Qui veut cadenasser le Web ?

Durant longtemps, des canaris et des pinsons ont travaillé dans les mines de charbon. Ces oiseaux étaient utilisés pour donner l'alarme quand les émanations de monoxyde de carbone se faisaient menaçantes.

Dès qu'ils battaient des ailes ou se hérissaient voire mouraient, les mineurs étaient avertis de la présence du gaz avant qu'eux-mêmes ne la perçoivent. Depuis, les alarmes électroniques ont pris le relais, évitant ainsi le sacrifice de milliers d'oiseaux.

(source)

Pour Cory Doctorow (faut-il encore présenter cet écrivain et militant des libertés numériques ?), le canari mort dans la mine, c'est le W3C qui a capitulé devant les exigences de l'industrie du divertissement et des médias numériques.

Il fait le bilan des pressions qui se sont exercées, explique pourquoi l'EFF a quitté le W3C et suggère comment continuer à combattre les verrous numériques inefficaces et dangereux.

Avant de commencer la lecture, vous pourriez avoir besoin d'identifier les acronymes qu'il mentionne fréquemment :

EFF : une organisation non-gouvernementale (*Electronic Frontier Foundation*) et internationale qui milite activement pour les droits numériques, notamment sur le plan juridique et par des campagnes d'information et de mobilisation. En savoir plus sur la page Wikipédia

W3C : un organisme a but non lucratif (*World Wide Web Consortium*) qui est censé proposer des standards des technologies du Web pour qu'elles soient compatibles. En savoir plus sur la page Wikipédia

DRM : la gestion des droits numériques (*Digital Rights Management*). Les DRM visent à contrôler l'utilisation des œuvres numériques. En savoir plus sur la page Wikipédia

EME : des modules complémentaires (*Encrypted Media Extensions*) créés par le W3C qui permettent aux navigateurs d'accéder aux contenus verrouillés par les

DRM. En savoir plus sur la page Wikipédia

Traduction Framalang : FranBAG, simon, jums, Moutmout, Lumibd, Makoto242, redmood, Penguin, goofy

(article original sur le site de l'EFF)

Alerte aux DRM : comment nous venons de perdre le Web, ce que nous en avons appris , et ce que nous devons faire désormais

Par **CORY DOCTOROW**

Cory Doctorow (CC-BY-SA Jonathan Worth)

L'EFF s'est battue contre les DRM et ses lois depuis une quinzaine d'années, notamment dans les affaires du « broadcast flag » américain, du traité de radiodiffusion des Nations Unies, du standard européen DVB CPCM, du standard EME du W3C, et dans de nombreuses autres escarmouches, batailles et même guerres au fil des années. Forts de cette longue expérience, voici deux choses que nous voulons vous dire à propos des DRM :

1. Tout le monde sait dans les milieux bien informés que la technologie DRM n'est pas pertinente, mais que c'est la loi sur les DRM qui est décisive ;
2. La raison pour laquelle les entreprises veulent des DRM n'a rien à voir avec le droit d'auteur.

Ces deux points viennent d'être démontrés dans un combat désordonné et interminable autour de la standardisation des DRM dans les navigateurs, et

comme nous avons consacré beaucoup d'argent et d'énergie à ce combat, nous aimerions retirer des enseignements de ces deux points, et fournir une feuille de route pour les combats à venir contre les DRM.

Les DRM : un échec technologique, une arme létale au plan légal

Voici, à peu près, comment fonctionnent les DRM : une entreprise veut fournir à un client (vous) un contenu dématérialisé (un film, un livre, une musique, un jeu vidéo, une application…) mais elle veut contrôler ce que vous faites avec ce contenu une fois que vous l'avez obtenu.

Alors elles chiffrent le fichier. On adore le chiffrement. Parce que ça fonctionne. Avec relativement peu d'efforts, n'importe qui peut chiffrer un fichier de sorte que personne ne pourra jamais le déchiffrer à moins d'obtenir la clef.

Supposons qu'il s'agisse de Netflix. Ils vous envoient un film qui a été chiffré et ils veulent être sûrs que vous ne pouvez pas l'enregistrer ni le regarder plus tard depuis votre disque dur. Mais ils ont aussi besoin de vous donner un moyen de voir le film. Cela signifie qu'il faut à un moment déchiffrer le film. Et il y a un seul moyen de déchiffrer un fichier qui a été entièrement chiffré : vous avez besoin de la clef.

Donc Netflix vous donne aussi la clef de déchiffrement.

Mais si vous avez la clef, vous pouvez déchiffrer les films de Netflix et les enregistrer sur votre disque dur. Comment Netflix peut-il vous donner la clef tout en contrôlant la façon dont vous l'utilisez ?

Netflix doit cacher la clef, quelque part dans votre ordinateur, dans une extension de navigateur ou une application par exemple. C'est là que la technologie atteint ses limites. Bien cacher quelque chose est difficile. Mais bien cacher quelque chose dans un appareil que vous donnez à votre adversaire pour qu'il puisse l'emporter avec lui et en faire ce qu'il veut, c'est impossible.

Peut-être ne pouvez-vous pas trouver les clefs que Netflix a cachées dans votre navigateur. Mais certains le peuvent : un étudiant en fin d'études qui s'ennuie pendant un week-end, un génie autodidacte qui démonte une puce dans son sous-sol, un concurrent avec un laboratoire entier à sa disposition. Une seule

minuscule faille dans la fragile enveloppe qui entoure ces clefs et elles sont libérées !

