Montres connectées : vos données personnelles sont peut-être en danger | Le Net Expert Informatiquedc

Montres connectées : vos données personnelles sont peut-être en danger

Des chercheurs en sécurité n'ont pas eu trop de mal à récupérer des données personnelles à partir des montres connectées LG G Watch et Samsung Gear 2 Neo.

Les révélations sur les possibilités d'intrusion et de récupération de données personnelles dans les téléphones portables par les agences de renseignement américaines dévoilées dans les documents d'Edward Snowden ont conduit les éditeurs de plates-formes mobiles à relever les niveaux de sécurité, notamment par le chiffrement systématique des données personnelles et documents dans les appareils mobiles.
Et pour les montres connectées, ces gadgets qui fleurissent (ou aimeraient le faire) sur les poignets ? Une publication de chercheurs de l'Université de New Haven suggèrent que si des hackers ont besoin d'information, ils feraient bien de commencer par cette porte d'entrée.
Il n'ont pas rencontré énormément de difficultés pour obtenir différentes informations personnelles, que ce soit avec la LG G Watch (agenda, contacts, adresses email, données du podomètre) sous Android Wear ou la Samsung Gear 2 Neo (messages, emails, contacts, données de santé) sous Tizen OS….d'autant plus que ces données n'étaient pas chiffrées.
Avec la multiplication des objets connectés qui seront autant de points d'entrée théoriques à différents types de données personnelles, cette petite expérience a de quoi faire réfléchir, alors que des objets comme les montres connectées ont justement besoin d'un large accès aux données personnelles pour être pleinement efficaces, comme dans le cas de Google Now sur Android Wear.
Chiffrer les données sur les montres connectées (et les objets connectés en général) serait une bonne chose, mais encore faut-il que ce soit fait correctement, préviennent les chercheurs. Un certain nombre de failles exploitées par les agences de renseignement (mais aussi les méchants hackers) sont justement des attaques de type man-in-the-middle qui outrepassent ces protections sans même avoir à les casser.
A voir si la montre Apple Watch, en cours d'analyse à l'Université de New Haven, saura mieux préserver la vie privée de son possesseur. Il vaudrait mieux, étant donné les volumes de plusieurs dizaines de millions d'unités qui son censés être écoulés dès cette année…

Source : http://www.generation-nt.com/lg-watch-samsung-gear-montre-protection-donnees-actualite-1915829.html

Votre identité complète ne coûte que 70 dollars sur le Dark Web | Le Net Expert Informatique

La croissance galopante de la cybercriminalité n'a d'égal que la sophistication de ses techniques. L'objectif de ces attaques: le vol de données personnelles afin de les revendre au plus offrant. Des chercheurs en sécurité informatique ont sondé pendant plusieurs mois le Darkweb afin de dévoiler les dessous des marchés cybercriminels et d'en dévoiler les tarifs en vigueur.

Les bas-fonds du web regorgent de produits illicites: drogues, armes, tueurs à gages, malwares… sont autant de biens et services qu'il est possible de vendre ou d'acheter à des prix variables en toute impunité puisque ces transactions sont intraçables. Car comme nous l'explique Jérôme Granger, chargé de la communication de ce groupe d'experts qui a fouillé ces marchés parallèles (comme Silkroad Reloaded, DeepBay, Pandra ou encore Agora), «les vendeurs accordent beaucoup d'importance à leur réputation et ils vont du coup proposer des prix défiant toute concurrence pour 'un produit de qualité'». À l'heure où des entreprises payent des mille et des cents pour les obtenir afin de nous bombarder de publicités ciblées, nous nous sommes déjà tous demandé ce que valaient nos vies privées sur le marché noir. Des chercheurs du G DATA SecurityLabs ont enquêté et ont passé au crible le fonctionnement de ces lieux d'échanges où moult produits et services illégaux sont disponibles. Et les résultats sont édifiants «puisque nos identités ne valent rien», nous glisse M.Granger.

