Les CNIL européennes haussent le ton contre le pistage de Facebook

Les CNIL européennes haussent le ton contre le pistage de Facebook

Après une décision de la justice belge, d'autres pays européens réclament que Facebook cesse de traquer les internautes en dehors de ses pages.

Facebook n'est pas encore sorti du bourbier européen.

L'autorité française de protection des données (la CNIL) a publié lundi une déclaration commune avec quatre de ses homologues européens concernant les règles de confidentialité du réseau social.

Elle fait suite à une décision de la justice belge, qui a demandé à Facebook de ne plus tracer les internautes non-inscrits sur le site américain. L'entreprise a finalement obtempéré il y a une semaine, en empêchant toute personne sur le territoire belge déconnectée du site d'accéder à ses pages.

Pas encore suffisant pour les cinq CNIL des Pays-Bas, de la France, de l'Espagne, de Hambourg et de la Belgique, qui réclament la généralisation du dispositif. «Le groupe de contact attend de la société qu'elle se conforme à ce jugement sur tout le territoire de l'Union européenne», précise le communiqué.

Mesures de sécurité

En Belgique, la justice contestait l'utilisation par Facebook d'un «cookie», un micro-fichier qui conserve les données ou habitudes des internautes, baptisé «datr».

Principale critique: cette collecte concerne les personnes ne disposant pas de compte Facebook, et qui ne consentent donc pas à ce suivi. Il suffit de visiter une page du site (par exemple un évènement public) pour se voir déposer ce cookie sur son ordinateur et mobile. Facebook est ensuite capable de connaître les fréquentations en ligne de l'internaute, s'il se rend sur des sites contenant des modules du réseau social, comme le bouton «like».

De son côté, Facebook affirme qu'il collecte des cookies pour des raisons de sécurité. «Nous les utilisons afin de distinguer les véritables visites des fausses», expliquait la semaine dernière Alex Stamos, en charge de la sécurité chez Facebook. «Depuis cinq ans, ces cookies nous servent à empêcher la création de faux comptes, d'empêcher le vol de données ou l'organisation d'attaques par déni de service.» Facebook précise que ces cookies sont utilisés afin de surveiller le comportement d'un navigateur Web, et non d'un utilisateur précis. Pour Alex Stamos, «si le cookie nous informe qu'un navigateur a visité des centaines de sites en cinq minutes, cela nous indique qu'il s'agit probablement d'un robot».

Facebook a ajouté qu'il comptait faire appel de la décision de la justice belge et qu'il était prêt à discuter du sujet du cookie «datr» avec les autres autorités de protection des données.

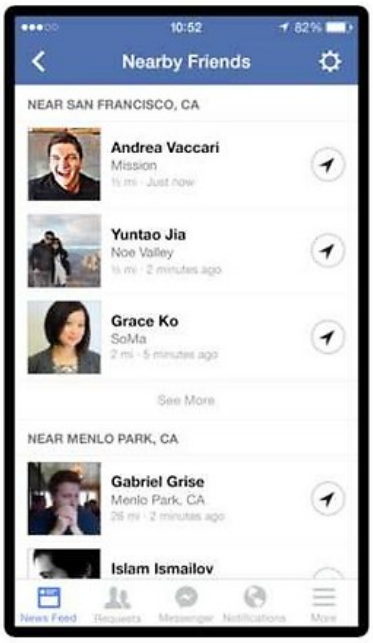
Le groupe des CNIL européennes dénonce lui une «ingérence dans la vie privée des internautes» qui «n'est pas acceptable». Il réclame à Facebook de «prendre les mesures nécessaires pour se mettre en conformité avec la législation européenne, et ce sur tout le territoire de l'Union européenne.»

Le groupe enquête depuis presque un an sur les règles de confidentialité de Facebook. Ces investigations sont menées par chacune des CNIL, mais coordonnées par le groupe de contact. Leurs conclusions ne devraient pas être rendues avant l'année prochaine.