Et une fois que cette faille est découverte, n'importe qui peut écrire une application ou une extension de navigateur avec un bouton « sauvegarder ». C'est l'échec et mat pour la technologie DRM (les clés fuitent assez souvent, au bout d'un temps comparable à celui qu'il faut aux entreprises de gestion des droits numériques pour révoquer la clé).

Il faut des années à des ingénieurs talentueux, au prix de millions de dollars, pour concevoir des DRM. Qui sont brisés au bout de quelques jours, par des adolescents, avec du matériel amateur. Ce n'est pas que les fabricants de DRM soient stupides, c'est parce qu'ils font quelque chose de stupide.

C'est là qu'intervient la loi sur les DRM, qui donne un contrôle légal plus puissant et plus étendu aux détenteurs de droits que les lois qui encadrent n'importe quel autre type de technologie. En 1998, le Congrès a adopté le Digital Milennium Copyright Act, DCMA dont la section 1201 prévoit une responsabilité pénale pour quiconque contourne un système de DRM dans un but lucratif : 5 ans d'emprisonnement et une amende de 500 000 $ pour une première infraction. Même le contournement à des fins non lucratives des DRM peut engager la responsabilité pénale. Elle rend tout aussi dangereux d'un point de vue légal le simple fait de *parler* des moyens de contourner un système de DRM.

Ainsi, la loi renforce les systèmes de DRM avec une large gamme de menaces. Si les gens de Netflix conçoivent un lecteur vidéo qui n'enregistrera pas la vidéo à moins que vous ne cassiez des DRM, ils ont maintenant le droit de porter plainte – ou faire appel à la police – contre n'importe quel rival qui met en place un meilleur service de lecture vidéo alternatif, ou un enregistreur de vidéo qui fonctionne avec Netflix. De tels outils ne violent pas la loi sur le droit d'auteur, pas plus qu'un magnétoscope ou un Tivo, mais puisque cet enregistreur aurait besoin de casser le DRM de Netflix, la loi sur les DRM peut être utilisée pour le réduire au silence.

La loi sur les DRM va au-delà de l'interdiction du contournement de DRM. Les entreprises utilisent aussi la section 1201 de la DMCA pour menacer des chercheurs en sécurité qui découvrent des failles dans leurs produits. La loi devient une arme qu'ils peuvent pointer sur quiconque voudrait prévenir leurs

consommateurs (c'est toujours vous) que les produits auxquels vous faites confiance sont impropres à l'usage. Y compris pour prévenir les gens de failles dans les DRM qui pourraient les exposer au piratage.

Et il ne s'agit pas seulement des États-Unis, ni du seul DCMA. Le représentant du commerce international des États-Unis a « convaincu » des pays dans le monde entier d'adopter une version de cette règle.

Les DRM n'ont rien à voir avec le droit d'auteur

La loi sur les DRM est susceptible de provoquer des dommages incalculables. Dans la mesure où elle fournit aux entreprises le pouvoir de contrôler leurs produits après les avoir vendus, le pouvoir de décider qui peut entrer en compétition avec elles et sous quelles conditions, et même qui peut prévenir les gens concernant des produits défectueux, la loi sur les DRM constitue une forte tentation.

Certaines choses ne relèvent pas de la violation de droits d'auteur : acheter un DVD pendant que vous êtes en vacances et le passer quand vous arrivez chez vous. Ce n'est de toute évidence pas une violation de droits d'auteur d'aller dans un magasin, disons à New Delhi, d'acheter un DVD et de le rapporter chez soi à Topeka. L'ayant droit a fait son film, l'a vendu au détaillant, et vous avez payé au détaillant le prix demandé. C'est le contraire d'une violation de droits d'auteur. C'est l'achat d'une œuvre selon les conditions fixées par l'ayant droit. Mais puisque le DRM vous empêche de lire des disques hors-zone sur votre lecteur, les studios peuvent invoquer le droit d'auteur pour décider où vous pouvez consommer les œuvres sous droit d'auteur que vous avez achetées en toute honnêteté.

D'autres non-violations : réparer votre voiture (General Motors utilise les DRM pour maîtriser qui peut faire un diagnostic moteur, et obliger les mécaniciens à dépenser des dizaines de milliers de dollars pour un diagnostic qu'ils pourraient sinon obtenir par eux-mêmes ou par l'intermédiaire de tierces parties); recharger une cartouche d'encre (HP a publié une fausse mise à jour de sécurité qui a ajouté du DRM à des millions d'imprimantes à jet d'encre afin qu'elles refusent des cartouches reconditionnées ou venant d'un tiers), ou faire griller du pain fait maison (même si ça ne s'est pas encore produit, rien ne pourrait empêcher une entreprise de mettre des DRM dans ses grille-pains afin de contrôler la

provenance du pain que vous utilisez).

Ce n'est pas non plus une violation du droit d'auteur de regarder Netflix dans un navigateur non-approuvé par Netflix. Ce n'est pas une violation du droit d'auteur d'enregistrer une vidéo Netflix pour la regarder plus tard. Ce n'est pas une violation du droit d'auteur de donner une vidéo Netflix à un algorithme qui pourra vous prévenir des effets stroboscopiques à venir qui peuvent provoquer des convulsions potentiellement mortelles chez les personnes atteintes d'épilepsie photosensible.