Grosse quantité à petits prix

Si vous désirez lancer une cyberattaque, vous pouvez trouver un kit du parfait pirate ou tout simplement vous octroyer les services d'un pirate expérimenté. Alors que tous les tutoriels vous sont gracieusement offerts, l'installation d'un programme malware vous coûtera 70 $, tandis qu'une attaque DDoS vous sera facturée 100 $. Mais la denrée la plus convoitée reste l'adresse email parce qu'elle permet de mener des opérations de spam ou d'hameçonnage. Comptez seulement 75 $ pour un million d'adresses valides et 70 $ l'identité complète (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires). Les accès à ces adresses -identifiants et mots de passe- sont eux légèrement plus chères: 20 $ pour un lot de 40.000 comptes. Un prix abordable pour celui qui désire usurper des identités afin de se lancer dans des escroqueries de plus haut vol. Pour les hackers fainéants, des données financières prêtes à l'emploi sont également disponibles, mais elles se payent plus cher à l'image d'une carte bancaire ou un compte Paypal qui sera monnayé à 50 $ pièce. Quant aux produits matériels illicites, ils sont également pléthore sur le Darkweb: le site 01Net nous apprend par exemple «qu'une fausse carte d'identité d'un pays européen se négocie aux alentours de 1.000 €, qu'il faudra verser 4.000 € pour un passeport et qu'au rayon drogues, un gramme de cocaïne de qualité (Amérique du Sud) se vend à partir de 75 € alors qu'un gramme d'ecstasy avec taux de pureté de 84% vaut 19 €».

Représailles compliquées

La lutte contre cette criminalité cachée s'avère aride pour plusieurs raisons. D'abord parce que ces cybercriminels sont difficilement identifiables de par l'utilisation de systèmes qui garantissent leur anonymat (comme Tor, I2P, des VPN ou des Proxy). Ensuite, les opérations menées par les différentes forces policières sont généralement trop lentes et «les sites sont hébergés sur d'autres serveurs en seulement quelques heures», selon Jérôme Granger qui indique qu'«à côté d'une protection redoutable, la seule solution réside dans une sensibilisation constante aux cyberdangers». D'autant plus que la recherche de ces cybercriminels se heurte souvent au droit international car si la coopération européenne est efficace, plusieurs pays comme la Russie et la Chine refusent toujours de céder une partie de leur souveraineté numérique. Un problème qui ne fera que s'amplifier avec le développement fulgurant des objets connectés qui sont déjà les nouvelles victimes de virus et autres logiciels malveillants.

Source : http://fr.metrotime.be/2015/06/11/must-read/votre-identite-complete-ne-coute-que-70-dollars-sur-le-darknet/
Par Gaëtan Gras

Les pirates ciblent désormais l'Internet of Things | Le Net Expert Informatique

Les pirates ciblent désormais l'Internet of Things

Les assaillants sur internet recourent généralement à des attaques DDos. Mais avec la percée de l'internet des choses (IoT), ils se tournent à présent vers de nouvelles techniques.

DDoS continue de gagner en popularité et évolue aussi. L'année dernière, il s'agissait surtout d'attaques exploitant brièvement une large bande passante. Aujourd'hui, les attaques font moins de 10 Gbps, mais durent plus de 24 heures. Voilà ce qu'affirme Akamai dans son tout dernier rapport State of the Internet.

« Ce type d'attaque de longue durée va souvent de pair avec par exemple des demandes de versement d'une somme d'argent. Car si un site ou un service web est paralysé, le fournisseur perd également de l'argent », déclare Tim Vereecke, senior solutions engineer chez Akamai. L'augmentation des attaques est partiellement due au fait que louer un botnet devient plus abordable pour les criminels. « Le coût initial d'exécution d'une attaque DDoS est à présent inférieur à ce qu'il était avant. Voilà qui explique pourquoi on enregistre aujourd'hui davantage d'attaques de plus longue durée, mais qui sont en moyenne moins puissantes. »

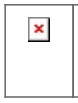
Il n'empêche que les attaques lourdes ne restent pas exceptionnelles. C'est ainsi qu'Akamai a encore enregistré au trimestre dernier huit attaques dépassant les 100 Gbps, dont la plus importante atteignait même 170 Gbps.

