http://www.droit-technologie.org

Présente :

Les risques majeurs de IPv6 pour la protection des données à caractère personnel

Jean-Marc Dinant
Informaticien expert pour la Commission de Protection de la Vie Privée
Directeur de Recherches au Centre de Recherche Informatique et Droit (CRID)
jean-marc.dinant@fundp.ac.be

Date de mise en ligne : 7 novembre 2001

1.1 Introduction

1. En organisant à Paris la 22ème conférence mondiale des Commissaires à la Protection des Données, la Commission Nationale Informatique et Libertés a judicieusement choisi de consacrer un atelier entier sur le thème "*les technologies pour la protection de la vie privée*". Pour sa part, cette intervention tentera de répondre à la question *: "les technologies : pour la protection de la vie privée ?*". Avant de tenter d'évaluer la manière dont la technologie peut protéger la vie privée, un préalable indispensable semble être d'analyser en quoi, pourquoi et comment les technologies déployées sur Internet sont "**privacides**[1]". Avant de répondre à cette question, deux remarques préliminaires s'imposent.

2. La technologie n'est pas, comme la météo, un obscur résultat de forces collossales et célestes, imprévisibles à long terme et non réglementables. La technologie Internet constitue toujours le fruit de l'interaction entre des forces sociales et finalement très humaines d'entreprises industrielles souvent multinationales, relativement prévisibles et légalement réglementables, voire reglementées.

3. L'industrie Internet produit non seulement du matériel et du logiciel mais aussi des protocoles de télécommunication. Actuellement, en Europe, la production et l'exportation ou l'importation de matériel, logiciel ou protocoles Internet ne sont pas soumises, en tant que tel, à une réglementation légale. La directive générale de 1995 vise en effet les utilisateurs de la technologie, mais non ses concepteurs ou ses vendeurs. Bizarrement, semblable réglementation légale se retrouve néanmoins aux Etats-Unis, lorsqu'il s'agit d'exporter du matériel ou du logiciel cryptographique susceptibles de protéger la vie privée des internautes[2]. Paradoxalement, la Chine a interdit l'importation des processeurs Intel Pentium III , susceptibles de menacer la vie privée des internautes gouvernementaux[3]

4. Durant plusieurs années, l'auteur de cet article a étudié de manière directe et technique de nombreux aspects privacides de la technologie Internet. Il est impossible d'en faire un exposé détaillé dans le cadre de cette intervention. Mais quelques jalons sommaires peuvent être posés.

---

[1] A comprendre comme insecticide ou paricide : tueur de vie privée. L'auteur a osé ce néologisme dès 1999 afin de ne rien perdre de la force du mot anglais "privacy killing". (Voir http://www.droit.fundp.ac.be/Textes/revuegeneralejmd.rtf, note 1 http://www.cecurity.com/cecurity/html/citation_du_mois.html)

[2] "*NSA provides the Department of State with technical advice to determine whether the commodity is a cryptographic system, equipment, assembly, module, integrated circuit, component or software "with the capability of maintaining secrecy or confidentiality of information*" covered under Category XIII(b)(1) of the United States Munitions List ("USML"). 22 C.F.R. § 121.1, XIII(b)(1). Cfr http://people.qualcomm.com/karn/export/crowell.html, visité en août 2001.

[3] Guangming Daily newspaper, Wednesday, June 30, 1999 disponible sur http://jya.com/cn-p3-peril.htm. dernière visite en août 2001.