Ce qui nous amène au W3C

Le W3C est le principal organisme de normalisation du Web, un consortium dont les membres (entreprises, universités, agences gouvernementales, associations de la société civile entre autres) s'impliquent dans des batailles sans fin concernant le meilleur moyen pour tout le monde de fournir du contenu en ligne. Ils créent des « recommandations » (la façon pour le W3C de dire « standards »), ce sont un peu comme des étais invisibles qui soutiennent le Web. Ces recommandations, fruits de négociations patientes et de compromis, aboutissent à un consensus des principaux acteurs sur les meilleures (ou les moins pires) façons de résoudre certains problèmes technologiques épineux.

En 2013, Netflix et quelques autres entreprises du secteur des médias ont convaincu le W3C de commencer à travailler sur un système de DRM pour le Web. Ce système de DRM, Encrypted Media Extensions, constitue un virage à 180 degrés par rapport aux habitudes du W3C. Tout d'abord, les EME ne seraient pas un standard à part entière : l'organisation spécifierait une API au travers de laquelle les éditeurs et les vendeurs de navigateurs pourraient faire fonctionner les DRM, mais le « module de déchiffrement du contenu » (*content decryption module*, CDM) ne serait pas défini par la norme. Ce qui signifie que les EME n'ont de norme que le nom : si vous lanciez une entreprise de navigateurs en suivant toutes les recommandations du W3C, vous seriez toujours incapables de jouer une vidéo Netflix. Pour cela, vous auriez besoin de la permission de Netflix.

Je n'exagère pas en disant que c'est vraiment bizarre. Les standards du Web existent pour assurer « une interopérabilité sans permission ». Les standards de formatage de texte sont tels que n'importe qui peut créer un outil qui peut afficher les pages du site web du New York Times, les images de Getty ou les

diagrammes interactifs sur Bloomberg. Les entreprises peuvent toujours décider de qui peut voir quelles pages de leur site web (en décidant qui possède un mot de passe et quelles parties du site sont accessibles par chaque mot de passe), mais elles ne décident pas de qui peut créer le programme de navigateur web dans lequel vous entrez le mot de passe pour accéder au site.

Un Web où chaque éditeur peut choisir avec quels navigateurs vous pouvez visiter son site est vraiment différent du Web historique. Historiquement, chacun pouvait concevoir un nouveau navigateur en s'assurant qu'il respecte les recommandations du W3C, puis rivaliser avec les navigateurs déjà présents. Et bien que le Web ait toujours été dominé par quelques navigateurs, le navigateur dominant a changé toutes les décennies, de sorte que de nouvelles entreprises ou même des organisations à but non lucratif comme Mozilla (qui a développé Firefox) ont pu renverser l'ordre établi. Les technologies qui se trouvaient en travers de cette interopérabilité sans permission préalable – comme les technologies vidéos brevetées – ont été perçues comme des entraves à l'idée d'un Web ouvert et non comme des opportunités de standardisation.

Quand les gens du W3C ont commencé à créer des technologies qui marchent uniquement quand elles ont reçu la bénédiction d'une poignée d'entreprises de divertissement, ils ont mis leurs doigts – et même leurs mains – dans l'engrenage qui assurera aux géants de la navigation un règne perpétuel.

Mais ce n'est pas le pire. Jusqu'aux EME, les standards du W3C étaient conçus pour donner aux utilisateurs du Web (i.e. vous) plus de contrôle sur ce que votre ordinateur fait quand vous visitez les sites web d'autres personnes. Avec les EME, et pour la toute première fois, le W3C est en train de concevoir une technologie qui va vous enlever ce contrôle. Les EME sont conçus pour autoriser Netflix et d'autres grosses entreprises à décider de ce que fait votre navigateur, même (et surtout) quand vous êtes en désaccord avec ce qui devrait se passer.

Il y a un débat persistant depuis les débuts de l'informatique pour savoir si les ordinateurs existent pour contrôler leurs utilisateurs, ou vice versa (comme le disait l'informaticien visionnaire et spécialiste de l'éducation Seymour Papert « les enfants devraient programmer les ordinateurs plutôt que d'être programmés par eux » – et ça s'applique aussi bien aux adultes). Tous les standards du W3C jusqu'en 2017 ont été en faveur du contrôle des ordinateurs par les utilisateurs. Les EME rompent avec cette tradition. C'est un changement subtil mais crucial.

…et pourquoi le W3C devrait faire ça ?

Aïe aïe aïe. C'est la question à trois milliards d'utilisateurs.

La version de cette histoire racontée par le W3C ressemble un peu à ce qui suit. L'apparition massive des applications a affaibli le Web. À l'époque « pré-applis», le Web était le seul joueur dans la partie, donc les sociétés devaient jouer en suivant ses règles : standards libres, Web libre. Mais maintenant que les applications existent et que presque tout le monde les utilise, les grandes sociétés peuvent boycotter le Web, obligeant leurs utilisateurs à s'orienter vers les applications. Ce qui ne fait qu'accélérer la multiplication des applis, et affaiblit d'autant plus le Web. Les applications ont l'habitude d'implémenter les DRM, alors les sociétés utilisant ces DRM se sont tournées vers les applis. Afin d'empêcher les entreprises du divertissement de tuer le Web, celui-ci doit avoir des DRM également.