Mais les pirates semblent déplacer leur intérêt pour DDos vers SSDP (Simple Service Discovery Platform), un protocole pour l'Internet of Things. Ce protocole s'assure entre autres que votre ordinateur reconnaisse les autres appareils internet dans la maison. « Mais ce protocole est aussi conçu pour recevoir toutes sortes de données, ce qui en fait un candidat idéalement utilisable comme intermédiaire pour une attaque. »

Concrètement, vingt pour cent de l'ensemble des attaques recensées au premier trimestre de cette année ont été lancées via SSDP. Et ce, alors que la technique ne s'était même pas manifestée dans les statistiques jusqu'à la seconde moitié de 2014. La solution pour éviter ces attaques, c'est une bonne sécurisation et configuration des appareils connectés entre eux et à internet.

Source : http://datanews.levif.be/ict/actualite/les-pirates-ciblent-l-internet-of-things/article-normal-397387.html

La voiture autonome vulnérable aux cyber-attaques, selon des experts | Le Net Expert Informatique



La voiture autonome vulnérable aux cyber-attaques, selon des experts

Le risque de voir des pirates informatiques prendre le contrôle de voitures autonomes est bien réel, estiment des experts américains, une hypothèse d'ores et déjà prise en compte par les constructeurs et les assureurs aux Etats-Unis.

Annoncées sur les routes en 2020, voire même dès 2017, la voiture sans conducteur devrait disposer des technologies dernier cri comme des capteurs numériques –caméras, radars, sonars, lidars (guidage par laser)– gérées à distance par des logiciels permettant de reconnaître des limites de chaussées, des panneaux ou encore des obstacles.
Mais, comme pour les automobiles connectées et leurs systèmes multimédias embarqués, ces nouvelles technologies de pointe censées rendre les véhicules plus sûrs et fiables, pourraient aussi les rendre vulnérables aux attaques de hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc.
Un pirate informatique s'est récemment vanté d'avoir pénétré les systèmes électroniques d'un avion de ligne dans lequel il voyageait, et d'en avoir modifié la trajectoire. Ceci en utilisant le système wifi proposé aux passagers.
Les deux sociétés de sécurité ont effectué, en collaboration avec l'Université de Virginie (est) et le ministère américain de la Défense, des tests en situation réelle qui ont montré, selon elles, qu'il était possible de désorganiser le système.
L'un des essais consistait à modifier le comportement de la voiture face à un obstacle: le piratage «oblige la voiture à accélérer au lieu de freiner même si l'obstacle a été détecté par le Lidar, entraînant une collision à grande vitesse», selon le rapport consultable sur le site internet de MSi (missionsecure.net).
Une autre cyber-attaque «provoque un freinage d'urgence inapproprié plutôt qu'un freinage en douceur, pouvant entraîner la perte de contrôle du véhicule», peut-on encore lire.
Selon ces experts, les pirates pénètrent le système grâce aux connexions sans fil, bluetooth et wifi.
MSi et Perrone Robotics, qui développent un système payant pour parer les cyber-attaques, estiment que «cette situation pose des défis importants et des risques pour l'industrie automobile ainsi que pour la sécurité publique».
– Primes d'assurances revues ? –
La plupart des constructeurs automobile s'attelant à la fabrication de leur voiture autonome n'ont pas donné suite aux sollicitations de l'AFP sur le sujet.
Mais, selon des sources proches de l'industrie, les éventualités de cyber-attaques ont été prises en compte et testées tout au long du processus de fabrication.
Le géant de l'internet Google, par exemple, aurait une équipe d'informaticiens de haut vol chargée de défier les logiciels destinés à sa propre voiture autonome qui va être testée sur la voie publique à partir de cet été, selon des sources industrielles.
Contacté par l'AFP, le groupe de Mountain View (Californie) s'est refusé à tout commentaire.
Cette question de sécurité préoccupe les assureurs américains qui sont dans l'expectative face à ces nouvelles technologies et à leur capacité à réduire réellement les risques d'accidents. Cela pourrait les obliger à repenser leurs contrats et à recalculer les primes.
Dans un premier temps, ces dernières pourraient augmenter à cause du prix des voitures autonomes, qui sera élevé en raison du coût des technologies embarquées et des réparations éventuelles, a expliqué l'assureur Nationwide à l'AFP.
Mais, a-t-il ajouté, cela pourrait être en partie compensé avec la généralisation de ces véhicules supposés éviter les accidents. Pour State Farm, autre assureur américain, il est nécessaire d'avoir une «vue d'ensemble».
«Certes les technologies des voitures autonomes et connectées réduisent ou éliminent certains risques auxquels font face aujourd'hui les conducteurs, mais de nouveaux risques vont probablement apparaître», a argumenté la compagnie.
Selon un important assureur américain ayant requis l'anonymat, il sera essentiel de bien baliser les responsabilités en cas d'accidents. Celles-ci seront établies en fonction des instructions des constructeurs automobiles sur ce que la voiture pourra faire ou non de manière autonome.