1.2 De quelques technologies privacides (Privacy Killing Technologies)

1.2.1 Les cookies

5. Les cookies sont l'objet d'une controverse depuis de nombreuses années. Ce débat s'apparente à un véritable dialogue de sourds pour de nombreuses raisons. Le grand public fait rarement la différence entre :

   - les cookies de session qui demeurent quelques minutes dans la mémoire vive de l'ordinateur et les cookies permanents qui sont stockés pendant plusieurs (dizaines d') années sur le disque dur;

   - les cookies indiquant une caractéristique (p.e. la langue parlée) d'un internaute anonyme et les cookies contenant un identifiant global universel[4]

   - les cookies issus du site visité et les cookies injectés via un hyperlien invisible par une firme de cybermarketing qui l'est tout autant

6. Outre ces trois distinctions, le phénomène des cookies ne peut être correctement appréhendé que si on le resitue dans le contexte plus large du protocole HTTP où il se développe. Quatre caractéristiques largement méconnues du protocole HTTP peuvent elles-aussi s'avérer privacides : le bavardage du programme de navigation, les hyperliens invisibles et la redirection automatique. Ces quatres éléments mis ensemble forment un cocktail explosif qui permet

   - par défaut[5]

   - à des entreprises multinationales de cybermarketing inconnues de l'utilisateur[6]

   - d'enregistrer les mots-clés tapés sur les moteurs de recherche ou les références des articles lus dans les journaux en ligne

   - en temps réel[7]

   - sur une base individuelle à l'aide d'un identificateur unique global

---

[4] Global Unique Identifier (GUID). Tel le cookie attribué par Double Click

[5] Les ingénieurs et utilisateurs avertis pourront facilement trouver sur le réseau des milliers de programmes divers permettant, dans le meilleur des cas, de se protéger gratuitement. Dans le monde réel, il est aussi possible de porter un gilet pare balles et/ou un masque à gaz et de rouler dans une voiture blindée flanquée de quelques garde du corps. Privacy for the clever and for the rich ?

[6] L'exemple type est bien évidemment Double Click qui produisait en 2000 plus d'un demi-milliard de bannières publicitaires sur le réseau chaque mois.

[7] Techniquement, l'entreprise de cybermarketing connaît le profil de l'internaute AVANT de transmettre la bannière

- programmé pour durer jusqu'en 2035
- plusieurs millions de fois par jour rien qu'en France

1.2.2 Le second clic

7. C'est le programme de navigation qui est programmé depuis de nombreuses années pour télécharger, sur le compte de l'internaute des bannières non sollicitées. Le premier clic c'est celui que l'internaute fait de manière consciente pour obtenir de l'information d'un site en cours de visite. Le second clic est effectué par le programme de navigation lui-même, vers un site invisible, inconnu et pas nécessairement européen, au nez à la barbe de l'utilisateur et lui raconte moult détails du comportement de ce dernier.

1.2.3 La responsabilité des fabricants de logiciel

8. Les caractéristiques privacides du protocole HTTP 1.1 ne sont pas intrinsèques au protocole lui-même. Bien plus, durant la définition de ce protocole technique[8], les ingénieurs ont mis l'accent les dangers pour la vie privée que représentaient telle ou telle option du protocole. En effet, le mot "privacy" n'intervient pas moins de 18 fois dans ce protocole pourtant technique, qui n'aborde pas le problème des cookies. En voici quelques extraits[9] choisis :

   - "*Having the user agent describe its capabilities in every request can be both very inefficient (given that only a small percentage of responses have multiple representations) and a potential violation of the user's privacy*" [page 68 below]
   - " *It may be contrary to the privacy expectations of the user to send an Accept-Language header with the complete linguistic preferences of the user in every request*" [page 98]
   - *" The client SHOULD not send the From header[10] field without the user's approval, as it may conflict with the user's privacy interests or their site's security policy. It is strongly recommended that the user be able to disable, enable, and modify the value of this field at any time prior to a request*." [page 118]
   - "*HTTP clients are often privy to large amounts of personal information (e.g. the user's name, location, mail address, passwords, encryption keys, etc.), and SHOULD be very careful to prevent unintentional leakage of this information via the HTTP protocol to other sources. We very strongly recommend that a convenient interface be provided for the user to control dissemination of such information, and that designers and implementers be particularly careful in this area. History shows that errors in this area are often both serious security and/or privacy problems, and often generate highly adverse publicity for the implementer's company*." [page 143]

   Est-il utile de noter qu'aucun des "grands" fabriquants[11, 12]de logiciels de navigation Internet n'a pris en ligne de compte ces recommandations ?