Toujours selon cette même théorie, même si ces sociétés n'abandonnent pas entièrement le Web, il est toujours préférable de les forcer à faire leurs DRM en suivant le W3C que de les laisser faire avec les moyens *ad hoc*. Laissées à elles-mêmes, elles pourraient créer des DRM ne prenant pas en compte les besoins des personnes à handicap, et sans l'influence modératrice du W3C, ces sociétés créeraient des DRM ne respectant pas la vie privée numérique des utilisateurs.

On ne peut pas espérer d'une organisation qu'elle dépense des fortunes pour créer des films ou en acquérir des licences puis distribue ces films de telle sorte que n'importe qui puisse les copier et les partager.

Nous pensons que ces arguments sont sans réel fondement. Il est vrai que le Web a perdu une partie de sa force liée à son exclusivité du début, mais la vérité c'est que les entreprises gagnent de l'argent en allant là où se trouvent leurs clients. Or tous les clients potentiels ont un navigateur, tandis que seul les clients déjà existants ont les applications des entreprises. Plus il y aura d'obstacles à franchir entre vous et vos clients, moins vous aurez de clients. Netflix est sur un marché hyper-compétitif avec des tonnes de nouveaux concurrents (p.ex. Disney), et être considéré comme « ce service de streaming inaccessible via le Web » est un sérieux désavantage.

Nous pensons aussi que les médias et les entreprises IT auraient du mal à se

mettre d'accord sur un standard pour les DRM hors W3C, même un très mauvais standard. Nous avons passé beaucoup de temps dans les salles remplies de fumée où se déroulait la standardisation des systèmes de DRM ; la dynamique principale était celles des médias demandant le verrouillage complet de chaque image de chaque vidéo, et des entreprises IT répondant que le mieux que quiconque puisse espérer était un ralentissement peu efficace qu'elles espéraient suffisant pour les médias. La plupart du temps, ces négociations s'effondrent sans arriver nulle part.

Il y a aussi la question des brevets : les entreprises qui pensent que les DRM sont une bonne idée adorent les brevets logiciels, et le résultat est un fouillis sans nom de brevets qui empêchent de parvenir à faire quoi que ce soit. Le mécanisme de regroupement de brevets du W3C (qui se démarque par sa complétude dans le monde des standards et constitue un exemple de la meilleure façon d'accomplir ce genre de choses) a joué un rôle indispensable dans le processus de standardisation des DRM. De plus, dans le monde des DRM, il existe des acteurs-clefs – comme Adobe – qui détiennent d'importants portfolios de brevets mais jouent un rôle de plus en plus réduit dans le monde des DRM (l'objectif avoué du système EME est de « tuer Flash »).

Si les entreprises impliquées devaient s'asseoir à la table des négociations pour trouver un nouvel accord sur les brevets sans le *framework* du W3C, n'importe laquelle de ces entreprises pourrait virer troll et décider que les autres doivent dépenser beaucoup d'argent pour obtenir une licence sur leurs brevets – elle n'aurait rien à perdre à menacer le processus de négociations et tout à gagner même sur des droits par utilisateur, même minuscules, pour quelque chose qui sera installé dans trois milliards de navigateurs.

En somme, il n'y a pas de raison de penser que les EME ont pour objectif de protéger des intérêts commerciaux légitimes. Les services de streaming vidéo comme Netflix reposent sur l'inscription de leurs clients à toute une collection, constamment enrichie avec de nouveaux contenus et un système de recommandations pour aider ses utilisateurs à s'y retrouver.

Les DRM pour les vidéos en streaming sont ni plus ni moins un moyen d'éviter la concurrence, pas de protéger le droit d'auteur. L'objectif des DRM est de munir les entreprises d'un outil légal pour empêcher des activités qui seraient autorisées sinon. Les DRM n'ont pas vocation à « fonctionner » (au sens de

prévenir les atteintes au droit d'auteur) tant qu'ils permettent d'invoquer le DMCA.

Pour vous en convaincre, prenez simplement l'exemple de Widevine, la version des EME de Google. Ce mastodonte a racheté la boîte qui développait Widevine en 2010, mais il a fallu attendre 2016, pour qu'un chercheur indépendant se penche réellement sur la façon dont elle empêchait la fuite de ses vidéos. Ce chercheur, David Livshits a remarqué que Widevine était particulièrement facile à contourner, et ce dès sa création, et que les erreurs qui rendaient Widevine aussi inefficace étaient évidentes, même avec un examen superficiel. Si les millions de dollars et le personnel hautement qualifié affectés aux EME avaient pour but de créer une technologie qui lutterait efficacement contre les atteintes au droit d'auteur, alors vous pourriez croire que Netflix ou une des autres entreprises de médias numériques impliquées dans les négociations auraient utilisé une partie de toutes ces ressources à un rapide audit, pour s'assurer que leur produit fonctionne réellement comme annoncé.

(Détail amusant : Livshits est un Israélien qui travaille à l'université Ben Gourion, et il se trouve que l'Israël est un des rares pays qui ne condamnent pas les violations de DRM, ce qui signifie que les Israéliens font partie des seules personnes qui peuvent faire ce type de recherche, sans craintes de représailles juridiques)

Mais la plus belle preuve que les EME étaient tout simplement un moyen d'éliminer les concurrents légitimes, et non une tentative de protection du droit d'auteur, la voici.

