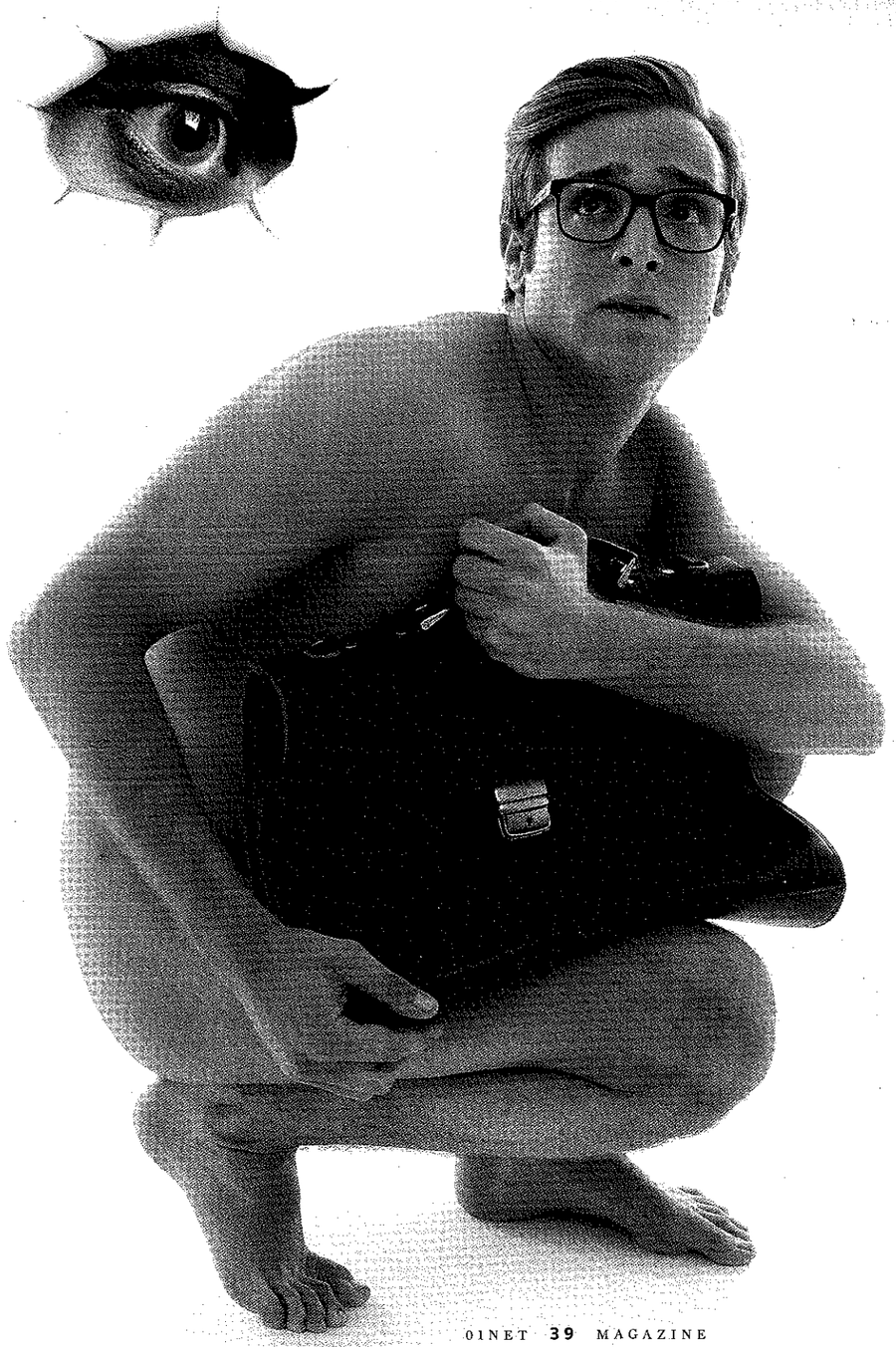
T'as vu la nouvelle assistante du boss ? Sexy, non ? À peine avez-vous posté ce mail à votre collègue de bureau qu'un avertissement s'affiche sur votre écran : "Attention, vous êtes en infraction avec le règlement intérieur de l'entreprise. Le service des ressources humaines est prévenu". Impossible ? Détrompez-vous. Google est aujourd'hui capable de proposer ce mouchard à votre employeur : il vient d'en déposer le brevet !

Des informations très intimes. Certes, le procédé n'est pas encore commercialisé. Mais il illustre ce qu'est devenu Google : un Big Brother que même George Orwell n'aurait jamais pu imaginer. Le célèbre moteur de recherche sait quand vous postez vos mails et à qui, connaît vos habitudes de consommation, les lieux où vous vous déplacez, les sites que vous visitez, les gens avec qui vous communiquez et mille autres choses encore. Il peut analyser toutes ces infos et en déduire votre comportement, vos goûts et même vos préférences politiques ou sexuelles. "Il en sait plus sur votre compte que vous-même", s'inquiète Andy Müller-Maguhn, cofondateur d'European Digital Rights (une ONG qui défend les droits du citoyen numérique), et auteur de "Menace sur nos libertés" (Robert Laffont, 2013).

Les autres géants du Web, Facebook, Apple, Amazon et consorts, emmagasinent un nombre à peu près aussi considérable de données. Les rares curieux qui ont osé demander à l'indiscret Facebook ce qu'il savait sur eux, comme l'étudiant autrichien Max Schrems (voir page 42), ont reçu des documents de 800 à 1 200 pages, la loi ayant obligé la firme à leur répondre. Ils y ont trouvé, entre autres : où, quand et avec quels appareils ils s'étaient connectés, les événements auxquels ils avaient été invités, les publications qu'ils appréciaient. Ils ont même découvert des données qu'ils avaient effacées !

Des conséquences fâcheuses. Des infos plus ou moins confidentielles sur vous-même, vous en laissez sur le Web tous les jours, au fil de vos pérégrinations numériques, la plupart du temps sans vous en rendre compte. S'y ajoutent celles que vos proches fournissent à votre sujet, involontairement, sur les réseaux sociaux. Elles sont stockées dans de gigantesques bases de données, ●●●

DOSSIER COORDONNÉ PAR **AMINE MESLEM** AVEC **AMÉLIE CHARNAY, MARC GIROUD, JEAN-MICHEL MANAT, SÉBASTIEN PIERROT ET KARINE SOLOVIEFF,**



FRANÇOIS DARMIGNY POUR 01NET ; MANNEQUIN : URBAN TALENS & MODELS ; TOMASZ PIETRYSZEK ET TATIANA POPOVA/ISTOCKPHOTO

compilées et exploitées à des fins publicitaires. Le fameux "big data", dans le jargon marketing.

Tout cela peut avoir de fâcheuses conséquences : récemment, les parents traditionalistes d'une jeune Texane, Bobbi Duncan, ont appris que leur fille était lesbienne quand celle-ci a été invitée à participer à un groupe de discussion homosexuel sur Facebook.

Si les géants du Web mettent autant d'ardeur à récolter nos informations privées, c'est qu' ils les vendent à très bon prix et en quantités vertigineuses. "C'est le nouvel or noir", résume Michel Calmejane, de la société Colt Technology, un spécialiste du sujet. Rien qu'en Europe, la commercialisation des données personnelles a généré en 2011 un chiffre d'affaires de 315 milliards d'euros, selon le Boston Consulting Group. Ces revenus colossaux proviennent essentiellement de la pub. Un marché dominé par les Google, Apple et autres Facebook.

Des garde-fous à l'étude. Évidemment, ces firmes assurent qu'elles ne nous veulent que du bien. Qu'il existerait un "pacte" tacite entre elles et les internautes : en échange des données que nous leur fournissons, nous bénéficions de services de plus en plus pointus et sophistiqués. C'est vrai, mais il est permis de s'en inquiéter. Selon Jérémie Zimmermann, porte-parole de la Quadrature du Net, une association de défense des droits des citoyens sur Internet, "le deal est déséquilibré car l'utilisateur n'a en général pas conscience des données qu'il fournit gratuitement".

Le Parlement européen s'attelle à dépoussiérer le cadre législatif sur les données personnelles. Il est question de donner au citoyen le droit de refuser l'exploitation de certaines informations. Mais les firmes font un intense lobbying pour s'y opposer. Un de leurs arguments est que les données personnelles sont vendues sous forme de fichiers anonymes (aucun individu ne peut y être identifié). Mais qu'en sera-t-il demain ? Vu l'extraordinaire potentiel du "big data", de nouveaux garde-fous ne seraient pas de trop pour nous protéger ! ■

GOOGLE, FACEBOOK, AMAZON, APPLE...

Les infos indiscrètes qu'ils récoltent à votre insu

Surf, mail, téléphone, toute la journée vous semez des données qui vont être méthodiquement enregistrées et indexées. Celles que vous pensiez n'avoir jamais divulguées aussi...

Plus ça va, plus on vous pose de questions. Dès que vous voulez vous inscrire sur un service en ligne, il faut remplir des formulaires de plus en plus indiscrets. Mais ces sites ne se contentent pas des infos que vous saisissez de votre plein gré. Ils en collectent beaucoup d'autres, comme les IP des appareils avec lesquels vous vous connectez, les adresses des autres sites que vous visitez ou les mots-clés que vous tapez dans les moteurs de recherche. La liste fait froid dans le dos. Démonstration.