Réagissez à cet article

Source : http://www.lefigaro.fr/secteur/high-tech/2015/12/07/32001-20151207ARTFIG00299-les-cnil-europeennes-haussent-le-ton-contre-le-pistage-de-facebook.php

Avec Facebook, on peut désormais savoir quand nos amis sont à proximité.. et lui aussi ! | Le Net Expert Informatique



Avec Facebook, on peut désormais savoir quand nos amis sont à proximité… et lui aussi !

Le réseau social propose ce mardi sur son application mobile une option baptisée « Nearby Friends » qui envoie une notification quand un ami se trouve à proximité.

Facebook veut savoir où nous sommes et souhaite également que nos amis le sachent. A partir de ce mardi, une nouvelle option apparaît sur le réseau social : « Nearby Friends », soit une bonne méthode pour scruter les activités de vos amis. L'application va ainsi envoyer une notification quand un ami de l'utilisateur se trouve à côté de lui.

Option désactivée par défaut

Les réseaux sociaux ne laissent donc plus de place aux mensonges. Impossible d'éviter un ami encombrant : « Lorsque vous allez au cinéma, 'Friends Nearby' vous dit si des amis à vous sont proches pour que vous alliez voir le film ensemble ou pour vous retrouver ensuite », indique Facebook.

Pour l'instant, il s'agit d'une option non-obligatoire, c'est à dire qu'elle est désactivée par défaut. En revanche, il est impossible de savoir à partir de combien de kilomètres Facebook considérera qu'un ami se trouve « à proximité ».

Avec cette option, le réseau social pourrait également franchir une nouvelle étape dans la collecte des données personnelles, alors que la nouvelle application débarque au lendemain d'une injonction de la justice belge . Cette dernière a ordonné Facebook d'arrêter de tracer tous les internautes, dont ceux qui ne sont pas connectés au réseau social.

Nouvelle tendance

La nouvelle option Facebook semble s'inscrire dans une nouvelle tendance. Il y a quelques jours, c'est Google qui annonçait le lancement d'une nouvelle application indiquant aux amis d'un utilisateur si celui-ci est disponible pour sortir manger, boire un verre, etc. Baptisée « Who's Down », l'option n'est disponible qu'aux Etats-Unis et constitue un premier test pour Google. Pour Facebook en revanche, cette phase a déjà été réalisée : l'option « Nearby Friends » a été l'ancée dès 2014 chez les anglo-saxons.

Facebook Messenger intègre la reconnaissance faciale

En Australie, le réseau social va encore plus loin en proposant une nouvelle application sur Facebook Messenger. Baptisée « Photo Magic », il s'agit d'un outil permettant de partager facilement des photos où apparaissent les personnes avec lesquelles on discute. Facebook utilise pour cela la reconnaissance faciale et scanne toutes les photos stockées sur le téléphone de l'utilisateur. Si un ami Facebook est détecté sur l'une des photos, l'application propose de la partager à la personne identifiée. Pour l'instant la fonctionnalité est optionnelle et ne devrait pas arriver tout de suite en France. Facebook a en effet cessé la reconnaissance faciale en Europe pour respecter la législation sur la protection des données personnelles.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lesechos.fr/tech-medias/hightech/021468123566-grace-a-facebook-on-peut-desormais-savoir-quand-nos-amis-sont-a-proximite-1174043.php

---

Invalidation du Safe Harbor – Un résumé pour mieux

comprendre l’initiative de Max Schrems | Le Net Expert Informatique

	Invalidation du Safe Harbor – Un résumé pour mieux comprendre l’initiative de Max Schrems

C’est en tant qu’utilisateur de Facebook « depuis 2008 » que ce citoyen (presque) ordinaire s’était adressé à l’équivalent de la Cnil en Irlande – où est implantée la filiale européenne du réseau social – pour s’opposer au transfert de ses propres données personnelles vers les serveurs américains de Facebook. La raison invoquée : les révélations de Snowden sur les pratiques de la NSA, justement, prouvaient que les Etats-Unis n’offraient pas les garanties suffisantes du respect de la vie privée.