8

9 The page numbering indicated between brackets refer to the numeration of W3C.

10 Note of the author : From header field is used for naming the referring page

11 Le navigateur Opéra version 3 et 4 permet à l'internaute de bloquer l'envoi de la page référente

12 Mozilla (http://www.mozilla.org) , navigateur open source (Netscape like) permet de bloquer le téléchargement d'images issues de sites tiers au site en cours de visite

9. La conclusion de la page 143 rappelle la phrase devenue historique qui se trouve encore actuellement sur la page de bienvenue du site de bigbrotherinside[13], à propos du numéro de série du processeur d'Intel : "*L'avantage que ce numéro de série aurait pu nous procurer dans le domaine de la sécurité n'était pas suffisant pour contrebalancer la mauvaise réputation que cela nous aurait donné*". Bruce Schneier, un cryptographe de renommée mondiale, aurait pour sa part déclaré : "*As a cryptographer, I cannot design a secure system to validate identification, enforce copy protection, or secure e-commerce using a processor ID. It doesn't help. It's just too easy to hack.*[14]"

1.2.4 Les firmes de mauvaise réputation

10. Historiquement, c'est cette mauvaise réputation et uniquement elle qui, jusqu'à présent, a incité avec succès les producteurs de logiciels à modifier les aspects privacides. Quelques évènements historiques méritent d'être rappelés :

    - Au début du mois de mars 1999, le NY Times rapportait que un identificateur spécidifque appelé identificateur global unique était systématiquement incorporé dans chaque document Word, Excel ou Powerpoint97 [15] [16]. En fait, cet identificateur global unique est basé sur le numéro de série de la carte réseau[17]. En réponse, le 8 mars 1999, Microsoft a publié sur son site Web[18] deux programmes. Ceux-ci permettent, respectivement d'éviter que ce numéro soit incorporé dans de nouveaux documents et d'effacer ces numéros de série des documents existants[19]. Simultanément, Microsoft a annoncé que la suite bureautique Office 2000 n'insérerait plus cet identificateur global unique dans ses documents.

    - C'est la pression populaire qui a (?) empêché la fusion entre les banques de données d'Abacus[20] et de Double Click. Au passage, on ne peut d'ailleurs que s'étonner que la fusion entre les profils "anonymes[21]" de Double Click et la banque de données nominatives d'Abacus soit techniquement possible.

    - En juillet 1999, Richard Smith un consultant en sécurité a mis en évidence que RealJukebox, un logiciel gratuit d'écoute de CD musicaux diffusé en Europe à des millions d'exemplaires transmettait à la maison mère américaine, de manière cryptée

---

13 http://www.bigbrotherinside.org

14 Cited in http://www.zdnet.com/zdnn/stories/comment/0,5859,2194863,00.html

15 http://www.junkbusters.com/ht/en/microsoft.html#history

16 http://www.techserver.com/noframes/story/0,2294,25591-41382-304399-0,00.html

17 Plus précisément sur l'adresse MAC (Medium Access Control) de la carte Ethernet

18 http://www.microsoft.com/PressPass/features/1999/03-08custletter2.asp

19 Notons au passage que l'utilisation de ces outils nécessite dans certains cas une mise-à-jour de Windows 95, en téléchargeant plus de trente millions d'octets sur le site de Microsoft

20 a *cooperative membership database, contains records from more than 1,100 merchandise catalogs, with more than 2* ***billion*** *consumer transactions from virtually all U.S. consumer catalog buying households* http://www.abacus-direct.com

21 http://www.doubleclick.net/company_info/about_doubleclick/privacy : " *DoubleClick does not collect any personally-identifiable information about you, such as your name, address, phone number or email address.*

et à intervalles réguliers les index des CDROM qui étaient insérés dans le lecteur du PC[22]. Cet événement a mis en évidence l'existence de ET software[23].