Source : http://www.liberation.fr/economie/2015/05/31/la-voiture-autonome-vulnerable-aux-cyber-attaques-selon-des-experts_1320239

| Le Net Expert Informatique

Android : vos données personnelles impossibles à effacer ? | Le Net Expert Informatique

Android : vos données personnelles impossibles à effacer ?

Des chercheurs ont mis en lumière les problèmes de sécurité du système d'exploitation mobile de Google.
Grâce à un seul petit bouton « Restaurer les paramètres d'usine », Google promet à ses utilisateurs de supprimer tous les contenus de leur smartphone Android. La mémoire du smartphone serait ainsi totalement effacée. Mais à en croire une étude menée par deux chercheurs de l'université de Cambridge, il n'en est rien : cette fonction de suppression serait inefficace sur plus de 500 millions de smartphones Android. Explications.

Quelles données ont été récupérées ?
Les chercheurs ont examiné 21 smartphones de 5 grandes marques et sous différentes versions d'Android : Samsung Galaxy S2 et S3, LG Optimus L7, Nexus 7, HTC Desire C, Motorola Razr I, etc. Cet échantillon représenterait près de 500 millions de smartphones actuellement en circulation. Sur la totalité des smartphones étudiés, les données personnelles ont pu être récupérées après avoir été effacées. Les deux chercheurs ont ainsi pu mettre la main sur les identifiants Google des utilisateurs sur tous les modèles. Puis, ils ont pu accéder aux informations des services Google associés à ces comptes : Gmail, Calendrier, Drive, etc. Enfin, les chercheurs ont pu récupérer des données de communications (SMS, e-mails, appels, etc.) et des fichiers multimédias (photos et vidéos).

Comment c'est possible ?
Comme l'explique le résultat des recherches, lorsqu'un utilisateur appuie sur le bouton pour effacer ses données, le smartphone supprime en réalité l'accès à ces données et non les informations elles-mêmes. « C'est comme pour un ordinateur : un formatage du disque dur ne suffit pas à effacer les données », explique à Europe 1 Jean-François Beuze, expert en sécurité informatique.

Comment être sûr que toutes les données sont effacées ?
« Il faut chiffrer ses données », conseille le spécialiste en sécurité. C'est à dire ajouter une étape de protection supplémentaire à ces informations personnelles. Pour cela, il faut se rendre dans les réglages du smartphone, puis dans le menu Sécurité et enfin cocher la case « chiffrer les données sur le smartphone ». Si une carte mémoire est utilisée pour étendre le stockage de l'appareil, l'utilisateur devra également chiffrer celle-ci. Pour les données les plus sensibles, « il existe des appareils émettant un champ électromagnétique pour effacer toute donnée sur le smartphone », ajoute Jean-François Beuze. Mais ces appareils restent réservés aux professionnels en raison de leur coût élevé.

Source : http://www.europe1.fr/technologies/android-les-donnees-personnelles-impossibles-a-effacer-970842

L’immatriculation des drones, solution à toutes les craintes ? | Le Net Expert Informatique

L’immatriculation des drones, la la solution à toutes les craintes ?

L’immatriculation des drones de loisir est-elle une solution efficace pour responsabiliser leurs propriétaires ? À vous de juger !

Doter les drones de loisir de plaques d’immatriculation : c’est l’une des pistes de réforme envisagées par le gouvernement pour éviter les survols intempestifs de ces petits robots volants au-dessus de la capitale et aux abords de centrales nucléaires. La soixantaine d’incidents recensés ces derniers mois a en effet révélé les lacunes de la réglementation et des systèmes de détection et d’interception existants.

Deux projets ont été sélectionnés par l’Agence nationale de la recherche (ANR) en vue de relever le défi que ces engins provocateurs lancent aux autorités. Des systèmes de captation de signaux entre le pilote et l’appareil et de brouillage GPS forçant le drone à atterrir sont en cours d’expérimentation. Il est aussi question de doter ces appareils de puces d’identification.