Une expérience sous contrôle

Lorsque l'EFF a rejoint le W3C, notre principale condition était « ne faites pas de DRM ».

Nous avons porté l'affaire devant l'organisation, en décrivant la façon dont les DRM interférent avec les exceptions aux droits auteurs essentielles (comme celles qui permettent à chaque individu d'enregistrer et modifier un travail protégé par droits d'auteur, dans le cadre d'une critique, ou d'une adaptation) ainsi que la myriade de problèmes posés par le DMCA et par d'autres lois semblables à travers le monde.

L’équipe de direction de la W3C a tout simplement réfuté tous les arguments à propos des usages raisonnables et des droits d’utilisateurs prévus par le droit d’auteur, comme étant, en quelque sorte, des conséquences malheureuses de la nécessité d’éviter que Netflix n’abandonne le Web, au profit des applications. Quant au DMCA, ils ont répondu qu’ils ne pouvaient faire quoi que ce soit à propos de cette loi irrationnelle, mais qu’ils avaient la certitude que les membres du W3C n’avaient aucunement l’intention de violer le DMCA, ils voulaient seulement éviter que leurs films de grande valeur ne soient partagés sur Internet.

Nous avons donc changé de stratégie, et proposé une sorte d’expérience témoin afin de savoir ce que les fans de DRM du W3C avaient comme projets.

Le W3C est un organisme basé sur le consensus : il crée des standards, en réunissant des gens dans une salle pour faire des compromis, et aboutir à une solution acceptable pour chacun. Comme notre position de principe était « pas de DRM au W3C » et que les DRM sont une si mauvaise idée, il était difficile d’imaginer qu’un quelconque compromis pouvait en sortir.

Mais après avoir entendu les partisans du DRM nier leurs abus du DCMA, nous avons pensé que nous pouvions trouver quelque chose qui permettrait d’avancer par rapport à l’actuel *statu quo* et pourrait satisfaire le point de vue qu’ils avaient évoqué.

Nous avons proposé un genre de pacte de non-agression par DRM, par lequel les membres du W3C promettraient qu’ils ne poursuivraient jamais quelqu’un en justice en s’appuyant sur des lois telles que la DMCA 1201, sauf si d’autres lois venaient à être enfreintes. Ainsi, si quelqu’un porte atteinte à vos droits d’auteur, ou incite quelqu’un à le faire, ou empiète sur vos contrats avec vos utilisateurs, ou s’approprie vos secrets de fabrication, ou copie votre marque, ou fait quoique ce soit d’autre, portant atteinte à vos droits légaux, vous pouvez les attaquer en justice.

Mais si quelqu’un s’aventure dans vos DRM sans enfreindre aucune autre loi, le pacte de non-agression stipule que vous ne pouvez pas utiliser le standard DRM du W3C comme un moyen de les en empêcher. Cela protégerait les chercheurs en sécurité, cela protégerait les personnes qui analysent les vidéos pour ajouter des sous-titres et d’autres outils d’aide, cela protégerait les archivistes, qui ont légalement le droit de faire des copies, et cela protégerait ceux qui créent de

nouveaux navigateurs.

Si tout ce qui vous intéresse c'est de créer une technologie efficace contre les infractions à la loi, ce pacte ne devrait poser aucun problème. Tout d'abord, si vous pensez que les DRM sont une technologie efficace, le fait qu'il soit illégal de les critiquer ne devrait pas avoir d'importance.

Et étant donné que le pacte de non-agression permet de conserver tous les autres droits juridiques, il n'y avait aucun risque que son adoption permette à quelqu'un d'enfreindre la loi en toute impunité. Toute personne qui porterait atteinte à des droits d'auteur (ou à tout autre droit) serait dans la ligne de mire du DMCA, et les entreprises auraient le doigt sur la détente.

Pas surprenant, mais très décevant

Bien entendu, ils ont détesté cette idée.

Les studios, les marchands de DRM et les grosses entreprises membres du W3C ont participé à une « négociation » brève et décousue avant de voter la fin des discussions et de continuer. Le représentant du W3C les a aidés à éviter les discussions, continuant le travail sur la charte de EME sans prévoir de travail en parallèle sur la protection du Web ouvert, même quand l'opposition à l'intérieur du W3C grandissait.

Le temps que la poussière retombe, les EME ont été publiés après le vote le plus controversé que le W3C ait jamais vu, avec le représentant du W3C qui a déclaré unilatéralement que les problèmes concernant la sûreté des recherches, l'accessibilité, l'archivage et l'innovation ont été traités au mieux (malgré le fait que littéralement rien de contraignant n'a été décidé à propos de ces sujets). La recherche de *consensus* du W3C a été tellement détournée de son cours habituel que la publication de EME a été approuvée par seulement 58% des membres qui ont participé au vote final, et nombre de ces membres ont regretté d'avoir été acculés à voter pour ce à quoi ils avaient émis des objections.

Quand le représentant du W3C a déclaré que n'importe quelle protection pour un Web ouvert était incompatible avec les souhaits des partisans des DRM, cela ressemblait à une justification ironique. Après tout, c'est comme ça que l'on a commencé avec l'EFF insistant sur le fait que les DRM n'étaient pas compatibles avec les révélations de faille de sécurité, avec l'accessibilité, avec l'archivage ou

encore l'innovation. Maintenant, il semble que nous soyons tous d'accord.