Vous envoyez un mail : il est décortiqué mot à mot

Si vous êtes utilisateur de Gmail, comme 9,6 millions de Français, sachez-le, tout ce que vous faites est surveillé : le contenu de vos messages, et de ceux qui vous écrivent (quelle que soit leur messagerie), est systématiquement analysé par des algorithmes sophistiqués. Ils identifient les mots que vous utilisez et découvrent ainsi vos préoccupations du moment. Le but ? Mieux vous connaître pour mieux vous servir... notamment des pubs ! En clair, vendre au prix fort des profils (très précis, mais anonymes) aux annonceurs pour qu'ils ciblent à la volée leurs publicités.

Pas dangereux, mais très désagréable. Quand vous ouvrez un mail, tournez la tête à droite : des pubs qui résonnent étonnamment avec le contenu de vos messages s'affichent en temps réel. La dernière fois, vous évoquiez la maladie d'un proche, et Google vous a proposé des sites pour organiser des obsèques. Ça ne s'invente pas, malheureusement.

Le remède : changer de messagerie. Et encore... Yahoo! Mail, le plus adopté au monde après Gmail, applique des méthodes similaires. En revanche, Outlook.com de Microsoft (l'ancien Hotmail) et le mail d'Orange s'engagent à ne collecter que les données que vous fournissez lors de votre inscription à leurs services. Microsoft a d'ailleurs lancé aux États-Unis une campagne dénonçant les méthodes de Google : ici, "vous ne verrez pas de publicités basées sur des mots-clés tirés de vos mails personnels".

Vous cherchez une info, vous en livrez sur vous-même

Quand vous lancez une requête dans Google, les mots que vous tapez, l'heure et la date auxquelles vous le faites, les fautes de frappe, le temps qu'a mis la page de résultats à s'afficher, vos clics sur les liens et l'adresse de votre ordi, le pays, votre langue ou encore le navigateur que vous utilisez : tout est enregistré en permanence. Google s'autorise même des supputations en fonction de ce que vous cherchez : il essaiera de deviner votre âge, et si vous êtes un homme ou une femme. Si vous êtes connecté à votre compte Google, c'est encore pire. La recherche sera étendue au réseau social Google+. Le géant du Web va alors puiser, sans votre autorisation, dans les publications de vos contacts. Toutes ces fouilles, pour répondre au mieux à votre requête, mais pas seulement. Les données récupérées sont également exploitées par la régie publicitaire du moteur de recherche, Doubleclick. Le fin du fin : vous ne tomberez plus jamais deux fois sur la même publicité, car Google a de la mémoire.

Difficile d'y échapper : le moteur de recherche Bing, commun à Yahoo! et Microsoft, utilise les mêmes techniques de pistage que Google. Mais au lieu d'interroger Google+, c'est avec Facebook qu'il enrichira sa base de données. Microsoft s'engage cependant à dissocier votre profil de surf de toute information nominative provenant de votre compte mail. L'ex-Big Brother est aujourd'hui le seul à être transparent sur la conservation des données : "Nous supprimons l'adresse IP au bout de 6 mois", peut-on lire, par exemple, dans la déclaration de confidentialité. Une éternité, pour Internet.

Vous surfez : vous êtes suivi par un pixel espion

Quand vous surfez, deux processus se mettent automatiquement en marche : la génération de cookies, ces fichiers d'identification qui mémorisent tout dans votre navigateur, et les pixels espions. Aussi méconnus qu'efficaces, les pixels espions (ou "balises pixel") sont des images quasi invisibles, de la taille d'un pixel, comme leur nom l'indique, intégrées à certaines pages Web. Il suffit de consulter le site pour lancer leur chargement. Vous indiquez alors à l'hébergeur votre provenance et même, plus précisément, la page que vous visitiez juste avant. Par exemple, ne vous demandez plus pourquoi un site affiche des pubs de lingerie quand votre épouse surfe, alors qu'il vous propose à vous la toute dernière gamme de PC Intel. Sur le moment, le résultat peut vous faire sourire, mais à la réflexion, cette surveillance vous agacera... au minimum.

Vous publiez sur Facebook, votre historique vous trahit

Facebook a plusieurs facettes : une partie visible (votre profil) affiche tout ce que vous publiez (photos, commentaires, etc.). Une partie cachée, accessible via l'historique. Depuis fin 2011, le réseau social mémorise vos publications, y compris celles que vous avez supprimées. En fait, ces dernières n'ont été que masquées. Pareil pour la liste de vos amis, qui contient toujours les noms de ceux que vous avez exclus. Dans votre historique, encore, cette photo sur laquelle une obscure rencontre d'un soir vous adressait un baiser compromettant. Jetée à la poubelle, mais facile à retrouver sur Facebook.

Ne vous avisez pas de laisser votre connexion active : si quelqu'un tombait dessus, il pourrait en quelques minutes télécharger l'intégralité de votre archive personnelle. Toutes les photos, avec leurs infos de localisation, toutes les vidéos avec la date et l'heure de la publication, et même les commen- ●●●

Attention aux boutons "J'aime" sur Facebook

Vos clics Facebook en disent long sur vous. C'est la démonstration réussie par deux chercheurs de l'Université de Cambridge. Ils ont analysé les pages dont les internautes sont fans, autrement dit, celles où ces derniers ont cliqué sur le bouton "J'aime" ou sur le bouton +1. Résultat : les chercheurs ont su déterminer l'orientation sexuelle des internautes à 88 %, mais aussi dans 67 % des cas si les sondés étaient en couple ou pas, ou encore à 95 % s'ils étaient de type caucasien ou africain ! De quoi vous faire réfléchir la prochaine fois que vous surfez sur le Web et que vous cliquez sur le fameux bouton "J'aime" situé en bas de la page, qui est connecté à votre compte Facebook, ou sur le bouton +1, lié à votre compte Google+. Plus vous "likez", plus votre profil sur ces réseaux se complète, et de façon très précise.

Votre identité numérique est alors principalement exploitée pour de l'affichage personnalisé de contenu ou de publicité. C'est ainsi qu'en arrivant sur un site d'informations, vous verrez que vos amis ont aimé un article, ou bien sur un site touristique, qu'ils ont apprécié un restaurant. À votre niveau, vous ne pouvez contrôler cette visibilité que vis-à-vis des autres utilisateurs individuels. Mais pas limiter le pistage publicitaire. Dans le cas de Facebook, une fois votre compte créé, il est informé de toutes vos visites au sein de son site mais aussi en dehors. Il est particulièrement intéressé par votre activité lorsque vous cliquez sur une pub. Jusqu'aux achats que vous avez effectués. Facebook explique qu'il stocke ces infos pour des raisons de performance et de sécurité. Et précise qu'elles deviennent anonymes passé 90 jours.

FRANÇOIS DARMIGNY POUR 01NET -; AMANDA ROHDE/ISTOCKPHOTO

Inutile de dire que vous êtes parti en vacances, les voleurs sont déjà au courant

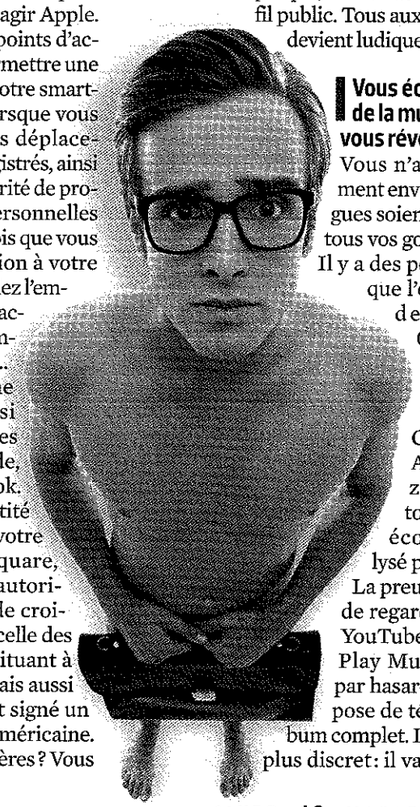
taires de vos ex, nouveaux et amis d'amis. Encore une petite frayeur ? Un proche un peu curieux saura même exactement quand et à quelle heure, combien de fois et combien de temps vous avez consulté le profil d'une certaine Tatiana, esthéticienne à Nantes.

Vous vous localisez... au détriment des autres

En avril 2011, des chercheurs en sécurité découvrent que l'iPhone enregistre la position de tous les points d'accès Wi-Fi rencontrés lors des déplacements des utilisateurs. Date, lieu et heure, tout était rassemblé dans un fichier jusqu'ici tenu secret. Petit scandale qui a immédiatement fait réagir Apple. Cette cartographie de points d'accès ne servirait qu'à permettre une localisation rapide de votre smartphone, par exemple lorsque vous voulez être guidé. Vos déplacements ne sont pas enregistrés, ainsi qu'a pu le vérifier l'autorité de protection des données personnelles (Cnil). Mais à chaque fois que vous demandez votre position à votre smartphone, vous dévoilez l'emplacement des points d'accès Wi-Fi alentour, y compris les box des voisins...

Les conséquences ne sont pas les mêmes si vous utilisez des services comme Google Latitude, Foursquare ou Facebook. Dans ce cas, votre identité est directement liée à votre position. Avec Foursquare, vous donnez même l'autorisation à l'application de croiser votre position avec celle des autres utilisateurs se situant à proximité. Des amis, mais aussi des entreprises qui ont signé un accord avec la société américaine. L'intérêt pour ces dernières ? Vous inciter à rentrer dans une boutique au coin de la rue pour profiter d'offres spéciales. Rien ne se fait à votre insu, mais faute de bien gérer ses paramètres, l'appli peut devenir très bavarde. En 2010, des petits malins avaient créé le site PleaseRobMe, qui se traduit par "Venez Me Cambrioler". Ils y recensaient les maisons laissées vacantes, leur occupant l'ayant annoncé innocemment sur Foursquare. Une affaire qui a fait le tour du Web et servi de leçon à l'éditeur. Depuis, il protège l'emplacement de votre domicile des regards indiscrets. Une maigre consolation pour ceux qui se sont fait piéger.