Max Schrems, dont la croisade contre le réseau social avait débuté alors qu’il était encore étudiant, accuse entre autres Facebook Ireland Ltd., la base européenne de l’entreprise, d’enfreindre le droit européen sur l’utilisation des données, et de participer au programme de surveillance Prism de la NSA, l’Agence de sécurité nationale américaine.

Toutes les données sont conservées
Au cours de ses études de droit, Max Schrems avait pu accéder à une compilation de ses données personnelles, soit 1 222 pages qui répertorient toutes ses activités sur Facebook, y compris ce qu’il pensait avoir supprimé. Le Viennois avait accusé en août 2011 le réseau social de détention abusive de données personnelles, déposant un recours comportant 22 réclamations devant l’Autorité de protection de la vie privée en Irlande (DPC), où l’entreprise américaine a son siège social européen. La DPC avait donné raison à l’étudiant et demandé à Facebook de clarifier sa politique sur les données privées.

Octobre 1987 : Naissance de Maximilian Schrems

08/2011 : Recours comportant 22 réclamations devant l’Autorité de protection de la vie privée en Irlande (DPC), où l’entreprise américaine a son siège social européen. La DPC avait donné raison à l’étudiant et demandé à Facebook de clarifier sa politique sur les données privées.

01/08/2014 : Dépôt par Maximilian Schrems devant le tribunal de commerce de Vienne d’un recours collectif contre Facebook ayant réuni 25 000 plaignants demandant chacun 500 euros de dommages et intérêts en réparation de l’utilisation présumée illégale de leurs données personnelles.
L’initiative « Europe vs Facebook » dirigée par Max Schrems réclame que le plus grand réseau social au monde « se mette enfin en conformité avec le droit, en ce qui concerne la protection des données ».

01/07/2015 : Rejet de la plainte contre Facebook. La cour a estimé qu’elle était irrecevable dans la forme et s’est déclarée incompétente sur le fond.

06/10/2015 : Par décision de la Cour de Justice de l’Union Européenne du 06 Octobre 2015 (affaire C-362/14), le mécanisme d’adéquation » Safe Habor » permettant le transfert de données vers les entreprises adhérentes aux Etats-Unis a été invalidé.
En conséquence, il n’est désormais plus possible de réaliser un tel transfert sur la base du Safe Harbor.
La CNIL examine actuellement avec ses homologues au sein du G29 les conséquences juridiques et opérationnelles de cet arrêt. Des informations complémentaires seront mises en ligne très prochainement.
Accéder au jugement

La Cour européenne de justice pourrait-elle remettre en cause ce safe harbor ?
Tout est ouvert. La Cour peut limiter son jugement à la question préjudicielle posée ou lui donner une portée plus large, en se fondant sur l’article 8 de la Charte européenne des droits fondamentaux sur la protection des données à caractère personnel. L’avocat général Yves Bot est réputé pour appliquer le droit à la lettre, alors que le juge rapporteur, Thomas von Danwitz, est plutôt du côté des libertés civiles. Il est donc possible que la Cour ne suive pas l’avis de l’avocat général comme ça été le cas à propos de la rétention des données

Quelles pourraient être les solutions?
Il y a deux options. Dans un premier cas, les entreprises impliquées dans la surveillance de masse, Google, Microsoft, Facebook, Yahoo… ne pourraient plus transférer les données vers leurs data centers aux Etats-Unis, ce qui porterait un sérieux coup à leur business model. La question s’est déjà posée à propos de Swift, le système international de messagerie bancaire. La solution avait été de stocker les données européennes dans un data center en Suisse, ce qui les plaçaient hors de la juridiction américaine. Ce pourrait être une solution pour Microsoft et d’autres qui ont de toute façon déjà des centres en Europe, même s’il n’est pas facile à mettre en place techniquement.
Dans un second cas, les juges pourraient prendre en compte les autres mécanismes existants, en dehors du safe harbor, comme les clauses contractuelles dans lesquelles les entreprises s’engagent individuellement à respecter la législation européenne sur les données. C’est ce que fait EBay par exemple, qui n’est pas couvert par le safe harbor.