De plus, ils se sont tous implicitement mis d'accord pour considérer que les DRM ne concernent pas la protection du droit d'auteur. Mais concerne l'utilisation du droit d'auteur pour s'emparer d'autres droits, comme celui de décider qui peut critiquer ou non votre produit – ou qui peut le concurrencer.

Le simulacre de cryptographie des DRM implique que ça marche seulement si vous n'êtes pas autorisé à comprendre ses défauts. Cette hypothèse s'est confirmée lorsqu'un membre du W3C a déclaré au consortium qu'il devrait protéger les publications concernant les « environnements de tests de confidentialité » des EME permettant l'espionnage intrusif des utilisateurs, et dans la minute, un représentant de Netflix a dit que cette option n'était même pas envisageable.

D'une certaine façon, Netflix avait raison. Les DRM sont tellement fragiles, tellement incohérents, qu'ils sont simplement incompatibles avec les normes du marché et du monde scientifique, où tout le monde est libre de décrire ses véritables découvertes, même si elles frustrent les aspirations commerciales d'une multinationale.

Le W3C l'a implicitement admis, car il a tenté de réunir un groupe de discussion pour élaborer une ligne de conduite à destination des entreprises utilisant l'EME : dans quelle mesure utiliser la puissance légale des DRM pour punir les détracteurs, à quel moment autoriser une critique.

« Divulgation responsable selon nos règles, ou bien c'est la prison »

Ils ont appelé ça *la divulgation responsable*, mais elle est loin de celle qu'on voit aujourd'hui. En pratique, les entreprises font les yeux doux aux chercheurs en sécurité pour qu'ils communiquent leurs découvertes à des firmes commerciales avant de les rendre publiques. Leurs incitations vont de la récompense financière (bug bounty), à un système de classement qui leur assure la gloire, ou encore l'engagement de donner suite aux divulgations en temps opportun, plutôt que de croiser les doigts, de s'asseoir sur les défauts fraîchement découverts et d'espérer que personne d'autre ne les redécouvrira dans le but de les exploiter.

La tension qui existe entre les chercheurs indépendants en sécurité et les grandes entreprises est aussi vieille que l'informatique. Il est difficile de protéger un ordinateur du fait de sa complexité. La perfection est inatteignable. Garantir la sécurité des utilisateurs d'ordinateurs en réseau nécessite une évaluation constante et la divulgation des conclusions, afin que les fabricants puissent réparer leurs bugs et que les utilisateurs puissent décider de façon éclairée quels systèmes sont suffisamment sûrs pour être utilisés.

Mais les entreprises ne réservent pas toujours le meilleur accueil aux mauvaises nouvelles lorsqu'il s'agit de leurs produits. Comme des chercheurs ont pu en faire l'expérience — à leurs frais — mettre une entreprise face à ses erreurs peut être une question de savoir-vivre, mais c'est un comportement risqué, susceptible de faire de vous la cible de représailles si vous vous avisez de rendre les choses publiques. Nombreux sont les chercheurs ayant rapporté un bogue à une entreprise, pour constater l'intolérable durée de l'inaction de celle-ci, laissant ses utilisateurs exposés au risque. Bien souvent, ces bogues ne font surface qu'après avoir été découverts par ailleurs par des acteurs mal intentionnés ayant vite fait de trouver comment les exploiter, les transformant ainsi en attaques touchant des millions d'utilisateurs. Bien trop nombreux pour que l'existence de bogues puisse plus longtemps être passée sous silence.

Comme le monde de la recherche renâclait de plus en plus à leur parler, les entreprises ont été obligées de s'engager concrètement à ce que les découvertes des chercheurs soient suivies de mesures rapides, dans un délai défini, à ce que les chercheurs faisant part de leurs découvertes ne soient pas menacés et même à offrir des primes en espèces pour gagner la confiance des chercheurs. La situation s'est améliorée au fil des ans, la plupart des grandes entreprises proposant une espèce de programme relatif aux divulgations.

Mais la raison pour laquelle les entreprises donnent des assurances et offrent des primes, c'est qu'elles n'ont pas le choix. Révéler que des produits sont défectueux n'est pas illégal, et donc les chercheurs qui mettent le doigt sur ces problèmes n'ont aucune obligation de se conformer aux règles des entreprises. Ce qui contraint ces dernières à faire preuve de leur bonne volonté par leur bonne conduite, des promesses contraignantes et des récompenses.

Les entreprises veulent absolument être capables de déterminer qui a le droit de dire la vérité sur leurs produits et quand. On le sait parce que, quand elles ont

une occasion d'agir en ce sens, elles la saisissent. On le sait parce qu'elles l'ont dit au W3C. On le sait parce qu'elles ont exigé ce droit comme partie intégrante du paquet DRM dans le cadre EME.

De tous les flops du processus DRM au sein du W3C, le plus choquant a été le moment où les avocats historiques du Web ouvert ont tenté de convertir un effort de protection des droits des chercheurs à avertir des milliards de gens des vulnérabilités de leurs navigateurs web en un effort visant à conseiller les entreprises quant au moment où renoncer à exercer ce droit. Un droit qu'elles n'ont que grâce à la mise au point des DRM pour le Web par le W3C.