1.3 Les numéros IP version 4 (Ipv4)

11. Tout réseau de télécommunication, qu'il s'agisse du réseau téléphonique ou du réseau Internet, nécessite l'attribution de numéros uniques à l'échelle mondiale. Sur Internet ce numéro qui identifie une machine particulière au niveau mondial est l'adresse IP (Internet Protocol). Historiquement, ce numéro a toujours été composé de quatre octets, ce qui permet d'identifier plus de quatre milliards de machines distinctes. Chaque internaute présent sur Internet peut donc être identifié par ce numéro unique.

12. Ce numéro IP peut-être attribué de manière **permanente** à une machine si celle-ci est reliée à un réseau local lui-même connecté de manière permanente à Internet, ou dans le cas des connexions de type DSL que ce soit via le fil téléphonique ou par le câble de télédistribution. Ce premier cas peut-être comparé à celui de l'abonné au télephone qui conserve le même numéro durant toute la durée de son abonnement.

13. Ce numéro IP peut être également attribué de façon **dynamique**, notamment lorsque l'abonné d'un fournisseur d'accès Internet se connecte au réseau Internet par le biais d'un modem téléphonique pour une session de durée limitée (quelques minutes, voire plusieurs heures). Lors des sessions ultérieures, le même internaute se verra attribuer par le même fournisseur d'accès un numéro IP différent du précédent. Cette situation peut-être comparée à celle d'une personne ne disposant pas d'un abonnement téléphonique et n'utilisant que des cabines téléphoniques et rarement les mêmes.

14. Toutefois, contrairement au réseau téléphonique[24], *il n'y a pas, sur le réseau Internet de moyens simples de masquer le numéro d'appel de la machine appelante*. La seule solution actuelle consiste à passer par un tiers de confiance (anonymiseur) qui masquera cette adresse IP au réseau en y substituant la sienne. Les procédés d'anonymisation restent toutefois globalement peu fiables, ralentissent le fonctionnement du réseau et nécessitent en général un paiement.

---

[22] http://www.thatworld.com/news/realjukebox.html

[23] L'image, extraite du film de *Steven Spielberg* est parlante. L'extraterrestre ET "téléphone" en cachette de temps en temps à la maison, pour raconter ce qui s'est passé sur la terre. Un *ET software* est donc un programme qui communique *via* Internet des détails sur le comportement de son utilisateur. Un exemple célèbre est le cas de *RealJukeBox Player*, *software* d'écoute de CD musicaux diffusé à plus de treize millions d'exemplaires qui rapportait régulièrement à la société mère (*RealNetworks*) le détails de CD insérées dans le lecteur, de manière encryptée, <http://www.tiac.net/users/smiths/privacy/realjb.htm>. À la suite d'un article paru dans le *New York Times*, *RealNetworks* a modifié son logiciel.

[24] Au niveau technique, ce numéro d'appel est TOUJOURS transmis sur les réseaux numérisés. Si le numéro est censé être secret, un bit particulier indiquera qu'il ne pourra être révélé (SIC).

1.4 Les numéros IP version 6 (Ipv6)

15. Pour des raisons techniques, il semble que cet espace de quatre milliards d'adresses soit proche de la saturation. La structure de cette addresse IP est donc en train de se modifier et sera notamment portée de 4 octets à 16 octets. Dans ces 16 octets, le protocole Ipv6 recommande que 6 de ces 16 octets soient constitués par le numéro de série électronique de la carte réseau Ethernet présente sur l'ordinateur personnel. Ce numéro de série (addresse MAC (Medium Access Control)) est un numéro unique au monde gravé dans l'électronique de la carte réseau de type Ethernet, le standard pour constituer des réseaux locaux connectés à Internet. Ce numéro de série posait un problème de vie privée auparavant mais restait normalement interne au réseau local et n'était pas transmis sur le réseau Internet.