Google et Facebook proposent des services similaires. Le simple fait de vous localiser et d'utiliser dans la foulée une appli de réseau social indiquera votre emplacement dans chacune de vos publications. Et pour que ce soit encore plus éloquent, vos amis pourront consulter toutes ces informations sur une carte géographique, consultable sur votre profil public. Tous aux abris : le flicage devient ludique.



Vous écoutez de la musique : vous révélez vos goûts

Vous n'avez pas forcément envie que vos collègues soient au courant de tous vos goûts musicaux... Il y a des péchés mignons que l'on préfère garder pour soi. Oubliez, ce n'est plus possible. Sur l'iTunes Store d'Apple, Google Play ou Amazon, Deezer ou Spotify, tout ce que vous écoutez est analysé par ces services. La preuve : vous venez de regarder un clip sur YouTube, de retour sur Play Musique, comme par hasard, on vous propose de télécharger l'album complet. ITunes n'est pas plus discret : il va vous faire des offres basées sur l'analyse de votre bibliothèque de fichiers MP3 personnelle.

Le cas de Deezer, Spotify et plus généralement des services de streaming sur ordi, tablette ou mobile est un peu plus complexe. La plupart sont interconnectés à Facebook, et cela dès l'inscription au service. Cette fois, ce n'est plus seulement le fournisseur, mais tous vos "amis" au sens large qui savent ce que vous écoutez en temps réel. S'il vous prenait l'envie de désactiver cette fonction, les sites ne vous lâcheraient pas jusqu'à ce que vous l'activiez de nouveau.

Vous allumez votre mobile : vous êtes pisté

En Allemagne, Malte Spitz, un responsable des Verts, a poursuivi son opérateur téléphonique en justice pour obtenir les données récoltées grâce à son portable. Et lorsque la justice lui a donné raison, il a découvert qu'il avait été géolocalisé 35 800 fois en six mois. On observerait le même résultat en France, car un portable allumé signale sans cesse sa position à son opérateur télécom, via les antennes relais. C'est la condition indispensable pour que l'opérateur puisse faire suivre les appels ou SMS à l'abonné. Mais l'opérateur n'enregistre pas seulement votre position. À des fins de facturation, il mémorise chaque appel, avec le numéro de téléphone, l'heure et sa durée, pendant deux ans. Idem pour les SMS et les MMS. Et cette fois, les données ne sont pas anonymes. Vous êtes identifié par un numéro unique, attribué à votre téléphone et qui figure dans une base de données nationale. Cela permet de localiser votre mobile en cas de perte ou de vol. Et même un téléphone éteint ou avec la batterie à plat peut être "interrogé" à distance. Si, en plus, vous utilisez un smartphone et que vous avez activé la localisation, dans le but de le protéger du vol par exemple, il va transmettre sa position à intervalles réguliers à l'éditeur du système : Microsoft, Apple ou Google.

Vous utilisez une appli mobile, elle vole vos contacts

Avant d'installer une appli, prenez le temps de lire sa description, et vous découvrirez que nombre d'entre elles sont extrêmement curieuses et n'hésitent pas à accéder à vos informations personnelles. La Cnil, en partenariat avec l'Inria, a mené l'enquête pendant un an, sur des iPhone. Elle a scruté l'activité des applis installées, et a prévu de le faire avec des smartphones Android prochainement. Elle a constaté que les applications accédaient à des données dont elles n'ont que faire a priori. 50 % des applis ont récupéré l'identifiant unique du téléphone et 17 % l'ont renvoyé à l'éditeur. Et la Cnil montre que près du tiers enregistrait la géolocalisation et 8 % accédaient au carnet d'adresses. En 2009, une entreprise suisse a vu l'une de ses applications retirées de l'App Store parce qu'elle débouchait sur un démarchage téléphonique de ceux qui avaient acheté l'appli. Depuis, Apple a introduit des contrôles du côté de l'utilisateur pour réduire ce genre de désagrément : l'accès au carnet d'adresses ou aux photos peut être contrôlé pour chaque appli. Mais impossible de savoir à l'avance si une appli vous demandera ces accès. Sur ce point, si Apple offre le plus de contrôle, Google est le plus transparent. Sur son Play Store, les autorisations que s'octroient les applis sont très détaillées. À l'inverse, Microsoft fournit très peu d'infos sur ce sujet, sur son Marketplace. Et le système ne donne aucun contrôle à l'utilisateur.

Vous payez un jeu, une appli... vous prenez de gros risques

Si vous craquez pour un jeu payant pour votre console, redoublez de vigilance avant de fournir vos informations personnelles, en particulier vos coordonnées bancaires. Une fois qu'elles sont mémorisées, c'est pour la vie. Pratique, mais parfois fatal, comme ont pu le constater les utilisateurs du réseau PlayStation. En avril 2011, les serveurs de Sony ont été piratés et les informations de 77 millions de comptes dérobées. Les pirates mettaient la main sur une mine d'or : les noms, adresses, dates de naissance, mots de passe et coordonnées bancaires, avec dates d'expiration. Résultat : les numéros de cartes de certaines victimes ont été mis en vente sur des réseaux mafieux. C'est le dernier plus gros piratage en date, les joueurs en tremblent encore. La firme japonaise, de son côté, a écopé d'une amende de 250 000 £ par la Cnil anglaise, pour défaut de protection des données personnelles. Deux ans après, l'affaire n'est toujours pas close.

Sur les magasins d'applications, ce n'est guère plus rassurant. Chacun d'entre eux enregistre la ●●●

"Facebook récolte plus de données que ne le faisait la Stasi"

C'est le combat de David contre Goliath. Max Schrems, un simple citoyen autrichien, tient la dragée haute à la multinationale Facebook depuis près de deux ans. Cité en exemple par la commissaire européenne à la Justice Viviane Reding, cet étudiant en droit âgé de 25 ans est devenu le champion européen de la protection des données personnelles. "Au début de cette histoire, je ne voulais pas voir mon nom ni ma photo dans les journaux mais les médias avaient besoin d'un visage", nous a confié, sourire en coin, Max Schrems. Il a déposé 22 plaintes contre Facebook auprès de la Cnil irlandaise.

Tout a commencé par une simple requête. En 2011, Max Schrems réclame l'historique de son profil à Facebook. Après plusieurs relances, il obtient un CD contenant un PDF de 1 222 pages envoyé par la poste. Là, il y découvre de vieilles discussions, d'anciennes photos et des commentaires qu'il avait pourtant supprimés. Des informations qui ont donc été archivées par Facebook contre son gré et en totale infraction avec le droit. "Facebook récolte davantage de données que ne le faisait la Stasi", s'emporte l'étudiant.

Max Schrems est parti en guerre contre Facebook. Ici, les 1 222 pages de données que le réseau social avait stockées sur lui.

Le siège européen de Facebook se trouvant à Dublin, Max porte l'affaire devant le préposé irlandais à la protection des données personnelles. Dans la foulée, il met en ligne le site "Europe versus Facebook" où il dévoile son dossier. Contre toute attente, Facebook délègue un porte-parole en Autriche pour rencontrer le plaignant. Et modifie ses règles de confidentialité : la fonction "supprimer" est ainsi rebaptisée "masquer". Le prochain combat de Max Schrems ? Se retourner contre la Cnil irlandaise pour "laxisme" envers Facebook. Le petit autrichien a lancé un appel à contributions sur son site dans ce sens. "Pour le moment, nous avons récolté 40 000 euros. C'est un bon début, mais il nous faudrait de 100 000 à 300 000 euros pour entamer une procédure", prévoit-il. Une bataille qui n'est pas gagnée d'avance...

FRANÇOIS DARMIGNY POUR 01NET ; COURTESY MAX SCHREMS

Vous cherchez un nouvel ami, et c'est tout votre carnet d'adresses qui est aspiré !

liste complète de celles que vous avez téléchargées, avec leur prix et la date d'achat. Rien d'étonnant. Mais pourquoi enregistrer tous les avis que vous laissez au sujet d'une application ? Pour ceux qui ne l'ont jamais fait, sachez qu'avant de laisser un avis sur iTunes ou le Play Store, il est nécessaire de s'identifier : vos opinions sont donc toutes accompagnées de votre nom. En cliquant sur votre nom, on peut alors remonter à tous vos autres commentaires sur iTunes. Chez Apple, cela s'arrête là. Mais chez Google, un clic sur votre identifiant et votre profil Google+ s'affichera aussi. Votre photo, vos informations publiques y sont librement consultables. Quand on est chez Google, on n'y est pas qu'à moitié.

Vous achetez chez un cybermarchand : il ne vous quitte plus

Avez-vous déjà eu l'impression, après une visite sur un site marchand, comme Priceminister ou Conforama, d'être suivi de site en site ? Ce n'est pas qu'une impression, c'est le tracking publicitaire. Lors de votre visite, un fichier (cookie) indiquant votre intérêt pour un certain type de produits a été enregistré sur votre ordinateur. Ce cookie est lié à une régie publicitaire. Si vous passez ensuite sur un autre site utilisant les services de cette régie, il va interroger le cookie pour vous proposer des produits analogues issus de son catalogue. Le roi en la matière est Amazon. Dès votre compte créé, vos gestes sont observés. Toutes les pages que vous consultez sont enregistrées. Un historique lié à votre compte, qui permet à Amazon de croiser vos données de navigation avec les notes que vous avez pu attribuer à des articles, et les comparer avec ce que d'autres clients ont acheté. Lorsque Amazon s'aperçoit que vous partagez des centres d'intérêt avec d'autres clients, le cybermarchand s'autorise à communiquer vos goûts et vice versa, il vous suggère d'acheter, chez lui mais aussi chez ses partenaires commerciaux. Aucune donnée nominative n'est transmise, mais cela n'empêche pas Amazon de s'en servir. Vous consultez à l'abri des regards la dernière production en DVD de Marc Dorcel, et bing ! vous recevez une promotion sur la collection complète dans la boîte mail familiale.

