Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 23-Dec-1998
Dist. : 04-Jan-1999

Or. Ang.

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

DSTI/ICCP/REG(98)6/FINAL
Non classifié

Groupe d'experts sur la sécurité de l'information et la vie privée

PRATIQUES RELATIVES A LA MISE EN OEUVRE SUR LES RESEAUX MONDIAUX DES LIGNES DIRECTRICES DE L'OCDE SUR LA VIE PRIVEE

73164

Or. Ang.

AVANT-PROPOS

Les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ont été adoptées en tant que Recommandation du Conseil de l'OCDE le 23 septembre 1980. Cette Recommandation définit des principes directeurs pour la collecte et le traitement d'informations de caractère personnel et ces principes technologiquement neutres figurent dans un grand nombre d'instruments nationaux et internationaux.

Eu égard à sa connaissance acquise lors de l'élaboration des Lignes directrices sur la vie privée, à son expérience renouvelée des questions liées à la protection de la vie privée et à ses travaux en cours dans le domaine de l'infrastructure globale de l'information, de la société globale de l'information (GII/GIS) et du commerce électronique, le Comité de la politique de l'information, de l'informatique et des communications (PIIC) de l'OCDE a décidé, en septembre 1997, d'entreprendre un programme de travail relatif à la mise en oeuvre, dans un environnement en ligne, des Lignes directrices sur la protection de la vie privée.

Dans ce contexte, le présent rapport, rédigé par M. S. Gauthronet, consultant, analyse des "pratiques" actuelles en matière de protection de la vie privée sur les réseaux globaux et comporte, dans une annexe, des suggestions pour un design "privacy friendly" des sites Web.

Le rapport a été soumis au Groupe de travail sur la Sécurité de l'information et la Vie Privée en mai 1998 et au Comité PIIC en septembre 1998 qui a décidé de le déclassifier sous l'autorité du Secrétaire Général. Le rapport reflète les vues de son auteur et non nécessairement celles de l'OCDE ou des gouvernements des pays Membres de l'OCDE.

TABLE DES MATIERES

INTRODUCTION 4

LA COLLECTE DE DONNEES PERSONNELLES SUR LES SITES COMMERCIAUX EN LIGNE 6

Modalités de collecte et nature des données personnelles collectées 6
Qualité et pertinence des données 8

LES TRAITEMENTS DE DONNEES PERSONNELLES SUR LES SITES COMMERCIAUX EN LIGNE 11

Nature des traitements de données 11
Cessions de données à des tiers 12

TRANSPARENCE DES SITES EN MATIERE DE PROTECTION DE LA VIE PRIVEE 14

La référence aux lois nationales 14
La présence de " Privacy Policy Statements " 15
Les références à des codes de conduite 17

LES TECHNOLOGIES DE SECURITE ET DE CONTROLE DES DONNEES 19

La sécurisation des paiements 19
L'exercice du droit d'accès 20
Les systèmes de contrôle des données (PETs) 20

RECOURS ET RESPONSABILITES 22

Les voies de recours proposées 22
Les responsabilités en matière de respect de la vie privée 22

CONCLUSION 24

ANNEXE 1 SUGGESTIONS POUR UN DESIGN *PRIVACY FRIENDLY* DES SITES WEB 25

ANNEXE 2 ETUDE RELATIVE A DES PRATIQUES EN MATIERE DE PROTECTION DE LA VIE PRIVEE EFFECTUEE SUR UN ECHANTILLON DE SITES WEB SITUES DANS DIVERS PAYS MEMBRES DE L'OCDE 27

INTRODUCTION

Ce rapport de synthèse s'appuie sur une enquête flash réalisée par le secrétariat de l'OCDE au cours du mois d'avril 1998 sur une cinquantaine de sites Web, principalement des sites commerciaux grand public, dont un résumé est présenté en annexe 2. L'objectif consistait à analyser dans quelle mesure et par quels moyens les Lignes directrices de l'OCDE en matière de protection des données étaient ou pouvaient être mises en pratique à travers ces différents sites. Les fortes contraintes liées à la nécessité de respecter le programme de travail de l'OCDE ont fait que cette étude a dû être réalisée dans des délais extrêmement courts et sur un échantillon restreint.