16. Avec le déploiement de la nouvelle numérotation Ipv6, chaque machine et donc chaque internaute, transmettra, le plus souvent à son insu, et sans qu'il puisse s'y opposer, un numéro de série unique au monde et stable dans le temps. Ce numéro sera transmis quelque soit le service utilisé sur Internet : envoi de courrier électronique, forums de discussion, accès aux moteurs de recherche (pour chercher les horaires des offices des mosquées, l'adresse d'un syndicat, du viagra ou des traitements pour guérir le sida, pour lire certains articles des journaux en ligne, etc.

17. Avec Ipv6, il n'y a plus de différence, au regard de la protection des données, entre l'attribution statique ou dynamique, pour la simple raison que le numéro de série MAC sera toujours une partie de l'adresse IP, quelque soit le fournisseur d'accès Internet

18. Le tableau ci-dessous montre l'importance de ce numéro par rapport à quelques risques plus classiques qui ont déjà été identifiés. Tous ces risques concernent la transmission sur le réseau d'un numéro unique au monde[25]. Ce tableau décrit la situation par défaut de "l'internaute de la rue". Il est clair que les "riches" et les "malins" qui en savent d'avantage peuvent se protéger bien mieux.

Tableau 1. Privacy scoring de quelques technologies privacides

Nom	*% intern. concernés*[26]	*Durée de vie moyenne*	*Infor-mation*	*Oppo-sition*	*Transmission à tout tiers*	*Transmission à un tiers*
Processor Number	40↓↓	**Celle de l'ordinateur**	Oui	Oui	Non	Oui
Microsoft GUID	40↓↓	Celle du document	Non	Non Oui	Non	Oui
Cookie de session	100→	+/- 20 minutes	Non	Non	Non	Oui
Ipv4 dynamique	50↓	Minutes ou heures	Non	Non	**Oui**	Oui
Cookie permanent	98↓	**Celle de l'ordinateur**	Non	Non	Non	Oui[27]

[25] Durant sa durée de vie, numéro unique identifiant un ordinateur par rapport à un tiers.
[26] Cette estimation a été faite ex æquo et bono.

Ipv4 permanent	50↓	Qqs mois ou années	Non	Non	**Oui**	Oui
MAC Address	90↑	**Celle de la carte réseau**	Non	Non	Non	Non
Ipv6 permanent	↑↑	**Celle de l'ordinateur**	Non	Non	**Oui**	Oui
Ipv6 dynamique	↑↑	**Celle de l'ordinateur**	Non	Non	**Oui**	Oui

Vert : Pas ou peu privacide ou en cours de résolution.
Rouge : Privacide. A éviter si possible.
Noir : Hautement privacide. A éviter à tout prix.

1.4.1 Les leçons non apprises de l'histoire

19. Chacun gardera en mémoire l'histoire du PSN d'Intel, qui a d'ailleurs rencontré le Groupe 29 à ce sujet en 1998[28]. Sous la pression populaire (http://www.bigbrotherinside.com), Intel, un géant de l'industrie du hardware Internet, a du faire marche arrière et a supprimé ce numéro de série en 2000. Microsoft a du faire la même marche arrière lors de la découverte de l'incorporation de ce fameux numéro MAC dans chaque document Word, Excel ou Powerpoint 97.

20. Dans le cadre d'IPv6, l'enjeu est sans commune mesure avec le PSN d'intel ou le GUID de Microsoft. Il ne s'agit plus de doter une version d'un processeur d'une marque particulière ou certains documents d'un numéro de série qui, dans certains cas et parfois avec l'accord de la personne concernée peut être transmis sur le réseau. Il s'agit présentement de d'incorporer de manière systématique dans toutes les communications Internet un numéro de série présent sur la grande majorité des ordinateurs personnels, sans que la personne concernée n'en soit informée, ni, a fortiori, ne puisse s'y opposer.