Vous publiez sur Twitter : il fouille votre carnet d'adresses

Twitter, et ses 500 millions d'utilisateurs, fait commerce de certaines de vos informations. Par exemple, pour vous proposer des publicités ciblées. Si vous suivez par simple curiosité un type un peu dingue, qui tient des discours extrêmes, ne vous étonnez pas de voir débarquer des pubs louches sur votre timeline. Et si vous voulez vous faire de nouveaux amis, d'autres surprises vous attendent. Gentiment, Twitter vous proposera son aide : cliquez sur "Trouver des amis", et là, au secours, il commencera par balayer votre propre carnet d'adresses, identifiant les noms, numéros de mobiles et adresses mail qu'il connaît déjà.

Une pratique généralisée dans les réseaux sociaux. Mais chez Twitter, on pousse l'exercice jusqu'à conserver pendant dix-huit mois les adresses mails et les numéros de téléphone de tous vos contacts. Le réseau social se justifie en expliquant que cela lui permettra de vous prévenir si l'un de vos amis ouvre un jour un compte. Raté, si votre ami voulait rester discret. Raté aussi si vous refusez de dévoiler votre numéro de mobile... une de vos connaissances s'en chargera certainement pour vous. ■

Vous regardez une vidéo, tout le monde le sait

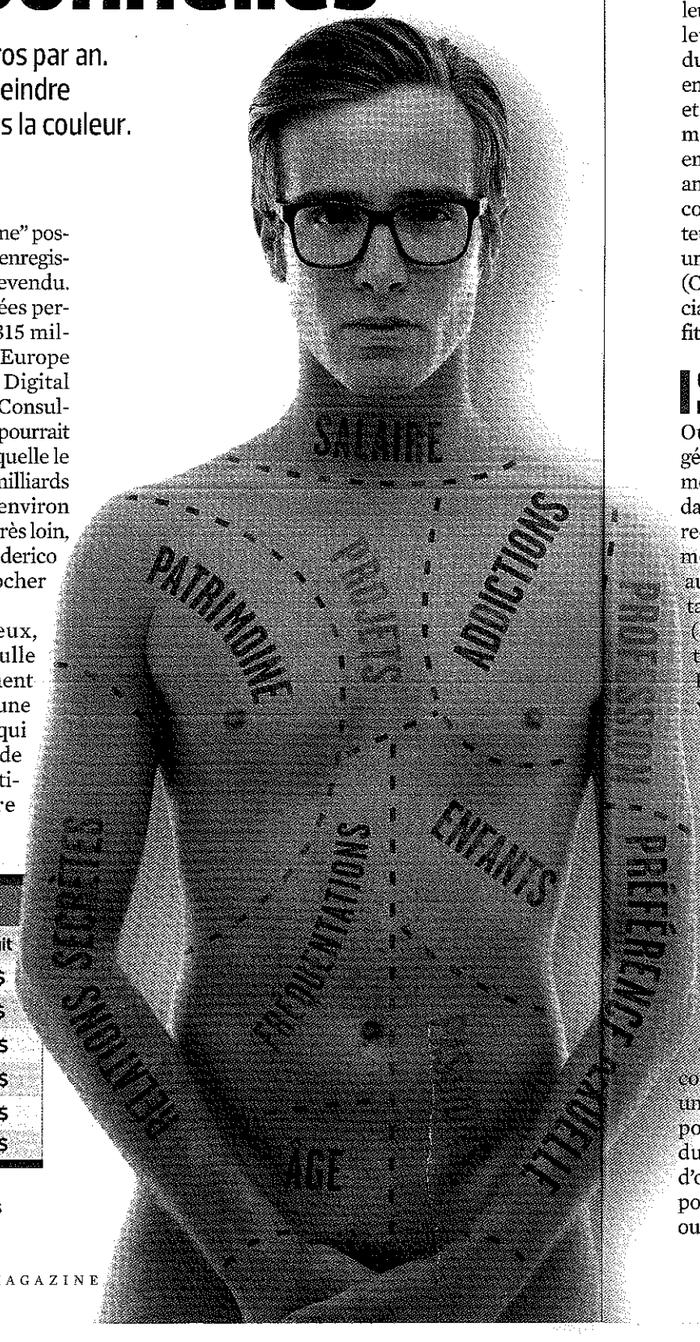
Les vidéos que vous regardez, celles que vous aimez, les chaînes auxquelles vous vous abonnez, les pubs sur lesquelles vous cliquez : YouTube associe toute votre activité à votre compte Google, qui les partage avec les éditeurs des vidéos et avec les régies publicitaires. Par défaut, votre compte YouTube se retrouve connecté à votre réseau social. Autrement dit, tous vos contacts sur Google+ peuvent voir les vidéos que vous avez aimées ou partagées sur YouTube. Si vos comptes Twitter et Facebook sont reliés à votre Gmail, vous pouvez alerter vos amis de ce que vous faites sur YouTube. Mais là, c'est vous qui décidez. Alors que sur Dailymotion, c'est lui qui décide. Sur sa page consacrée aux données personnelles, il précise que "les pages visitées, le type de navigateur utilisé, l'heure et la date de navigation, les publicités sur lesquelles vous cliquez" sont notamment mémorisés. La connexion avec Facebook se fait toute seule : pendant que vous regardez un film, vos amis sont instantanément au courant. Plus globalement, tous les sites de vidéo en streaming, y compris les WebTV et les sites de rattrapage des chaînes de télévision, sont les nouveaux eldorados des publicitaires. Ils permettent un ciblage très pointu des annonces, et ces dernières ne sont pas de simples bandeaux de texte mais de vrais spots de pub télévisuels, des bandes-annonces de films ou encore des clips promotionnels d'artistes internationaux, bien plus rémunérateurs.

Il suffit que vous ayez consulté votre compte Gmail pour que Google vous reconnaisse automatiquement sur tous ses services.

GOOGLE, FACEBOOK, AMAZON, APPLE...

Ce qu'ils font de vos données personnelles

Le saviez-vous ? Vos informations valent 2 000 euros par an. Un business florissant qui, d'ici sept ans, devrait atteindre 1 000 milliards d'euros. Mais dont vous ne verrez pas la couleur.



Federico Zannier est un sacré farceur. Depuis le 6 mai, cet habitant de Brooklyn vend à qui veut ses données numériques personnelles sur Kickstarter. Des informations personnelles qui, en deux semaines, lui ont déjà rapporté plus de 1 800 dollars. "L'an dernier, explique-t-il, le chiffre d'affaires de la publicité sur Internet s'est élevé à 30 milliards de dollars aux États-Unis. Moi, en 2012, je n'ai gagné aucun dollar avec mes propres données. En les trackant et en les vendant moi-même, j'essaie de récupérer quelques dollars". À ce jour, la démarche a séduit plus de 160 internautes. En déboursant 2 dollars, n'importe qui peut ainsi accéder à une journée de sa vie numérique : listing détaillé de 70 sites Web visités, 500 captures d'écran, images de lieux visités immortalisés par sa webcam, suivi de ses déplacements via GPS... Et pour 200 dollars, Federico propose à qui s'y intéresserait plus de 50 000 fichiers divers ainsi que des applications dédiées à l'autotracking. "Si tout le monde m'imitait, peut-être que les marchands du Web nous rémunéreraient directement", conclut-il.

Une boutade pas si farfelue. Par sa démarche, Federico rappelle que nos données personnelles valent beaucoup d'argent. Notre identité, nos coordonnées, les sites sur lesquels nous surfons, les photos que nous publions, les SMS que nous envoyons et jusqu'aux "J'aime" postés sur Facebook... Tout est enregistré, trié, commercialisé, revendu. La valeur totale des données personnelles est estimée à 315 milliards d'euros, rien qu'en Europe (selon The Value of Our Digital Identity, étude du Boston Consulting Group de 2012). Et elle pourrait tripler d'ici 2020, date à laquelle le business atteindrait 1 000 milliards d'euros. Soit 2 000 euros environ par habitant et par an. Pas très loin, curieusement, de ce que Federico Zannier s'apprête à empocher dans son coin.

Ces chiffres faramineux, le grand public n'en a nulle conscience. "30 % seulement des consommateurs ont une idée à peu près claire de qui collecte leurs données et de la façon dont elles sont utilisées", souligne encore l'enquête. Frédéric Fréry, professeur de Stratégie à ESCP-Europe, en décrit le mécanisme : "Deux modèles économiques coexistent chez les géants du Net. Le premier s'appuie sur l'e-commerce. Les sites marchands (Amazon ou Apple via iTunes) collectent des informations leur servant à cibler les clients pour leur proposer de nouveaux produits. Le second modèle repose entièrement sur la publicité. Google et Facebook ne vivent que de cette manne. Les internautes sont suivis en permanence afin de vendre aux annonceurs les publicités censées correspondre au profil des utilisateurs". Et entre ces deux modèles, une kyrielle de plus petits acteurs (Critéo, Experian, Weborama), spécialistes des bases de données, profite également du business.