Quel serait l’impact pour les entreprises du net ?
Actuellement, les entreprises sont entre deux chaises : les autorités américaines exigent l’accès à toutes les données d’un côté et les Européens de l’autre, qui disent “non”. Elles suivent les exigences américaines parce que les conséquences juridiques d’un refus sont immédiates, alors que du côté européen, tout ce qu’elles risquent est un courrier…
A long terme, les entreprises ont intérêt à ce que cette question de juridiction soit résolue. Pour des raisons structurelles, elles tombent à la fois sous le coup de la législation américaine, parce que ce sont des entreprises américaines, et sous la juridiction irlandaise, indienne,… parce qu’elles y sont établies pour des raisons fiscales. Tout le monde a donc intérêt à ce que la Cour tranche.

Comme tout professionnel de l’informatique et de l’Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l’ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l’hygiène informatique.
Besoin d’informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Sources :
http://rue89.nouvelobs.com/2015/10/06/surveillance-max-schrems-heros-tres-discret-a-lombre-snowden-261526
http://www.lemonde.fr/pixels/article/2014/08/07/maximilian-schrems-le-but-est-de-faire-respecter-a-facebook-la-legislation-europeenne_4468090_4408996.html
http://www.usine-digitale.fr/article/rencontre-avec-le-juriste-qui-a-porte-plainte-contre-facebook-et-force-l-europe-a-trancher-sur-la-surveillance-de-masse.N351697

E-réputation : la diffamation sur Facebook punie comme ailleurs | Le Net Expert Informatique

La diffamation et les d'injures sur internet constituent un des axes de l'e-réputation. Un récent jugement du TGI de Béthune (16 septembre 2015) vient rappeler fort justement que le délit de diffamation s'applique sur Facebook dès lors que les propos constituant le délit sont consultables dans le ressort du tribunal, « en tout cas sur le territoire national ».

Des propos diffamatoires évidents

Une personne avait publié sur son compte Facebook des propos diffamatoires à l'encontre d'une discothèque de la région, c'est-à-dire alléguant des faits qui « portent atteinte à l'honneur et à la considération de la personne » (article 29 de la loi du 29 juillet 1881). En l'occurrence, la personne diffamée est la société propriétaire de la discothèque.

Il est aussi remarquable qu'aucune circonstance atténuante ou exonératoire de la responsabilité de la prévenue ne soit ici retenue, comme on l'a vu dans d'autres affaires.

La qualité de directeur de la publication retenue

À signaler que dans l'ensemble des textes retenus contre la personne en question, figure l'article 93-3 de la loi du 29 juillet 1982, c'est-à-dire la responsabilité éditoriale du directeur de la publication. En d'autres termes, la qualité de directeur de la publication est reconnue au titulaire d'un compte Facebook, tout comme à celui d'un blog, ce qui paraît logique puisque c'est le titulaire du compte qui décide de ce qui est publié sur l'espace qu'il maîtrise, la plateforme Facebook n'étant que l'hébergeur du compte. C'est là aussi une solution classique et de bon sens.

En savoir plus

Voir le jugement du TGI de Béthune du 16 septembre 2015 sur le site Legalis.net :
www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4750

Et la présentation succincte de la décision sur le même site :
www.legalis.net/spip.php?page=breves-article&id_article=4751

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.les-infostrateges.com/actu/15102075/e-reputation-la-diffamation-sur-facebook-punie-comme-ailleurs
Par Didier FROCHOT

Facebook : vous serez prévenu en cas de piratage par un Etat. Vraiment ? | Le Net Expert Informatique

Dans un post de blog, le RSSI de Facebook, Alex Stamos, indique que le réseau social préviendra les utilisateurs qu'il soupçonne d'être victimes d'une cyberattaque perpétrée par un groupe étatique. Une politique que Google avait déjà mise en place sur ses services.

Facebook souhaite renforcer la sécurité des données personnelles des utilisateurs et annonce, dans un post de blog signé par son RSSI, son intention de signaler les tentatives de piratage menées par des groupes liés aux gouvernements contre les utilisateurs de ses services. Une notification spécifique sera ainsi affichée sur les comptes répondant aux critères retenus par Facebook, invitant les utilisateurs à activer l'authentification double facteur proposé par le site.