1.5 Conclusions et recommandations

1.5.1 L'interdiction des identifiants globaux uniques (GUID)

21. Au regard de la protection des données, l'utilisation des identifiants globaux universels (GUID) doit être systématiquement interdite. Elle contrevient de manière évidente aux principes élementaires de sécurité contenus dans les articles 16 et 17 de la directive générale 95/46. Si deux traitements poursuivent des finalités différentes voire incompatibles, il doit être rendu aussi techniquement difficile que possible d'effectuer un

---

[27] Il est possible de partager un cookie entre plusieurs ordinateurs serveurs du même sous domaine.
[28] C'est dans ce contexte que le Groupe 29 a produit la recommandation sur les traitements invisibles effectués par hardware ou par software (http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp17fr.pdf)

rapprochement entre les données d'un individu inscrit dans ces deux traitements. Une mesure **élémentaire** de sécurité propre à prévenir ce rapprochement non autorisé est de doter un même individu d'identifiants différents selon le traitement auquel il participe. Ceci est spécialement vrai lorsqu'un ou plusieurs des traitements en question poursuit une finalité sensible, judiciaire ou médicale. Le responsable de traitement qui manque à cette obligation élémentaire de sécurité contrevient aux articles 16 et 17 de la directive. Dans les cas ou des rapprochements ponctuels doivent être possibles au cas par cas, il convient que cet identifiant unique soit encrypté[29] à l'aide d'une clé secrète propre à chaque responsable de traitement et à chaque traitement. De cette manière, semblable rapprochement ne peut techniquement être réalisé qu'avec le consentement des des responsables de traitement concernés.

1.5.2 La suppression du numéro MAC

22. Le numéro identifiant de la carte Ethernet était jusqu'il y a peu un GUID relativement peu privacide dans la mesure où ce numéro de série restait local au niveau d'un intranet et n'était pas relayé au delà d'un routeur, passerelle classique entre un réseau local et Internet. Toutefois la présence de ce numéro unique au monde a déjà provoque le dérapage évoqué ci-dessus dans la mesure où il fut incorporé de manière clandestine par Microsoft dans tous les documents Word, Excel ou Powerpoint 97. Rien, au niveau technique, ne justifie l'unicité, au niveau mondial de ce numéro. Il suffit que ce numéro soit unique au niveau du réseau local pour éviter des problèmes techniques. La taille typique d'un réseau local est de quelques dizaines de machines. Il est donc tout à fait possible que ce numéro soit généré de manière automatique et aléatoire ou même choisi et communiqué par l'utilisateur[30]. La probabilité que deux cartes, au sein d'un même intranet, possèdent le même numéro est de l'ordre de un sur mille milliards.

1.5.3 Le contrôle des logiciels et matériels

23. Il est difficile de baser ce contrôle sur la directive générale 95/46 parce que les concepteurs de logiciel ou de matériel ne gèrent pas directement les données[31]. Cette considération est aujourd'hui empreinte d'une très grande naïveté technologique[32]. Au fil de la dernière décennie, l'utilisateur des technologies informatiques en général et de produits liés en particulier se trouve face à une immense usine à gaz effectuant des milliards d'opérations par seconde et dont la logique le dépasse. L'écran n'est plus qu'un pâle reflet des données qui circulent sur le réseau. De nombreux traitements invisibles sont effectués par-dessus son épaule.

---

[29] "compte tenu de l'état de l'art", comme précisé dans l'article 17 de la Directive 95/46. Dans ce cadre, il est opportun de considérer le hacking comme un "art".