COMBIEN VOUS VALEZ

Type d'informations	Valeur
Age, sexe, ville	Gratuit
Statut marital	0,01 $
Présence d'un enfant	0,01 $
Niveau d'études	0,02 $
Possesseur de smartphone	0,03 $
Centres d'intérêts	0,03 $
Pack de données persos	0,05 $

Avec des centaines de millions de profils, il n'y a pas de petits profits (source : Forbes).

Ces entreprises partagent-elles nos infos avec d'autres ?

Oui... mais pas en totalité. Les géants du Web conservent jalousement les données brutes ou "first data" : requêtes dans un moteur de recherche, commentaires postés, messages envoyés... Elles sont au cœur de leur business, d'autant que, plus elles progressent (50 % par an), plus les informations vous concernant s'affinent. En revanche, après avoir masqué votre identité réelle (nom, âge, adresse...), les entreprises revendent votre profil "anonymisé".

Mais cette mainmise sur les données va encore plus loin. Dès lors que vous utilisez un service, vous permettez à l'entreprise de disposer comme bon lui semble de vos contenus. Ainsi, Google explique-t-il, dans les conditions d'utilisation de sa messagerie Gmail (400 millions d'inscrits) qu'en soumettant des contenus à ses services, "l'utilisateur (lui) accorde sur ses contenus (messages + pièce jointe) une licence dans le monde entier pour leur utilisation (...), reproduction, modification, création d'œuvres dérivées". Même chose pour Dropbox, Twitter, Facebook ou encore Yahoo! qui prévient que, pour améliorer ses services, vos mails sont scannés pour "identifier des éléments clés de signification".

Où stockent-ils ces données qui valent de l'or ?

Dans des bâtiments appelés data centers ou fermes de données. Ces "fermes" sont en réalité de grands hangars climatisés, hautement sécurisés et fonctionnant 365 jours par an. Ils abritent des milliers de serveurs capables d'absorber l'inflation des données provenant du boom des réseaux sociaux, de l'augmentation des transactions en ligne, de la multiplication des objets connectés et du succès des sites de streaming tels Deezer, Spotify ou Netflix. Google dispose de treize entrepôts dans le monde : six en Amérique du Nord, un au Chili, trois en Asie et trois en Europe occidentale (Finlande, Irlande, Belgique). Facebook, lui, possède trois data centers dont deux situés aux États-Unis : un dans l'Oregon et un en Caroline du Nord. Il vient d'ouvrir le troisième au Nord de la Suède, près du cercle polaire. Un quatrième verra le jour en 2014 toujours outre-Atlantique, dans l'Iowa.

FRANÇOIS DARMIGNY POUR 01NET ; AMANDA ROHDE/ISTOCKPHOTO

La reconnaissance faciale, déjà active sur Picasa, pourrait bientôt servir à établir des profils publicitaires plus précis.

Pendant combien de temps sont conservées ces données ?

"Aussi longtemps que nécessaire" et en général, "jusqu'à la suppression de votre compte" est-il précisé chez Facebook. Quant à Google, il garde toutes vos données des six derniers mois. Pourquoi un semestre ? "Pour faire de la publicité ciblée, il est nécessaire que la donnée soit récente. En six mois, la situation des consommateurs et leurs besoins peuvent changer du tout au tout", insiste Alexandra Pelissero, porte-parole de Critéo. Cet acteur français de l'analyse de données possède sept data centers : en Europe, en Asie et en Amérique.

À qui vendent-ils leurs collectes ?

Officiellement... à personne. Sauf à des "partenaires de confiance", ce qui reste bien vague. S'ils ne commercialisent pas votre identité réelle, les géants du Net constituent en revanche des profils permettant de cibler les internautes en fonction de leurs activités numériques (historique et fréquence des sites consultés, participation à des forums, achats, etc.). Ce sont ces profils qui servent à faire des recommandations et sont revendus à des tiers. Par exemple, la liste des entreprises avec qui Apple se réserve le droit de partager sa récolte d'infos recouvre un vaste champ d'activités. Des prestataires œuvrant dans les domaines suivants : "traitement de l'information, extension de crédit, exécution de commandes, livraison de produits, gestion et développement des données clients, fourniture de services clients, enquêtes satisfaction et développement de clientèle" (conditions d'utilisateurs du site, consulté le 16 mai). Facebook fait "remonter" les données de ses utilisateurs à des entreprises via Facebook Connect. La mécanique, dévoilée par un acteur du secteur, est simple : "Un annonceur paie pour diffuser une bannière sur Facebook. Chaque fois qu'un des membres du réseau (1,1 milliard de personnes dans le monde ; 26 millions en France) clique dessus, ses données Facebook (profil, journal, activités) sont transmises à l'annonceur". Et si l'identité de l'internaute a été effacée, l'annonceur n'ignore toutefois plus rien de ses pré- ●●●

férences, goûts et sociostyles : "fan de jazz", "jeune parent", "ayant l'intention d'acheter une voiture"... Des profils convoités par les publicitaires, Facebook en compte ainsi plusieurs dizaines. Et puisque la connaissance des consommateurs est telle, pourquoi ne pas l'affiner même lorsqu'ils ne pratiquent aucune activité numérique ?

Peut-on continuer de suivre un consommateur... hors ligne ?

Oui. Les tests, réalisés pour l'instant aux États-Unis, semblent concluants. Comment ? En nouant des partenariats avec des spécialistes de la data qui gèrent les programmes de fidélité de la grande distribution. En croisant les "vraies" données personnelles (noms, adresses, dates de naissance...) – celles de Facebook avec celles d'une chaîne d'hypermarchés, par exemple –, l'annonceur peut comparer les centres d'intérêts qu'un type d'utilisateur déclarait sur le réseau avec ses achats et dépenses dans la vraie vie. "Cette juxtaposition est idéale pour délivrer le message publicitaire le plus efficace et le plus ciblé possible", reconnaît Stéphane Baranzelli, directeur France d'Experian.

Facebook est ainsi fortement soupçonné de délivrer à ses clients les données personnelles de ses utilisateurs. Un chercheur parisien raconte une anecdote étonnante. En visite chez un fabricant d'électroniques, il a constaté que la cellule en charge de l'e-réputation de l'entreprise pouvait contacter directement les internautes mécontents de ses produits sur Facebook. "Elle a donc accès à des informations que les consommateurs estimaient confidentielles, comme leur identité ou leur mail", souligne-t-il.

Comment sont exploitées ces infos confidentielles ?

À partir de ces données analysées et modélisées, il est possible de faire de la prédiction et de la recommandation. Ainsi, lorsque vous préparez vos vacances, vous surfez sur des sites de réservation d'hôtels, de ventes de billets d'avion, de train... Chaque fois que vous tapez l'un de ces mots-clés dans Google, le moteur de recherche envoie sur votre page de résultats, une pub en rapport avec votre requête censée vous intéresser, sous la forme de bannière ou de lien sponsorisé. Ces formats sont facturés à l'affichage ou au clic et valent de 2 à 7 euros au CPM (coût pour mille bannières diffusées) ou quelques dizaines de centimes d'euros au clic.

Sur Facebook également, il existe des posts ou des statuts "sponsorisés". Signalées comme tel, ces publicités semblent efficaces : "Une campagne de promotion organisée pendant trois jours par la marque Le Slip Français auprès de ses 13 350 fans lui a coûté 150 euros. Elle aurait rapporté 1 500 euros de chiffre d'affaires", indique-t-on chez le premier des réseaux sociaux.

Voilà pour les méthodes classiques. Mais aujourd'hui, les cibles (c'est-à-dire vous) sont vivantes. Elles comparent, hésitent, renoncent, etc. La gestion des données sert donc à les suivre à la trace. C'est ce que les spécialistes du marketing appellent le "re-targeting" (ou "re-marketing"). Vous cliquez sur un lien sponsorisé dans votre moteur de recherche, visitez le site d'un annonceur, mais décidez de le quitter sans effectuer d'achat. Les spécialistes de la pub (Google et Facebook notamment) peuvent vous retrouver. Votre première visite a généré l'envoi d'un cookie (un mouchard) dans votre ordinateur. Le publicitaire active alors son réseau de sites partenaires. Google en compte des dizaines de milliers dans le monde, Critéo 5 000 environ. Dès que vous surfez sur l'un de ces sites, votre cookie est reconnu et Google (par exemple) diffuse instantanément dans la page affichée, une seconde pub du même annonceur. Et ainsi de suite jusqu'à ce que vous cliquiez sur sa bannière.

"Voilà pourquoi lorsque vous vous renseignez sur Internet pour un appareil photo, les jours suivants, vous ne voyez que de la publicité pour des marques photographiques, indique Guillaume de la Fléchère, directeur général de Néo@ogilvy, l'agence média d'Ogilvy. Tant que vous ne cliquez pas dessus, vous restez une cible". Si, en revanche, vous effectuez ce simple geste, vous rapportez entre 10 et 20 euros à Google. Le marketing ciblé se facture plus cher que lorsqu'il est classique.

Les applications imaginées à partir de cette profusion de données vont se montrer encore plus malignes qu'actuellement. Et effectuer un ciblage encore plus fin. "Il va y avoir davantage d'informations sélectionnées selon votre activité du moment et mises en avant sur vos terminaux mobiles, tablettes, téléphones ou autres", assure Jérôme Colin, consultant au cabinet d'analyse Roland Berger.

Et demain, à quoi devons-nous nous attendre ?

Apple (avec l'appli Siri) et Google (avec Google Now!) font déjà de l'hyper-contextualisation : à partir de la position géographique d'une personne et de l'analyse de son activité sur Internet, ils savent ce qu'elle fait (courses, balade, restaurant...), et peuvent lui envoyer les bonnes informations sur son mobile. Rien ne les empêche donc de cibler la publicité sur son smartphone en fonction des enseignes qui l'entourent : "Après le dîner, tel bar, à 50 mètres, vous propose deux cocktails pour le prix d'un".