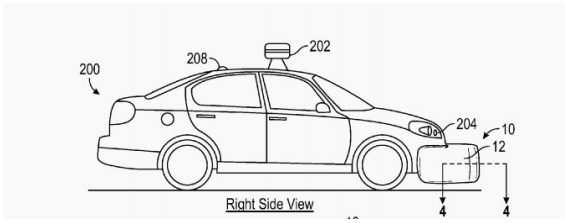
La dissuasion passe également par des sanctions plus lourdes que celles encourues actuellement pour le non-respect des règles de sécurité, à savoir un an d’emprisonnement et 75 000 euros d’amende, outre les peines encourues pour mise en danger de la vie d’autrui. Car les drones présentent des risques, peuvent blesser des gens, s’écraser sur une route ou sur une piste d’aéroport. Une collision avait été évitée de justesse entre un A320 et un drone à l’aéroport de Heathrow en juillet 2014…
Faut-il obliger les propriétaires de drones à les faire immatriculer à leurs frais comme le font les propriétaires d’aéronefs civils ? À vous de juger – et de voter après avoir regardé nos deux expertes, Myriam Quéméner et Christiane Féral-Schuhl, plaider le « pour » et le « contre » en… trois minutes !

Faut-il immatriculer les drones ? *par LePoint*

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

Source : http://www.lepoint.fr/justice-internet/au-tribunal-de-l-internet-faut-il-immatriculer-les-drones-18-05-2015-1929083_2081.php
Par Laurence NEUER ET Anne-Sophie JAHN

La voiture sans conducteur de Google pourrait disposer d’airbags à l’extérieur | Le Net Expert Informatique



La voiture sans conducteur de Google pourrait disposer d’airbags à l’extérieur

La voiture sans conducteur de Google pourrait s’enrichir d’une nouveauté destinée à protéger non pas les passagers du véhicule, mais les piétons aux environs : un système d’airbags extérieurs.

Les airbags intégrés à l’intérieur d’une voiture sont aujourd’hui de série au sein de la très grande majorité des véhicules proposés sur le marché. Néanmoins, les airbags extérieurs restent, eux, inédits. Google souhaite vraisemblablement remédier à la situation : l’entreprise a déposé un brevet qui décrit un pare-chocs bardé de « sacs d’air » capables de se gonfler automatiquement et très rapidement dans certaines situations, à l’image d’un airbag destiné à protéger les passagers du véhicule.

Une protection pour les piétons
Fixés à l’avant du véhicule, ces airbags extérieurs seraient principalement destinés à protéger les piétons qui pourraient se faire percuter par le véhicule au niveau des jambes. Le brevet est d’ailleurs intitulé « Système de protection des jambes des piétons lors d’un impact avec un véhicule », ce qui résume parfaitement la mécanique décrite au sein du document.

Rassurer les sceptiques
Les prototypes de voitures autonomes de Google circulent en Californie depuis plusieurs années, et aucun incident important n’a été relevé jusque-là. Cependant, cela n’empêche pas de nombreux observateurs de s’inquiéter concernant les risques liés à ce genre de véhicule.
Il n’est donc pas étonnant que l’entreprise cherche à renforcer au maximum la sécurité de ses voitures autonomes : de telles innovations pourraient, par ailleurs, trouver un intérêt au-delà des seuls véhicules sans conducteur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.clubic.com/mag/transports/actualite-760399-voiture-conducteur-google-airbags-exterieur.html
http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=70&f=G&l=50&d=PTXT&s1=google.ASNM.&p=2&OS=AN/google&RS=AN/google

Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ? | Le Net Expert Informatique

12

	Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ?