Les DRM sont le contraire de la sécurité

Depuis le début de la lutte contre les DRM au W3C, on a compris que les fabricants de DRM et les entreprises de médias qu'elles fournissent n'étaient pas là pour protéger le droit d'auteur, mais pour avoir une base légale sur laquelle asseoir des privilèges sans rapport avec le droit d'auteur. On savait aussi que les DRM étaient incompatibles avec la recherche en sûreté : puisque les DRM dépendent de l'obfuscation (NdT: rendre illisible pour un humain un code informatique), quiconque documente comment les DRM marchent les empêche aussi de fonctionner.

C'est particulièrement clair à travers ce qui n'a pas été dit au W3C : quand on a proposé que les utilisateurs puissent contourner les DRM pour générer des sous-titres ou mener des audits de sécurité, les intervenants se demandaient toujours si c'était acceptable, mais jamais si c'était possible.

Il faut se souvenir que EME est supposé être un système qui aide les entreprises à s'assurer que leurs films ne sont pas sauvegardés sur les disques durs de leurs utilisateurs et partagés sur Internet. Pour que ça marche, cela doit être, vous savez, compliqué.

Mais dans chaque discussion pour déterminer quand une personne peut être autorisée à casser EME, il était toujours acquis que quiconque voulait le faire le pouvait. Après tout, si vous cachez des secrets dans le logiciel que vous donnez aux mêmes personnes dont vous voulez cacher les secrets, vous allez probablement être déçu.

Dès le premier jour, nous avons compris que nous arriverions à un point où les

défenseurs des DRM au W3C seraient obligés d'admettre que le bon déroulement de leur plan repose sur la capacité à réduire au silence les personnes qui examineront leurs produits.

Cependant, nous avons continué à espérer : une fois que cela sera clair pour tout le monde, ils comprendront que les DRM ne peuvent coexister pacifiquement avec le Web ouvert.

Nous avions tort.

Photo par Elitatt (CC BY 2.0)

Le canari dans la mine de charbon

Le succès des DRM au W3C est une parabole de la concentration des marchés et de la fragilité du Web ouvert. Des centaines de chercheurs en sécurité ont fait du lobbying au W3C pour protéger leur travail, l'UNESCO a condamné publiquement l'extension des DRM au Web, et les nombreuses crypto-monnaies membres du W3C ont prévenu que l'utilisation de navigateurs pour des applications critiques et sûres, par exemple pour déplacer les avoirs financiers des gens, ne peut se faire que si les navigateurs sont soumis aux mêmes normes de sécurité que les autres technologies utilisées dans nos vies (excepté les technologies DRM).

Il ne manque pas de domaines d'activités qui veulent pouvoir contrôler ce que leurs clients et concurrents font avec leurs produits. Quand les membres du

Copyright Office des États-Unis ont entendu parler des DRM en 2015, il s'agissait pour eux des DRM dans des implants médicaux et des voitures, de l'équipement agricole et des machines de votes. Des entreprises ont découvert qu'ajouter des DRM à leurs produits est la manière la plus sûre de contrôler le marché, une façon simple et fiable de transformer en droits exclusifs les choix commerciaux pour déterminer qui peut réparer, améliorer et fournir leurs produits .

Les conséquences néfastes sur le marché économique de ce comportement anticoncurrentiel sont faciles à voir. Par exemple, l'utilisation intempestive des DRM pour empêcher des magasins indépendants de réparer du matériel électronique provoque la mise à la poubelle de tonnes de composants électroniques, aux frais des économies locales et de la possibilité des clients d'avoir l'entière propriété de leurs objets. Un téléphone que vous recyclez au lieu de le réparer est un téléphone que vous avez à payer pour le remplacer – et réparer crée beaucoup plus d'emplois que de recycler (recycler une tonne de déchets électroniques crée 15 emplois, la réparer crée 150 emplois). Les emplois de réparateurs sont locaux et incitent à l'entrepreneuriat, car vous n'avez pas besoin de beaucoup de capital pour ouvrir un magasin de réparations, et vos clients voudront amener leurs objets à une entreprise locale (personne ne veut envoyer un téléphone en Chine pour être réparé – encore moins une voiture !).

Mais ces dégâts économiques sont seulement la partie émergée de l'iceberg. Des lois comme le DMCA 1201 incitent à l'utilisation de DRM en promettant de pouvoir contrôler la concurrence, mais les pires dommages des DRM sont dans le domaine de la sécurité. Quand le W3C a publié EME, il a légué au Web une surface d'attaque qu'on ne peut auditer dans des navigateurs utilisés par des milliards de personnes pour leurs applications les plus risquées et importantes. Ces navigateurs sont aussi l'interface de commande utilisée pour l'Internet des objets : ces objets, garnis de capteurs, qui peuvent nous voir, nous entendre, et agir sur le monde réel avec le pouvoir de nous bouillir, geler, électrifier, blesser ou trahir de mille façons différentes.

Ces objets ont eux-mêmes des DRM, conçus pour verrouiller nos biens, ce qui veut dire que tout ce qui va de votre grille-pain à votre voiture devient hors de portée de l'examen de chercheurs indépendants qui peuvent vous fournir des évaluations impartiales et sans fard sur la sécurité et de la fiabilité de ces appareils.

Dans un marché concurrentiel, on pourrait s'attendre à ce que des options sans DRM prolifèrent en réaction à ce mauvais comportement. Après tout, aucun client ne veut des DRM : aucun concessionnaire automobile n'a jamais vendu une nouvelle voiture en vantant le fait que c'était un crime pour votre mécanicien préféré de la réparer.