La reconnaissance faciale devrait, elle aussi, se développer. L'appli Scene Tap est déjà capable de calculer l'ambiance régnant le samedi soir, dans les bars des villes d'Austin, de Chicago et d'Augusta, aux États-Unis. Elle calcule le taux de remplissage des établissements, puis reconstitue le genre des consommateurs et leur moyenne d'âge. Comment ? À partir de la base de données d'Intel comptant 500 000 visages de sexe, d'âge et d'origine ethnique différents.

Quant à Facebook, qui a racheté Face.com, elle aurait constitué, grâce aux milliards de photos à sa disposition, "le plus grand fichier anthropométrique jamais réalisé", prévient Franck Leroy dans son livre "Réseaux sociaux et compagnie". "Avec les lunettes Google annoncées pour 2014, et qui afficheront des informations contextuelles devant nos rétines, on pourra bientôt entendre "Pas la peine d'aller parler à ce type dans la rue, c'est un salaud", plaisante Yannick Delsahut, consultant high-tech au cabinet de formation Orsys. Mais est-ce vraiment drôle ? ■ SP

La Cnil peut s'appuyer sur un vrai arsenal juridique, mais les sanctions sont rares

Décembre 2012. Le réseau social de photos Instagram annonce une modification de ses conditions générales d'utilisation (GCU). Indignation de ses utilisateurs qui menacent de fermer leur compte. Cette fronde est l'arbre qui cache la forêt. Il est rare, en effet, que les géants du Web rencontrent des telles résistances : les internautes signent souvent les CGU les yeux fermés sans vérifier si leurs droits sont respectés.

La réglementation En France, c'est la directive européenne 95/46/CE de 1995 et la loi Informatique et libertés, modifiée en 2011, qui fixent le cadre juridique général. Surprise, rien ne s'oppose à la collecte et l'exploitation commerciale des données personnelles. Sous réserve que l'internaute en soit informé et qu'il ait exprimé son consentement à ce sujet dans les conditions générales. Mais cela ne suffit pas toujours. Notamment pour les données dites sensibles qui nécessitent un consentement express : "Pour les données bancaires, mails et numéros de téléphone. Mais aussi tout ce qui concerne les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, ou relatives à la vie sexuelle de celle-ci", précise Judicaël Phan, juriste à la Cnil. Et surtout, il est obligatoire de préciser l'identité d'un "responsable de traitement" auquel vous pouvez vous adresser en cas de problème. Les CGU doivent indiquer dans quel but vos données sont collectées et à qui elles vont être transmises. Enfin, l'internaute dispose impérativement d'un droit d'accès, de rectification et d'opposition. Concernant la durée de conservation de ces données, les choses sont plus complexes. "Elle dépend du type de données et de l'usage qui en est fait. Mais elle ne peut être illimitée", résume maître Barbry, avocat spécialisé dans les nouvelles technologies.

Le contrôle de la Cnil En théorie, un réseau social ne peut conserver votre profil plus de deux mois après sa suppression. Sauf que les sites sont tenus de garder pendant un an vos données d'identification (nom, prénom, adresse IP, mots de passe, pseudo) dans le cas où la justice les réclamerait. La Cnil est chargée en France de contrôler le respect de ce cadre légal et de sanctionner les infractions. En 2012, le nombre de plaintes de particuliers a bondi de 40 %. "Nous en avons enregistré plus d'un millier", confirme Judicaël Phan. Mais, avertissements ou amendes, les pénalités de la Cnil sont rares et mesurées. En 2012, treize sanctions ont été prononcées. Comme cet avertissement contre le site de la Fnac pour "défaut du recueil du consentement des personnes et non respect d'une durée de conservation" concernant leurs données bancaires.

Peu de sanctions Le G29, le groupe des Cnil européennes, a aussi chargé l'autorité française d'enclencher une procédure à l'encontre de Google dont les règles de confidentialités ne seraient pas conformes à la loi. Du simple patronyme au numéro de carte bancaire, Google stocke et croise en effet une multitude d'informations sur ses utilisateurs. Première infraction, les internautes ne sont pas assez informés sur le traitement de leurs données personnelles. En outre, "Google ne permet pas le contrôle par les utilisateurs de la combinaison de données entre ses nombreux services", accuse la Cnil. Enfin, la durée de conservation de ces données n'est pas limitée. Un dossier chargé contre Google, mais les sanctions ne tombent pas.

Google en ligne de mire En octobre dernier, la Cnil avait posé un ultimatum à la société de Larry Page. À charge pour elle de se mettre en conformité dans les quatre mois. Mais Google joue la montre et refuse d'obtempérer. "Notre politique de confidentialité respecte la loi européenne et nous permet d'offrir des services plus simples et efficaces. Nous nous sommes pleinement impliqués tout au long des échanges avec la Cnil", se défend-on au siège français. Les représentants du groupe ont été reçus une dernière fois à Paris le 19 mars. "À l'issue de cette réunion, aucun changement n'a été mis en œuvre", souligne la Cnil. On attendait donc la phase de répression. Las ! Le G29 s'est contenté d'annoncer que "chaque autorité nationale allait poursuivre ses investigations au regard de son droit national"... En France, Google risque tout au plus 300 000 euros d'amende. AC

Isabelle Falque-Pierrotin, présidente de la Cnil, a Google en ligne de mire.

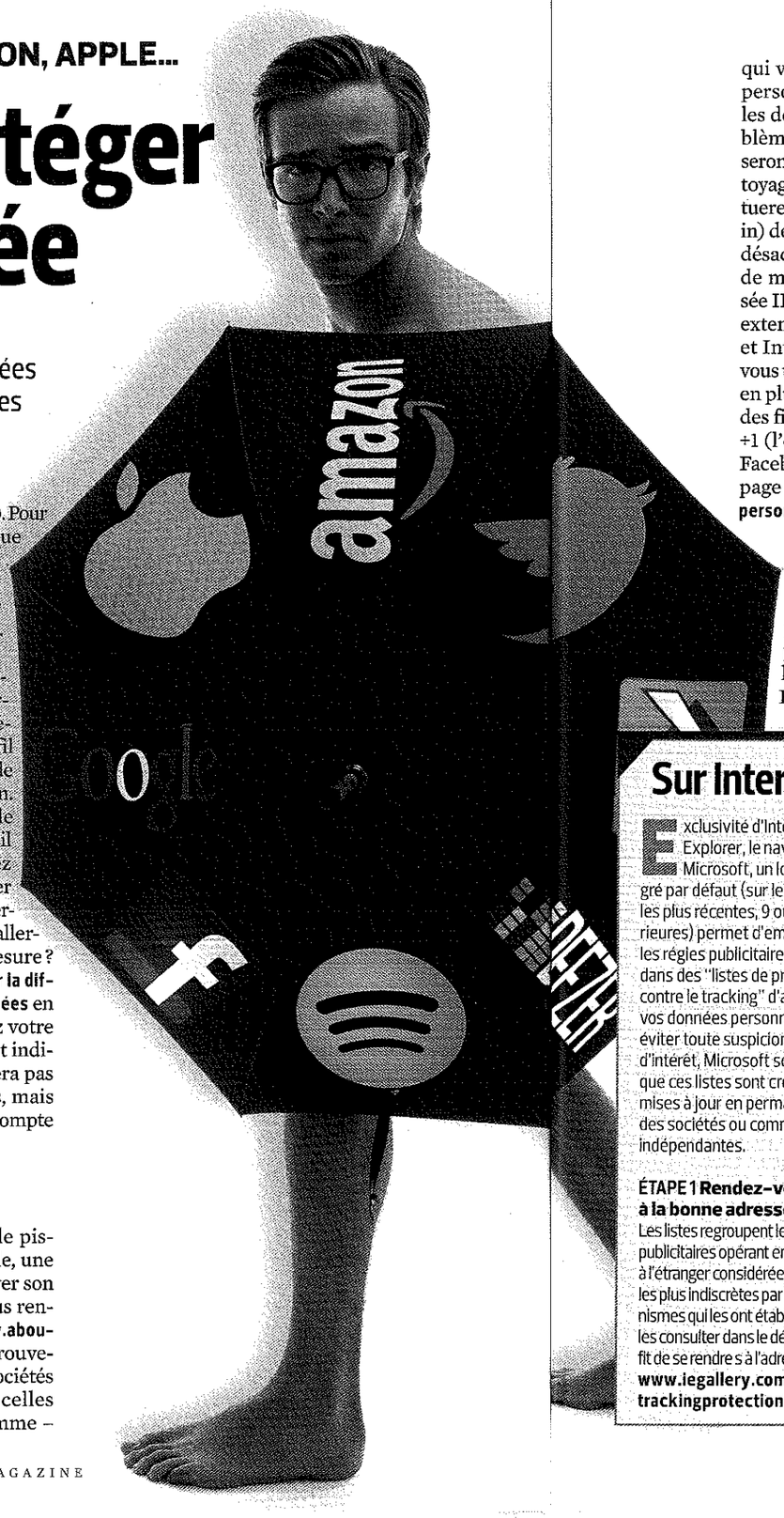
Immense data center de Google situé juste à la sortie d'Atlanta aux États-Unis.

COURTESY GOOGLE ; THIBAULT SAVARY/SIPA

GOOGLE, FACEBOOK, AMAZON, APPLE...

Comment protéger votre vie privée

Ne rêvez pas : il est malheureusement impossible d'échapper à 100 % au suivi et au stockage des données personnelles. Mais il existe des logiciels et des astuces pour en cacher une bonne partie. Revue de détail.