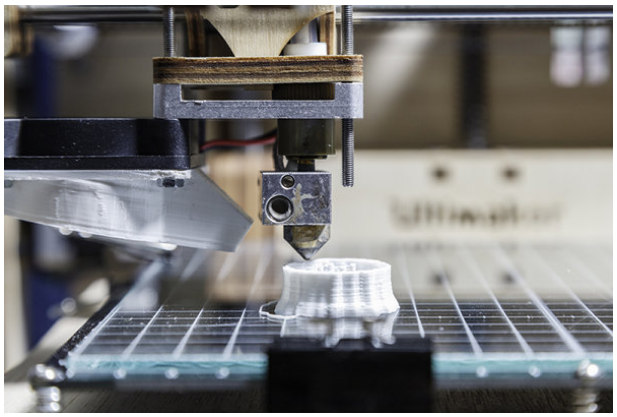
Le piratage à distance en 2020 du stimulateur cardiaque d'un dirigeant d'un grand pays est le point de départ de la nouvelle « Café, Wi-Fi et la Lune » de Nikolas Katsimpras, qui a été primée ce mardi 17 mars par le Conseil Atlantique. Les candidats étaient invités par ce think tank de Washington, à présenter des textes courts, fictifs, de « unes » de journaux, sur le déclenchement du prochain conflit majeur, en s'inspirant des événements qui ont emporté le monde dans la Grande Guerre en 1914.

Le choix du jury souligne deux consensus. En premier, nous devrions à très court terme être immergés dans une multitude d'Objets Connectés, senseurs et capteurs qui nous aideront sur de nombreux aspects de notre vie. En second, la sécurisation de cet Internet des Objets face à des actes de maladresse comme de malveillance, pose encore de nombreux problèmes techniques et politiques. Enfin, le Conseil Atlantique ouvre par cette initiative la question de la contribution de l'art et de la littérature à ce débat, en terme de communication ou pour faciliter la prise de conscience par le grand public du travail restant à faire dans le domaine de la cyber-sécurité et du respect de la sphère privée.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.bulletins-electroniques.com/actualites/78150.htm

Des sénateurs PS veulent taxer l’impression 3D avec la redevance copie privée | Le Net Expert Informatique



Des sénateurs PS veulent taxer l’impression 3D avec la redevance copie privée

Le groupe PS du Sénat a déposé un amendement visant à faire tomber l'impression 3D sous le coup de la redevance copie-privée, une taxe visant à compenser le préjudice causé aux ayants droits à l'occasion de la reproduction de leurs oeuvres.

Tandis que le Sénat américain pousse pour une résolution en faveur de l'internet des objets, l'exception française continue de s'appliquer en matière de hautes technologies… La France entrave la vente de Dailymotion et un amendement déposé par le groupe socialiste au Sénat pourrait même aboutir à une taxation de l'impression 3D. Un comble.

La redevance copie-privée :
Au Sénat, un texte qui sera pourtant débattu à l'occasion du passage en séance du projet de loi Macron sur la croissance, l'activité et l'égalité des chances. Dans ce cadre, un amendement sera examiné à propos de la soumission de la fabrication additive à la redevance copie privée, censée compenser le préjudice subi par les ayant-droits d'oeuvres reproduites.
Cette compensation a été créée il y a plusieurs années lorsque les supports numériques et le téléchargement illégal mettaient en péril l'équilibre financier de la culture. La plupart des supports numériques, comme les CD et DVD vierges, disques durs externes, clefs USB, cartes mémoires, GPS et autoradios avaient ainsi écopés d'une taxe censée compenser le préjudice causé aux ayants droits à l'occasion de la reproduction de leurs oeuvres.

L'impression 3D dans la ligne de mire :
Des sénateurs socialistes aimeraient que ce mécanisme s'étende désormais aux systèmes d'impressions 3D. C'est en tous cas le sens d'un amendement déposé en ce sens par son groupe au Sénat, qui vent modifier la formulation lexicale du texte, qui réserve la taxe aux seuls « supports », qui pourraient se voir adjoindre également les reproductions faites « par une technologie d'impression en trois dimensions ». Si cet amendement était voté, la redevance copie-privée porteraient dès lors également sur les œuvres en trois dimensions et serait soit prélevée sur les imprimantes 3D lors de l'achat, soit sur les consommables, c'est à dire la matière-première servant à l'impression 3D.
Au Ministère de la Culture, on envisage aussi de faire porter cette taxe sur les liseuses électroniques, les consoles de jeux vidéos, ou les technologies de stockage dan le Cloud… on a décidément beaucoup d'imagination en France pour taxer ce qui marche

---

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://www.aruco.com/2015/04/senat-taxe-impression-3d/
Par Geoffray