Facebook propose déjà des alertes dans les cas où il soupçonne une authentification frauduleuse : ainsi, quand l'utilisateur se connecte depuis une adresse IP différente, celle-ci est notifiée sur le compte. L'authentification à double facteur empêche entièrement de se connecter depuis une IP inconnue de Facebook si l'utilisateur n'est pas en mesure d'entrer un code que le service envoie sur son téléphone.

Un air de déjà vu?

Beau geste de la part de Facebook, mais le réseau social reste particulièrement avare en terme de précisions. Ainsi, Facebook ne communique pas sur les critères qu'il retient pour déterminer l'implication d'un gouvernement dans le piratage d'un compte : la tache n'a pourtant rien d'aisé tant on sait que l'attribution des cyberattaques est une science qui n'a rien d'exact. Alex Stamos explique ainsi que ces critères sont tenus secrets pour « protéger l'intégrité de nos méthodes » mais que ces notifications ne seront utilisées que dans les cas « où les preuves viennent fortement appuyer nos suppositions. »

On peut également s'interroger sur la mise en place d'un système à deux vitesses : il paraît évident que Facebook notifiera un utilisateur américain victime d'un piratage d'origine chinoise ou russe, mais en fera-t-il autant pour un citoyen russe victime d'un piratage orchestré par la NSA ? Difficile à dire, Facebook reste peu disert sur la question.

La mise en place de cette mesure par Facebook est en tout point similaire à ce qu'avait déployé Google en 2012 : chez le géant du moteur de recherche, on se garde également de mentionner les critères retenus pour qualifier l'attaque et on pousse l'utilisateur à mettre en place un mécanisme d'authentification à deux facteurs.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.zdnet.fr/actualites/facebook-vous-serez-prevenu-en-cas-de-piratage-par-un-etat-vraiment-39826746.htm

---

Panne de Facebook ? La carte

des dysfonctionnements | Le Net Expert Informatique

Panne de Facebook ? La carte des dysfonctionnements

Facebook est un réseau social en ligne sur internet. Il permet de publier des informations (photos, liens, textes) en contrôlant la visibilité.
Il est aujourd'hui le réseau social le plus populaire. Fondé en 2004 par Mark Zuckerberg, le site est devenu incontournable au fil des années.

Les statistiques d'usages sont ahurissantes :
Utilisateurs actifs mensuels (MAU, juillet 2015) : 1,49 milliard
En Europe : 3011 millions
En Amérique du Nord : 213 millions
En Asie : 496 millions
Dans le reste du monde : 471 millions
En France : 30 millions d'utilisateurs

Utilisateurs actifs mensuels sur mobile : 1,314 milliard.
En France : 24 millions d'utilisateurs
Utilisateurs actifs mensuels uniquement sur mobile : 655 millions.
Utilisateurs actifs quotidiens (DAU) : 968 millions

Ainsi, une panne de Facebook de quelques minutes, ou plus comme celles passées en Octobre 2015, impactera des utilisateurs de toute la planète.
Lien vers la carte des pannes de Facebook

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : https://touteslespannes.fr/statut/facebook/carte/

Facebook de nouveau en panne mondialement, pendant un heure | Programmez! | Le Net Expert Informatique

Facebook de nouveau en panne mondialement, pendant un heure

Facebook connaît de temps en temps une panne mondiale, qui empêche les utilisateurs de se connecter au réseau social. La dernière grande panne mondiale date du début de l'année. A l'époque, les Lizard Quad avaient prétendus avoir lancé une attaque DDoS sur Facebook ce qui avait provoqué le problème. Facebook avait alors démenti l'attaque DDoS, et indiqué que des modifications techniques avaient été responsables du problème, sans plus d'informations.