La protection de vos données personnelles sur Internet présente quelques inconvénients. En désactivant les fonctions de pistage des sites Web, vous vous priverez par la même occasion de certaines fonctionnalités auxquelles vous êtes habitué : recherches personnalisées, modules Facebook et autres formulaires préremplis. Si vous vous sentez prêt à ce petit sacrifice, vous trouverez dans ces pages quelques astuces et outils qui vous permettront de vous sentir un peu moins épié sur le Web. Sachez toutefois que ces protections ne sont jamais absolues : elles limitent les informations que vous transmettez aux régies publicitaires, mais n'empêchent pas leur enregistrement et leur stockage. Et méfiez-vous de certaines protections intégrées dans les navigateurs (l'option "navigations privée", par exemple), leur efficacité est toute relative : elles consistent à vous demander vos "préférences", mais rien n'oblige formellement les éditeurs de sites à les respecter (un peu comme l'autocollant "Pas de pub" sur votre boîte aux lettres).

Modifiez vos paramètres de préférences sur Google

C'est la première précaution à prendre. Connectez-vous à votre compte Google et consultez la synthèse des services que vous utilisez, appelée Dashboard (**https://www.google.com/dashboard/?hl=fr**). Pour connaître les informations que Google utilise pour personnaliser les pubs qui vous sont adressées, rendez-vous sur la page **https://www.google.com/settings/ads/onweb/**. Vous y trouverez divers renseignements vous concernant, certains étant directement extraits de votre profil Google+ et d'autres déduits de vos habitudes de navigation. Si vous trouvez que Google en sait trop sur vous (ou qu'il est mal renseigné), n'hésitez pas à supprimer ou modifier les informations vous concernant. Vous êtes carrément allergique à la publicité sur mesure ? Cliquez sur le lien **Désactiver la diffusion d'annonces personnalisées** en bas de page puis confirmez votre choix. Comme cela vous est indiqué, cette action ne bloquera pas les annonces publicitaires, mais celles-ci ne tiendront plus compte de votre profil.

Désactivez le cookie DoubleClick de Google

Pour réellement stopper le pistage publicitaire sur Google, une solution consiste à désactiver son cookie DoubleClick en vous rendant sur la page **http://www.aboutads.info/choices/**. Vous y trouverez une liste de toutes les sociétés publicitaires – du moins celles qui adhèrent à ce programme – qui vous envoient des annonces personnalisées, et vous pourrez les désactiver une à une. Le problème, c'est que ces préférences seront annulées dès le premier nettoyage de cookies que vous effectuerez. Mais une extension (plug-in) de votre navigateur permet de désactiver le cookie DoubleClick de manière permanente. Baptisée IBA sur Google Chrome, cette extension existe aussi sur Firefox et Internet Explorer. À noter : si vous utilisez Google+, vous pouvez en plus désactiver l'exploitation à des fins publicitaires des boutons +1 (l'équivalent des "J'aime" sur Facebook) en vous rendant sur la page **https://plus.google.com/+1/personalization?hl=fr**.

Faites passer un check-up à votre profil Facebook

Facebook n'est franchement pas le champion de la transparence en ce qui concerne les données personnelles. Entre la multitude de points à vérifier et les incessants changements de politique de confidentialité, Mark Zuckerberg lui-même y perdrait ses petits. Un bon logiciel valant mieux qu'un long discours, téléchargez PrivacyFix et rendez-vous sur la page **www.privacyfix.com/start**. Malgré une traduction partielle et parfois très approximative, l'interface vous permettra de vérifier un à un tous les points sensibles de votre profil, que ce soit au sein de Facebook ou dans les applications externes. Elle vous signalera notamment qui peut voir vos informations, si vos préférences sont utilisées pour la publicité ou encore si vos amis sont autorisés à vous identifier sur des photos. Un simple clic sur un point litigieux vous conduira sur la page Facebook correspondante, agrémentée d'infobulles vous indiquant comment remédier au problème. Difficile de faire plus simple ! PrivacyFix vous propose également de passer au scanner votre profil LinkedIn ainsi que quelques réglages de Google. Mieux encore : dans la section **Traçage**, vous trouverez une impressionnante liste des cookies publicitaires présents sur votre ordinateur. Après avoir supprimé ces mouchards, vous pourrez les interdire afin de prévenir toute "réinfection" lors de vos prochaines sessions de navigation.

Désactivez le pistage publicitaire sur Firefox

Dans la barre des menus, cliquez sur **Outils** puis sur **Options**. Sélectionnez ensuite l'onglet **Vie privée**, judicieusement illustré par un masque de loup, et cochez la case **Indiquer aux sites Web de ne pas me pister**. Si vous utilisez Firefox sous Mac OS X, vous trouverez la fenêtre des options en cliquant sur **Firefox** puis sur **Préférences**, ou en tapant le raccourci clavier **cmd,**. Vous remarquerez au passage la présence sous cet onglet **Vie privée** du lien **Supprimer des cookies spécifiques**. Le champ de recherche proposé s'avère

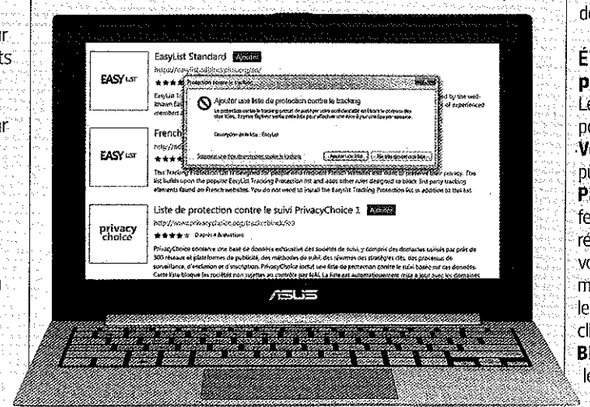
Sur Internet Explorer, barrez la route aux curieux indésirables

Exclusivité d'Internet Explorer, le navigateur de Microsoft, un logiciel intégré par défaut (sur les versions les plus récentes, 9 ou supérieures) permet d'empêcher les régies publicitaires figurant dans des "listes de protection contre le tracking" d'accéder à vos données personnelles. Pour éviter toute suspicion de conflits d'intérêt, Microsoft souligne que ces listes sont créées et mises à jour en permanence par des sociétés ou communautés indépendantes.

ÉTAPE 1 Rendez-vous à la bonne adresse
Les listes regroupent les régies publicitaires opérant en France ou à l'étranger considérées comme les plus indiscrètes par les organismes qui les ont établies. Pour les consulter dans le détail, il suffit de se rendre à l'adresse **www.iegallery.com/fr-fr/trackingprotectionlists**.

ÉTAPE 2 Sélectionnez une ou plusieurs listes
Cliquez sur le lien **Les plus populaires** pour choisir une ou plusieurs listes de filtrage. Vous remarquerez que certaines sont dédiées en particulier aux internautes français. Faites un simple clic sur l'un des boutons **Ajouter**, confirmez avec le bouton **Ajouter une liste** et le tour est joué.

ÉTAPE 3 Gérez vos listes
Par la suite, vous pourrez désactiver ou supprimer chacune de ces listes. Sur Internet Explorer 10, cliquez sur la roue crantée en haut à droite de la fenêtre, survolez la mention **Sécurité** avec le curseur puis cliquez sur **Protection contre le tracking**. Sélectionnez une liste pour afficher ses informations, la désactiver temporairement ou la supprimer définitivement.



Internet Explorer propose plusieurs listes de protection contre le pistage publicitaire. Vous n'avez plus qu'à choisir celles qui vous convient.

ÉTAPE 4 Créez une liste personnalisée
Les plus exigeants peuvent opter pour du sur-mesure. Sélectionnez **Votre liste personnalisée** puis cliquez sur le bouton **Paramètres**. Dans la nouvelle fenêtre, sélectionnez les régies publicitaires auxquelles vous voulez fermer la porte (les choix multiples sont possibles via les touches **Ctrl** ou **Shift**), cliquez sur **Autoriser** ou **Bloquer** puis validez avec le bouton **OK**. N'oubliez pas d'activer votre liste personnalisée via le bouton ad hoc avant de fermer la fenêtre.

FRANÇOIS DARMIGNY POUR 01NET ; COURTESY ASUS ; AMANDA RONDE/ISTOCKPHOTO

Plusieurs logiciels permettent de repérer les mouchards qui se sont glissés dans votre PC

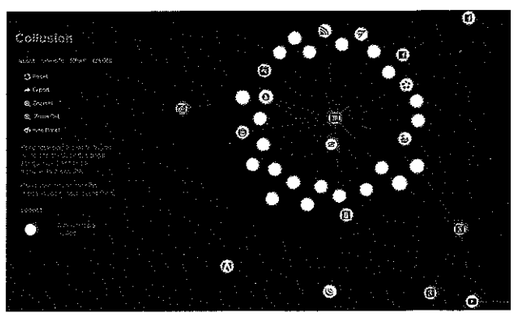
très pratique pour faire une recherche ciblée de ces mouchards publicitaires.

Activez les options de Safari sur votre Mac

Dans son menu **Préférences**, à l'onglet **Confidentialité**, le navigateur d'Apple propose un nettoyage en un seul clic de tous les cookies et autres données stockés par des sites Web extérieurs. Côté prévention, une option intéressante consiste à bloquer uniquement les cookies "des tierces parties et des annonceurs". Elle permet en effet d'interdire le tracking publicitaire tout en conservant les cookies – et les fonctions qui en dépendent –des sites que vous avez visités. En ce qui concerne les informations de localisation, l'option **Refuser sans confirmation** réglera définitivement la question.