[30] Cette possibilité est explicitement prévue dans le RFC 3041Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (http://www.ietf.org/rfc/rfc3041.txt?number=3041)

[31] Cette restriction ne vaut pas pour les systèmes privacides de type Passport ou Hailstorm conçus et gérés par Microsoft et qui auraient pour effet de rapatrier vers ce dernier des détails du comportements des utilisateurs de Windows XP.(cfr plainte déposée par l'EPIC : http://www.epic.org/privacy/consumer/MS_complaint.pdf)

[32] La directive 95/46 a été conçue à un moment où Internet était marginal et où Windows 95 n'était pas encore utilisé sur la majorité des ordinateurs personnels.

La directive 1999/5/CE du Parlement européen et du Conseil, du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité définit comme (art. 2 (b)) "équipement terminal de télécommunications", un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications. Un simple programme de navigation ou de courrier électronique ou encore un routeur peuvent donc être considérés comme équipements terminaux de télécommunication. Dans son article 3 c (exigences essentielles), la même directive pose, que la Commission peut décider *que les appareils relevant de certaines catégories d'équipements ou certains types d'appareils sont construits de sorte qu'ils comportent des sauvegardes afin d'assurer la protection des données à caractère personnel et de la vie privée des utilisateurs et des abonnés*. La Commission Européenne possède donc là un instrument juridique contraignant et directement disponible.

1.5.4 La concurrence loyale dans le marché des programmes Internet

24. Un programme de navigation est nettement plus complexe à réaliser qu'un logiciel serveur Web. Or le prix de ces deux types de programmes est inversément proportionnel à leur coût. Les premiers sont gratuits et les deuxièmes sont de l'ordre du millier d'euros. C'est une vue de l'esprit. En fait, la société qui achète un serveur web paie implicitement pour que les logiciels clients permettant d'accèder à son serveur soient distribués de manière gratuite. Cette situation entraîne deux biais à terme préjudiciable pour la protection des données de l'Internaute.

25. Les clients qui rapportent de l'argent à l'industrie du logiciel Internet sont les entreprises qui, de manière naturelle, désirent collecter le maximum d'informations sur leurs visiteurs virtuels. Les Internautes représentent un coût pour cette entreprise et la protection de leurs données pourrait être considérée une moins value pour les produits qu'elle distribue. Entre un serveur qui respecte l'anonymat des visiteurs du site ou un serveur permettant une connaissance intime, automatique et personnalisée de chaque visiteur, lequel une entreprise de commerce électronique aura-t-elle tendance à choisir ?

26. Les entreprises qui désirent se lancer dans la production de programmes de navigation payants[33] subissent une concurrence déloyale de la part de celles qui distribuent ces mêmes produits de manière gratuite. On peut comparer la situation actuelle des autoroutes de l'information à un réseau routier où les voitures seraient gratuites mais où les compagnies de distribution de carburant (le commerce électronique) seraient toutes équipées de pompes électroniques et robotisées fournies à plus 90% par un seul constructeur…qui serait celui qui fabriquerait les voitures gratuites. Dans ce monde imaginaire, il y a fort à parier que tous ces véhicules gratuits seraient rapidement bardés d'une série impressionnante de mouchards aptes à renseigner les stations de distribution d'essence (qui ont payé bien cher les pompes robotisées) sur la consommation des

[33] par exemple Opera : http://www.operasoftware.com

véhicules, leur itinéraire, les personnes présentes à bord du véhicule (avec des enfants ? des animaux de compagnie ?), leur profession, leurs revenus, leurs habitudes, leur psychologie, leurs centres d'intérêt, etc…

Jean-Marc Dinant[34]

[34] Les propos exprimés dans ces articles n'engagent que son auteur. Jean-Marc Dinant (http://www.droit.fundp.ac.be/cv/jmdinant/) est informaticien expert pour la Commission de Protection de la Vie Privée et directeur de Recherches au Centre de Recherche Informatique et Droit (CRID) de l'Université de Namur. Ce texte a été présenté à la 23ème conférence internationale des commissaires à la protection des données, à Paris en octobre 2001. (http://www.paris-conference-2001.org)