Hier soir rebelote. Facebook a été en panne mondialement, ou dans nombreuses régions du monde, dont l'Europe, pour être plus précis. Toujours pas d'attaque DDoS des Lizard Squad, mais un problème technique. Facebook a ainsi indiqué que son API Graph a été temporairement indisponible. Ce qui veut tout dire et rien dire. Pas d'API Graph = pas de réseau social certes, mais cela n'explique rien quand au pourquoi. C'est d'ailleurs la ligne de conduite habituelle de Facebook d'être plus que sibyllin dans ce genre de situation.

Que fait-on quand un réseau social est en panne ? On en utilise un autre pour se plaindre du premier C'est ainsi que l'incident a fait les choux gras de Twitter, avec un hashtag #facebookdown qui est monté dans le Top 10 des hashtags Twitter.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.programmez.com/actualites/facebook-de-nouveau-en-panne-mondialement-pendant-un-heure-23249

Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles | Le Net Expert Informatique

	Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles

Des pirates peuvent en toute impunité obtenir le nom, la photo de votre profil et votre emplacement de votre compte Facebook vu que le réseau social n'a pas estimé que cette faille en est réellement une.

Via une faille de sécurité dans Facebook, Reza Moaiandin, un ingénieur logiciel, a réussi à obtenir les noms, les photos de profil et les emplacements des utilisateurs du réseau social, ce qui correspond tout de même à des données privées.
Pour obtenir ces données, le chercheur n'a rien piraté, il a simplement utilisé des possibilités offertes. En l'occurrence, la fonction permettant de trouver un utilisateur à partir de son numéro de téléphone, un paramètre de confidentialité méconnu est qui est par défaut autorisé pour « Tout le monde ». Cela signifie que n'importe qui peut retrouver n'importe qui simplement en connaissant son numéro de téléphone.
Futé, Reza Moaiandin a utilisé un algorithme simple pour générer des milliers de numéros mobiles possibles valables pour les États-Unis, le Royaume-Uni et le Canada. Via une API, il a ensuite simplement cherché à obtenir les données associées aux numéros.
Le fait que le système donne la possibilité de relier des profils Facebook à des numéros de téléphone à une telle échelle est une véritable de faille de sécurité vu que c'est une porte ouverte à tous les abus.
Alors que cette faille a été communiquée au réseau social au mois d'avril, Facebook ne la pas corrigée. Un ingénieur indique que cette vulnérabilité n'est pas considérée comme étant une faille de sécurité.
Si Facebook ne compte rien faire pour protéger les données personnelles de ses utilisateurs, la solution est donc que ce soient eux qui se protègent.
Pour ce faire, ils doivent limiter l'accès à leurs informations via cette fonctionnalité méconnue. Pour ce faire, il faut aller dans « Paramètres », puis « Vie privée » et chercher les personnes qui peuvent vous chercher en utilisant le numéro de téléphone fourni. Il faut modifier ce paramètre pour le mettre sur « Amis ».
Il est à souligner que Facebook s'est réfugié justement derrière le fait que chaque utilisateur peut régler la confidentialité de ses données. En clair, le réseau social ne se déclare pas responsable !

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.linformatique.org/facebook-laisse-ouvert-une-faille-permettant-a-des-pirates-de-recolter-vos-donnees-personnelles/

Votre crédit bientôt refusé à cause de vos amis Facebook ?

| Le Net Expert Informatique

	**Votre crédit bientôt refusé à cause de vos amis Facebook ?**

Le réseau social a déposé un brevet qui permettrait aux banques de scruter les contacts d'un client afin de déduire sa capacité à rembourser un crédit.

Et si votre assureur savait tout de votre état de santé… Le smartphone tuera-t-il la carte bancaire (et les banques) ?
A quoi joue Facebook ? Un brevet, déposé mardi 4 août, pourrait permettre aux banques d'examiner les relations d'un utilisateur sur le réseau social avant de lui accorder (ou non) un prêt.
Intitulé « Autorisation et authentification basée sur le réseau social de l'individu », le brevet entend proposer une nouvelle méthode d'authentification de l'internaute en fonction de ses amis Facebook, afin de limiter la propagation de spams (messages indésirables) et d'améliorer les résultats du moteur de recherche. Néanmoins, cette technique sera proposée à « des tiers », en particulier des banques. Le texte spécifie :
Lorsqu'un individu demande un prêt, le prêteur examine les scores de crédit des membres du réseau social de cet individu via un nœud autorisé. Si le score de crédit moyen de ces membres atteint le score de crédit minimum, le prêteur continue d'examiner la demande de prêt. Sinon, la demande est rejetée. »
En somme, si vos amis Facebook ont du mal à rembourser leurs prêts, alors la banque pourrait refuser de vous en accorder un. C'est une blague ? Non.

