

Internet du futur : performances et respect de la vie privée

Claude Castelluccia, Vincent Roca, Françoise Breton

► **To cite this version:**

Claude Castelluccia, Vincent Roca, Françoise Breton. Internet du futur : performances et respect de la vie privée. Collection "20 ans d'avancées et de perspectives en sciences du numérique", INRIA, 2012, 3 p. <hal-00812734>

HAL Id: hal-00812734

<https://hal.inria.fr/hal-00812734>

Submitted on 12 Apr 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Internet du futur : performances et respect de la vie privée



Protection de la vie privée sur terminal mobile - © Inria /
Photo H. Raguét

Les internautes sont de plus en plus courtisés par un e-commerce fleurissant. S'ils bénéficient déjà, pour certains, de la télévision en *streaming* sur des terminaux mobiles comme les *Smartphones*, ils sont aussi activement profilés à des fins publicitaires. Impossible aujourd'hui de penser l'Internet et les terminaux mobiles sans se préoccuper de leur fiabilité, de leur sécurité et de la préservation de la vie privée.

Avec le développement de l'e-commerce sont nées les préoccupations sur les atteintes à la vie privée sur le Web

Témoignage de Claude Castelluccia, responsable de l'équipe Privatics

L'essor de l'économie sur Internet a bouleversé le domaine de la protection de la vie privée.

Il y a 20 ans, on utilisait de façon anonyme Internet, ce qu'avait croqué un dessinateur satirique, Peter Steiner, dans le *New Yorker*, par un chien discutant avec un autre devant un ordinateur « *Ce qui est bien avec Internet, c'est que personne ne sait que nous sommes des chiens* ».

Aujourd'hui, c'est loin d'être le cas. Grâce à des systèmes de graphes et de recoupements de bases de données, des entreprises comme *Google* ou *FaceBook*, savent énormément de choses sur les internautes : leur âge, leur sexe, leur adresse, sur quels sites et à quels endroits réels (par géo-localisation) ils sont allés, avec quelles personnes ils ont eu des contacts, etc. Ces données sont vendues aux publicitaires ; elles sont, soit disant, le prix payé à leur insu par les internautes pour obtenir des services gratuits.

Depuis 5 à 6 ans, les chercheurs s'intéressent à ces questions, à la fois pour mieux comprendre comment fonctionnent ces systèmes d'extorsion de données privées et pour trouver des algorithmes d'anonymisation présentant de fortes garanties de sécurité, par exemple en ajoutant du bruit de fond dans les grandes bases de données. C'est un domaine émergent et difficile car il est éminemment pluridisciplinaire, nécessitant des compétences en réseaux, sécurité et cryptographie mais aussi en sciences juridiques et sociales, et avec de fortes implications politiques.



Source : Wikipedia - *The New Yorker* -
Peter Steiner

L'équipe Privatics est la première dédiée à ce thème dans l'institut, à la fois pour alermer en cas de dérive et pour proposer des solutions. Par exemple, afin de mieux gérer la production et la distribution d'électricité, EDF veut installer des compteurs intelligents qui relèvent la consommation électrique des ménages toutes les 5 minutes. De quoi tout connaître sur votre vie quotidienne ! Quand vous êtes là, quand vous vous levez ou prenez une douche, etc. Pourtant, même si cela est un peu plus compliqué à mettre en œuvre, le suivi de la consommation à l'échelle d'un quartier est suffisante. Nous avons par ailleurs élaboré avec la Cnil une plateforme de test permettant de surveiller les applications sur *Smartphone* car nous nous sommes aperçus que beaucoup d'entre elles récupèrent des données personnelles, comme la liste des contacts. L'objectif est de développer des logiciels capables de prévenir l'utilisateur de qui cherche à obtenir quelles données et de lui donner la possibilité d'autoriser ou non ce transfert.

Internet : de l'échange point à point à la diffusion large échelle

Témoignage de Vincent Roca, membre de l'équipe Privatics

Si aujourd'hui, dans certains pays, on peut recevoir la télévision en *streaming*, ainsi que des guides de programmes et divers contenus multimédias sur un *Smartphone*, c'est grâce à des règles particulières de transmission définies par un protocole mis

au point au cours de ces dix dernières années. Un tel système est indispensable car les réseaux ne sont pas parfaits : il y a des pertes d'information lors des transmissions.

Jusqu'au début des années 2000, les protocoles permettaient d'assurer la fiabilité des transmissions sur Internet en instaurant un dialogue permanent entre émetteurs et récepteurs : chaque arrivée d'un paquet d'information était suivi d'un accusé de réception et une retransmission avait lieu en absence de confirmation de bonne réception. Mais avec l'essor des terminaux mobiles, de nouveaux besoins de transmission ont émergés, soutenus par de forts enjeux économiques : comment diffuser des contenus multimédias, souvent volumineux, à des millions d'utilisateurs simultanément ?