Découvrez qui vous piste avec le plug-in Collusion de Firefox

L'extension logicielle Collusion pour Firefox n'a pas son pareil pour bien vous faire comprendre la problématique du pistage publicitaire. En temps réel, lors de vos sessions de navigation, elle est capable de dessiner un schéma très clair montrant comment vos données sont échangées entre les annonceurs et les sites sur lesquels vous vous rendez. Vous pouvez alors découvrir précisément quelles sociétés vous pistent sur chacune des pages visitées. En quelques clics, vous voyez se former des constellations qui font froid dans le dos. À visée uniquement informative, cette extension doit être complétée par outil de gestion et/ou de prévention pour éliminer les cookies (voir plus haut). **http://t.01net.com/tc118460**



Collusion vous montre graphiquement les sociétés qui suivent vos données personnelles.

Repérez les applis indiscrètes sur votre mobile avec Clueful

Mondialement connu grâce à son antivirus gratuit pour Windows, l'éditeur BitDefender vient de lancer une toute nouvelle application – la première du genre, à notre connaissance – destinée à contrôler les applis logées dans votre smartphone. Disponible gratuitement sur Android comme sur iOS, Clueful vous alerte sur les éventuels risques d'atteinte à votre vie privée en attribuant une note globale de confidentialité à votre appareil et en classant les applications selon leur niveau de risque. C'est donc davantage un outil d'information qu'un remède contre les intrusions dans vos données personnelles. Gratuit, il s'avère très pratique pour savoir, avant ou après l'installation d'une application, si celle-ci peut fouiner dans votre liste de contacts, lire et écrire sur votre carte SD ou envoyer des SMS à votre insu.

Désactivez sur votre mobile les pubs personnalisées

Les pubs ciblées grâce à l'exploitation des données personnelles peuvent facilement être supprimées ou limitées sur votre smartphone. Si votre appareil utilise Android, allez sur le Play Store (ex-Android Market), appuyez sur le bouton **Menu** et choisissez **Paramètres**. Déroulez la page jusqu'en bas pour faire apparaître la section **Préférences des annonces Google Admob** et décochez la case.

Si vous avez un iPhone sous iOS 6, rendez-vous dans **Paramètres**, **Informations**, **Général**, **Publicités** puis activez le bouton **Suivi publicitaire limité**. Cela veut dire qu'Apple continuera à vous envoyer des publicités ciblées sur votre profil personnel, mais que les éditeurs d'applis extérieurs ne pourront plus le faire. S'ils transgressent cette règle ils risquent d'être bannis de l'App Store.

Avec DoNotTrackMe, bloquez les mouchards publicitaires

L'extension DoNotTrackMe (ou DNTMe) présente l'avantage, pour les novices et les paresseux, de bloquer par défaut et en un seul clic beaucoup plus de mouchards publicitaires que les simples options des navigateurs. Libre à vous ensuite de donner des autorisations dans le panneau des Paramètres (clic sur l'icône dans la barre des modules, puis clic sur l'icône en forme d'engrenage). Disponible pour Firefox, Internet Explorer, Chrome et Safari, versions Windows et Mac OS.

Grâce à Ghostery, protégez-vous quand vous surfez

Ghostery est encore plus efficace que DoNotTrackMe pour la protection de la vie privée sur le Web. Déclinée en différentes versions pour les principaux navigateurs (Explorer, Firefox, Chrome, Safari Opera) cette extension logicielle permet d'être informé de la présence de mouchards en tous genres (pixels invisibles, widgets...) sur les pages Web que vous visitez avec votre ordinateur, et de connaître les sociétés indiscrètes qui les utilisent. Surtout, vous pouvez bloquer de manière permanente les cookies de votre choix, classés t par catégories (tracking publicitaire, statistiques d'audience, widgets...). Bien pratique, un système de "liste blanche" permet d'accorder un feu vert aux sites de confiance sur lesquels vous souhaitez profiter de toutes les fonctions. Une version mobile existe aussi pour l'iOS de l'iPhone.
http://t.01net.com/tc47949.html

Les parades à mettre en place sur un mobile Android (version 4.1.2)

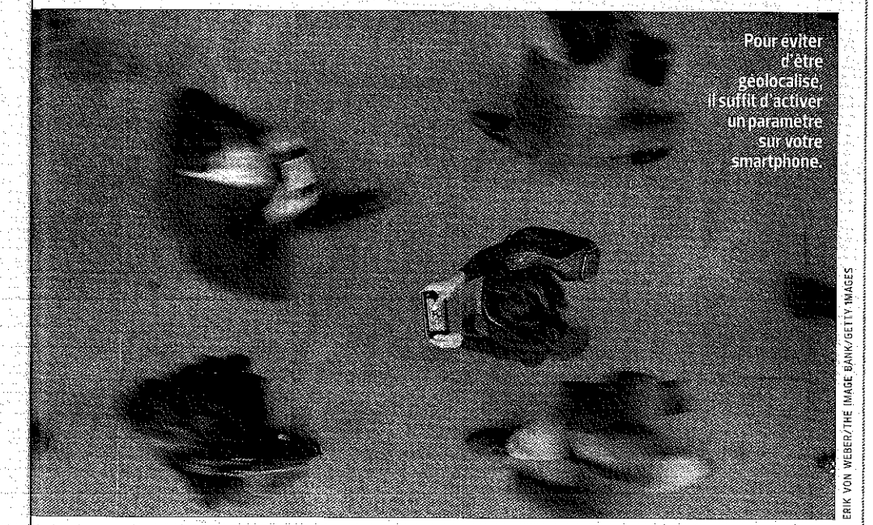
Le système Android pour smartphones et tablettes n'est pas moins risqué que les autres en matière de protection des données personnelles. Google a toutefois doté son navigateur Chrome d'options permettant de limiter les intrusions dans la vie privée des utilisateurs. Simples à mettre en place.

ÉTAPE 1 Désactivez complètement la localisation
Ouvrez les **Paramètres système** d'Android via la touche **Menu** et appuyez sur **Services de localisation**. Pour empêcher toute tentative de géolocalisation par une application ou un site Web, décochez les cases **Utiliser réseaux sans fil** et **Utiliser les satellites GPS**. Si vous ne souhaitez pas que vos résultats de recherche sur Google soient influencés par votre position géographique, décochez aussi la troisième option.

ÉTAPE 2 Nettoyez le navigateur Chrome
Lancez Chrome et appuyez sur la touche **Menu** de votre smartphone. Allez dans **Paramètres**, **Confidentialité** puis **Effacer données navigation**. Cochez les cases concernant l'historique, le cache, les cookies et les données de saisie automatique puis appuyez sur le bouton **Effacer**. Désormais, le navigateur ne sait (presque) plus rien de vous.

ÉTAPE 3 Fermer la porte aux mouchards
Une fois les cookies supprimés, reste à les empêcher de revenir. Toujours dans **Paramètres**, allez dans **Paramètres du contenu** et décochez la case **Accepter les cookies**. Les plus paranos iront jusqu'à bloquer l'exécution de codes JavaScript, au risque de se priver d'un certain nombre de fonctionnalités des sites Web.

ÉTAPE 4 Effacez les données stockées par les sites que vous avez visités
Rendez-vous maintenant dans la rubrique **Paramètres des sites Web** où vous voyez s'afficher une liste de certains sites que vous avez visités. Choisissez le site concerné et appuyez sur **Effacer les données stockées**. Vous récupérerez par la même occasion quelques mégaoctets sur votre espace de stockage. Si vous voulez filtrer individuellement la localisation par les sites Web, appuyez sur l'option **Accès à la position** lorsqu'elle est présentée. Dans ce cas, vous pouvez vous dispenser de la première étape de ce petit guide pratique.



Pour éviter d'être géolocalisé, il suffit d'activer un paramètre sur votre smartphone.

ERIK VON WEBER/THE IMAGE BANK/GETTY IMAGES

Téléchargez Better Privacy pour éliminer les cookies flash

Les LSO (Local Shared Objects, appelés cookies flash) conservent quelques données personnelles sur vous. Ils présentent la fâcheuse particularité de ne pas être concernés par les méthodes précédentes de suppression des cookies. Seule parade contre ces mouchards potentiels: l'extension Better Privacy, disponible pour Firefox uniquement. Petite astuce: dans les options, vous pouvez faire en sorte que les LSO soient inclus dans le menu **Supprimer l'historique récent**, ce qui vous évite une double manipulation lors de vos nettoyages de cookies.
http://t.01net.com/tc47282.html

Contrôlez la géolocalisation sur votre iPhone ou iPad

Si vous souhaitez désactiver complètement la géolocalisation sur l'iOS 6, qui équipe les mobiles d'Apple, rendez-vous dans **Réglages**, **Confidentialité**, **Service de localisation** et faites glisser le bouton. Sur iOS 5, l'option se trouve dans **Réglages**, **Service de localisation**. Cette fonction étant énergivore, l'opération vous permettra aussi d'économiser votre batterie. Cependant, sachez que votre iPhone reste susceptible d'être localisé malgré cette désactivation "pour faciliter l'arrivée des secours" en cas d'appel d'urgence, dixit Apple.

Utilisez le navigateur sécurisé SRWare Iron

Le navigateur Iron de l'éditeur SRWare se présente comme une version open source de Chrome sans ses fonctions intrusives. En clair, Iron ne transmet pas vos données personnelles à Google, ni a fortiori aux publicitaires. Le numéro d'identification de votre navigateur, notamment, reste confidentiel. Ce navigateur est pourtant aussi puissant que Chrome. Il offre les mêmes fonctionnalités, sauf celle qui consiste à fouiner dans vos données. Un logiciel libre récent et promis à un bel avenir!
http://t.01net.com/tc100058.html ■ JMM