Des start-ups américaines sur la brèche
Généralement, les banques se basent sur l'historique financier pour déterminer la fiabilité d'un client, mais cette procédure est impossible si un tel historique n'existe pas. Du coup, les tentatives se multiplient pour éviter les personnes « à risque » en fonction des informations publiées sur les réseaux sociaux. Plusieurs start-ups s'en sont fait une spécialité.
Lenddo part du principe que si vos amis sont pauvres ou de mauvais payeurs, alors vous devez l'être aussi. L'entreprise américaine parcourt ainsi Facebook pour déterminer si le client potentiel est ami avec une personne ayant déjà remboursé un prêt en retard ou, pire, s'ils interagissent régulièrement.
La société LendUp, spécialisée dans le prêt en ligne, examine elle les comptes Facebook et Twitter des demandeurs, observant notamment le nombre d'amis et les interactions, afin d'accorder ou non le prêt.
De son côté, InVenture se base sur les données recueillies par le smatphone. Une application est proposée aux consommateurs pour gérer ses dépenses quotidiennes, tandis qu'un « score de crédit » est calculé en fonction des frais. Score qui sera fourni aux banques, afin de déterminer la capacité du client à rembourser un prêt.
Et même pas besoin d'appli : l'économiste Daniel Björkegren a montré qu'il suffit de croiser les dépenses des emprunteurs avec l'historique et la durée de leurs appels téléphoniques, pour réduire les défauts de paiement de 42%.

Illustration de l'ogre Facebook (Dimitris Kalogeropoylos/Flickr/CC)

En France, l'étape du « partenariat »
En France aussi, les rapprochements entre banques et réseaux sociaux commencent timidement. Début juillet, la Banque postale s'est associée avec Facebook pour que ses conseillers ouvrent des comptes sur le réseau social afin de rester en contact avec leurs clients. S'agira-t-il aussi de scruter les profils ? La banque ne s'épanche pas là-dessus, vantant la « prolongation de la relation client ».

A la mi-juillet, BNP-Paribas s'est alliée à Facebook, mais aussi Google, Twitter et LinkedIn afin d'améliorer « la pertinence de ses offres en fonction des attentes des clients ». La banque devrait ainsi bientôt proposer d'ouvrir un compte directement depuis Facebook.

La banque marche dans les pas du groupe BPCE (Banque populaire et Caisse d'épargne), allié à Facebook depuis la fin mai, dans une optique de proposer des « offres et produits innovants ». BNP-Paribas et BPCE n'ont en revanche pas précisé s'ils pourront récupérer des données de Facebook sur leurs clients.

CNN souligne néanmoins que les établissement bancaires rechignent encore à utiliser les données personnelles des réseaux sociaux pour évaluer le risque d'un crédit. « Ces données sociales n'indiquent pas nécessairement la fiabilité d'un client à rembourser un prêt à temps », note d'ailleurs John Ulzheimer, expert économique interrogé par la chaîne.

Alors, faut-il se précipiter sur son compte Facebook pour faire le tri parmi ses amis, avant que le nouveau brevet ne soit utilisé ? Pas sûr. Le site spécialisé Presse-citron tempère :

Les entreprises comme Google, Microsoft ou Facebook déposent de nombreux brevets, mais tous ne sont pas utilisés. Il est fort possible que Facebook n'utilise jamais ce brevet ou du moins pas la partie qui risque de vraiment fâcher ses utilisateurs. »

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://tempsreel.nouvelobs.com/tech/20150807.OBS3843/votre-credit-bientot-refuse-a-cause-de-vos-amis-facebook.html#xtor=EPR-1-Actu8h-20150808
Par Boris Manenti

Première forte condamnation pénale d’atteinte à la E-réputation | Le Net Expert Informatique

L'excellent site Légalis.net vient de rendre public un jugement du Tribunal correctionnel de Paris en date du 24 novembre 2014, qui a condamné à 2 ans de prison avec sursis, 3 ans de mise à l'épreuve ainsi que 50 000 € de dommages-intérêts à verser aux victimes et 27 000 € pour participation aux frais de justice des plaignants.