Impossible dans ce cas de s'appuyer sur un dialogue incessant entre récepteurs et émetteurs ! Il fallait redéfinir les règles de transmission, un travail auquel nous avons largement contribué et qui a abouti à l'adoption du standard Flute par l'IETF, l'organisme de standardisation de l'Internet.

Nous avons également travaillé sur un composant essentiel, le code correcteur d'erreur, qui ajoute un peu de redondance aux envois afin de permettre aux récepteurs de retrouver l'information perdue, évitant ainsi d'engorger le réseau avec des retransmissions. J'ai également développé la première implémentation de Flute qui a été commercialisée par la PME française Expway et déployée de façon opérationnelle pour la première fois à l'occasion du mondial de foot en Italie en 2006.

Flute et codes correcteurs d'erreur ont été intégrés à d'autres standards par la suite, notamment en 2012 au Japon. C'est une reconnaissance de l'excellence française dans ce domaine.

ET DANS 20 ANS ?

Claude Castelluccia, directeur de recherche, responsable de l'équipe Privatics



Photo Philippe Trannoy

« Je suis inquiet car les motivations économiques priment aujourd'hui largement sur la vie privée, et les motivations sécuritaires vont dans le même sens en justifiant une surveillance de plus en plus étroite des citoyens. Il faut espérer que des lois veilleront à protéger la vie privée sur le web. Je vois aussi avec inquiétude le déploiement de technologies informatiques présentant de faible niveau de sécurité : le réseau des voitures peut être attaqué, tout comme les implants médicaux du type *pacemakers* ou les télévisions. La recherche dans ce domaine est vital et, à mon avis, une mission importante pour un centre de recherche publique comme Inria, sans compter les implications géo-politiques qui sont considérables ! L'équipe Privatics a largement de quoi s'occuper pour les 20 ans à venir.... Je propose que l'on refasse un point en 2032 pour voir comment la situation aura évolué ! »

Vincent Roca, chercheur, équipe Privatics



© Vincent Roca

« Mon rêve est d'arriver à imposer des solutions libres et ouvertes, afin que les recherches de la communauté scientifique puissent être exploitées et donner lieu à de nombreuses innovations. Un autre souhait est que nos solutions continuent à être déployées commercialement car les enjeux économiques sont énormes et porteurs d'emplois. Notre travail a été soutenu par l'état et par Inria, j'ai à cœur qu'en retour ce travail soit valorisé en France. »

Dates clés

- **2005** : premier scandale ayant donné lieu à poursuites judiciaires: le système anti-piratage de Sony installe un logiciel espion sur l'ordinateur communiquant à Sony l'adresse IP de l'utilisateur et le CD écouté
- **2006** : AOL met à disposition des chercheurs un fichier de 20 millions de requêtes émises par 65 000 utilisateurs sur une période de 3 mois. En moins de 3 jours ce fichier a été désanonymisé: certains utilisateurs ont été identifiés.
- **2010** : Facebook reconnaît que les données personnelles de ses 10 applications les plus répandues sont vendues à des publicitaires ; la Cnil envoie aux 40 000 classes de CM2 des exemplaires d'une édition spéciale de "Mon Quotidien" sur le thème "Protège ta vie privée sur Internet"
- **2011** : Google street views est soumis à une amende de 100 000 euros par la Cnil et est en bute à de nombreuses plaintes pour atteintes à la vie privée en Suisse, Belgique, Allemagne, Corée du Sud, etc. ; Apple est critiqué pour conserver la trace des déplacements des utilisateurs d'iPhone et d'iPad
- **2012**: création de PRIVATICS, la première équipe Inria consacrée à la protection de la vie privée sur Internet.

Numérique & société

- **septembre 2000** : Amazon est accusée de moduler les prix de ventes des articles proposés en fonction du profil individuel de ses utilisateurs

Source : Rapport CNIL "La publicité en ligne" (février 2009)

- **mars 2005** : Lancement de la télévision numérique terrestre (TNT). La TNT exploite les normes DVB-T, MPEG-2 pour la résolution d'image standard et H.264 pour la « haute définition ». Elle a achevé son déploiement le 29 novembre 2011 pour couvrir aujourd'hui plus de 97 % de la population.

Source : ddm.gouv.fr

- **mai 2009** : Le Sénat publie 15 recommandations dans son étude sur "La vie privée à l'heure des mémoires numériques"

Source : senat.fr

1992 - 2012



- Collection "20 ans d'avancées et de perspectives en sciences du numérique" par les chercheurs d'équipes Inria de Grenoble et Lyon.

- www.inria.fr/20ansgrenoble

© Inria - Editions
Victoria