Mais nous ne vivons pas dans un marché concurrentiel. Les lois telles que DMCA 1201 minent toute concurrence qui pourrait contrebalancer leurs pires effets.

Les entreprises qui se sont battues pour les DRM au W3C – vendeurs de navigateurs, Netflix, géants de la haute technologie, l'industrie de la télévision par câble – trouvent toutes l'origine de leur succès dans des stratégies commerciales qui ont, au moment de leur émergence, choqué et indigné les acteurs du secteur déjà établis. La télévision par câble était à ses débuts une activité qui retransmettait des émissions et facturait ce service sans avoir de licence. L'hégémonie d'Apple a commencé par l'extraction de cédéroms, en ignorant les hurlements de l'industrie musicale (exactement comme Firefox a réussi en bloquant les publicités pénibles et en ignorant les éditeurs du web qui ont perdu des millions en conséquence). Bien sûr, les enveloppes rouges révolutionnaires de Netflix ont été traitées comme une forme de vol.

Ces boîtes ont démarré comme pirates et sont devenus des amiraux, elles traitent leurs origines comme des légendes de courageux entrepreneurs à l'assaut d'une structure préhistorique et fossilisée. Mais elles traitent toute perturbation à leur encontre comme un affront à l'ordre naturel des choses. Pour paraphraser Douglas Adams, toute technologie inventée pendant votre adolescence est incroyable et va changer le monde ; tout ce qui est inventé après vos 30 ans est immoral et doit être détruit.

Leçons tirées du W3C

La majorité des personnes ne comprennent pas le danger des DRM. Le sujet est bizarre, technique, ésotérique et prend trop de temps à expliquer. Les partisans des DRM veulent faire tourner le débat autour du piratage et de la contrefaçon, qui sont des histoires simples à raconter.

Mais les promoteurs des DRM ne se préoccupent pas de ces aspects et on peut le prouver : il suffit de leur demander s'ils seraient partants pour promettre de ne

pas avoir recours au DMCA tant que personne ne viole de droit d'auteur. On pourrait alors observer leurs contorsions pour ne pas évoquer la raison pour laquelle faire appliquer le droit d'auteur devrait empêcher des activités connexes qui ne violent pas le droit d'auteur. À noter : ils n'ont jamais demandé si quelqu'un pourrait contourner leurs DRM, bien entendu. Les DRM sont d'une telle incohérence technique qu'ils ne sont efficaces que s'il est interdit par la loi de comprendre leur fonctionnement. Il suffit d'ailleurs de les étudier un peu attentivement pour les mettre en échec.

Demandez-leur de promettre de ne pas invoquer le DMCA contre les gens qui ont découvert des défauts à leurs produits et écoutez-les argumenter que les entreprises devraient obtenir un droit de veto contre la publication de faits avérés sur leurs erreurs et manquements.

Ce tissu de problèmes montre au moins ce pour quoi nous nous battons : il faut laisser tomber les discussions hypocrites relatives au droit d'auteur et nous concentrer sur les vrais enjeux : la concurrence, l'accessibilité et la sécurité.

Ça ne se réglera pas tout seul. Ces idées sont toujours tordues et nébuleuses.

Voici une leçon que nous avons apprise après plus de 15 ans à combattre les DRM : il est plus facile d'inciter les personnes à prêter attention à des problèmes de procédure qu'à des problèmes de fond. Nous avons travaillé vainement à alerter le grand public sur le *Broadcasting Treaty*, un traité d'une complexité déconcertante et terriblement complexe de l'OMPI, une institution spécialisée des Nations Unies. Tout le monde s'en moquait jusqu'à ce que quelqu'un dérobe des piles de nos tracts et les dissimule dans les toilettes pour empêcher tout le monde de les lire. Et c'est cela qui a fait la Une : il est très difficile de se faire une idée précise d'un truc comme le *Broadcast Treaty*, mais il est très facile de crier au scandale quand quelqu'un essaie de planquer vos documents dans les toilettes pour que les délégués ne puissent pas accéder à un point de vue contradictoire.

C'est ainsi qu'après quatre années de lutte inefficace au sujet des DRM au sein du W3C, nous avons démissionné ; c'est alors que tout le monde s'est senti concerné, demandant comment résoudre le problème. La réponse courte est « Trop tard : nous avons démissionné, car il n'y a plus rien à faire ».

Mais la réponse longue laisse un peu plus d'espoir. EFF est en train d'attaquer le gouvernement des États-Unis pour casser la Section 1201 du DMCA. Comme on

l’a montré au W3C, il n’y a pas de demande pour des DRM à moins qu’il y ait une loi comme le DMCA 1201. Les DRM en soi ne font rien d’autre que de permettre aux compétiteurs de bloquer des offres innovantes qui coûtent moins et font plus.

Le Copyright Office va bientôt entendre des nouveaux échos à propos du DMCA 1201.

Le combat du W3C a montré que nous pouvions ramener le débat aux vrais problèmes. Les conditions qui ont amené le W3C à être envahi par les DRM sont toujours d’actualité et d’autres organisations vont devoir faire face à cette menace dans les années à venir. Nous allons continuer à affiner notre tactique et à nous battre, et nous allons aussi continuer à rendre compte des avancées afin que vous puissiez nous aider. Tout ce que nous demandons est que vous continuiez à être vigilant. Comme on l’a appris au W3C, on ne peut pas le faire sans vous.