Les faits en bref

Il s'agit d'une femme qui n'a pas supporté d'être quittée par son amant. Elle s'est donc déchaînée contre lui, en n'hésitant pas à user de toute la technique d'internet pour usurper son identité et créer à son nom des comptes sur des réseaux sociaux (Facebook, Viadeo, LinkedIn, Twitter), harcelant sa famille, sa nouvelle compagne et même l'employeur de cet homme, ainsi que de nombreux autres agissements tels que du harcèlement téléphonique, montrant pour le moins le manque de stabilité psychologique de l'intéressée.

L'affaire avait été classée par le Procureur de la République sous la condition que la personne se tienne tranquille, ce qu'elle a été incapable de faire et elle a continué ses agissements nuisibles, d'où les poursuites et cette lourde condamnation.

Quant la méchanceté rejoint la lâcheté

Ce cas d'espèce n'est pas aussi particulier ni exceptionnel qu'on pourrait le penser. Même si les faits ne sont pas toujours portés devant la justice et médiatisés, notre expérience de nettoyeurs de net nous apporte de nombreux cas de réel acharnement de personnes qui ont le goût de nuire ou la haine suffisants pour chercher à détruire des personnes, par exemple à démolir la vie de la femme qui a osé demander le divorce contre eux, ou encore qui se sont juré qu'ils auraient la peau d'un dirigeant d'entreprise en proférant les plus graves accusations non fondées et qui continuent à le faire, sur des sites hébergés à l'étranger, alors même qu'ils sont déjà lourdement condamnés pour diffamation en correctionnelle puis en appel.

La technique du pseudonyme – ou ici celle de l'usurpation d'identité – donne très souvent aux personnes malfaisantes l'impression grisante de puissance et d'impunité (voir notre actualité du 26 février 2010 : Sur le Web 2.0 c'est carnaval tous les jours). Ce qui permet ainsi de nuire en toute impunité et en toute lâcheté…

Il y a encore la possibilité de publier sur des sites hors d'atteinte du droit français, ce qui rend les choses encore plus compliquées et plus longues à neutraliser. Mais il faut savoir qu'une telle neutralisation, même si elle est plus longue, est rarement impossible.

Dans le cas de la jurisprudence que nous évoquons, on a eu affaire à une personne suffisamment instable et incontrôlable pour qu'elle laisse des traces et qu'on remonte très vite à son identité. Mais les cas sont hélas fréquents où il est impossible d'identifier rapidement l'auteur de telles manœuvres de démolition. Il faut alors saisir la justice, avec tous les délais et les frais que cela suppose pour que, au cours de l'enquête, le juge ordonne des mesures pour remonter jusqu'à l'auteur des faits, notamment par voie d'injonction aux hébergeurs ou aux opérateurs de réseaux.

Une décision de justice exemplaire

Malgré ces réserves, il faut saluer cette décision de justice comme exemplaire au sens fort du terme : elle doit servir d'exemple pour toute personne qui serait tentée de nuire avec autant d'acharnement contre des personnes.

L'affaire reste à suivre car le jugement a été frappé d'appel : on aura donc sans doute prochainement des nouvelles de ce cas et la confirmation ou l'infirmation de la sentence par la Cour d'appel de Paris.

Le jugement : http://www.legalis.net/spip.php?page=breves-article&id_article=4672
La décision de justice intégrale : http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4671

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.les-infostrateges.com/actu/15072025/e-reputation-premiere-forte-condamnation-penale-assortie-de-dommages-interets