Le choix des sites n'est pas statistiquement significatif ; délibérément il n'est pas non plus représentatif du monde des services en ligne : on s'est efforcé plutôt de sélectionner des sites commerciaux pour leur exemplarité et leurs " bonnes pratiques" en matière de protection des données et de la vie privée de leurs utilisateurs. La sélection s'est opérée avec l'aide informelle de différentes personnes ressources dans plusieurs pays. L'échantillon comporte 3 sites choisis en Australie, 5 au Canada, 1 au Danemark, 2 en Finlande, 6 en France, 1 en Allemagne, 2 en Italie, 2 au Japon, 1 au Mexique, 2 en Espagne, 2 au Royaume-Uni et 23 aux Etats-Unis.

La problématique de l'étude consiste à observer concrètement comment dans ces sites les grands principes des Lignes directrices de l'OCDE sont mis en pratique à travers les références qu'ils peuvent faire à des corpus de règles (lois nationales, politiques internes ou codes déontologiques professionnels) ; comment ils sont appliqués que ce soit à travers des procédures d'inscription, des contrats d'abonnement par exemple ou à travers des solutions technologiques additionnelles ; à quelles obligations en la matière les opérateurs de ces sites sont contraints ou s'astreignent eux-mêmes.

Pour les besoins de ce rapport que l'on a souhaité assortir de suggestions présentées en annexe 1, les résultats de l'enquête réalisée sur les sites Web sont traités, selon le schéma ci-après, en cinq chapitres dans lesquels on retrouvera une correspondance avec les huit principes fondamentaux des Lignes directrices de l'OCDE:

- ***La limitation en matière de collecte de données*** : ce point est traité dans la première partie du chapitre I à travers une présentation des différentes techniques appliquées pour collecter les données personnelles.

- ***La qualité des données*** : ce point est traité dans la deuxième partie du chapitre I où l'on s'efforce de reconstituer la notion de pertinence de la collecte telle qu'elle ressort à travers les sites concernés par rapport à leurs objectifs ; on répertorie aussi quelles sont les informations facultatives et quelles sont celles qui sont obligatoires ; accessoirement on identifie également les données sensibles que ces sites peuvent être amenés à enregistrer dans leurs fichiers.

- ***La spécification des finalités*** : l'application de ce principe est étudiée dans le chapitre II où l'on distingue les traitements selon qu'il s'agit de ciblage marketing ou d'analyse navigationnelle.

- ***La limitation de l'utilisation*** : la mise en œuvre de ce principe, notamment la question de la cession de données à des tiers et les possibilités d'*opt-out* offertes aux personnes sont présentées dans les deux dernières parties du chapitre II.

- ***Les garanties de sécurité*** : cette question est abordée dans la première partie du chapitre IV dans le cadre des procédures de paiement en ligne.

- ***La transparence*** : la notion de transparence des pratiques par les sites Web est analysée dans le chapitre III à travers les différentes références qu'ils font que ce soit aux lois nationales, à des politiques internes ou à une déontologie professionnelle. Cette analyse comporte également un diagnostic quant à la visibilité de ces principes directeurs à travers les pages des sites ainsi qu'une typologie du contenu des "*privacy statements*" ou des contrats accessibles en ligne.

- ***La participation individuelle*** : il s'agit des droits individuels des personnes tels que les sites de l'étude les reconnaissent à leurs visiteurs ou à leurs abonnés ; ils sont examinés dans les deux dernières parties du chapitre IV.

- ***La responsabilité*** : la mise en application de ce principe est analysée dans le chapitre V à travers les voies de recours proposées par les opérateurs de site et une évaluation de leur loyauté quant à l'application des règles qu'ils se fixent.

LA COLLECTE DE DONNEES PERSONNELLES SUR LES SITES COMMERCIAUX EN LIGNE

Modalités de collecte et nature des données personnelles collectées

Les sites étidués collectent les données selon deux protocoles principaux : l'implantation de fichiers de *cookies* sur les micro-ordinateurs des utilisateurs et le remplissage de formulaires divers.

Les fichiers de cookies

Une majorité de sites implante des fichiers de *cookies*[1] ; dans quelques cas, notamment le secteur de la presse et des média ou les moteurs de recherches, les *cookies* sont liés à l'incrustation de bannières publicitaires (*Ad-banner*) dont l'emplacement est géré par une agence de commercialisation d'espace (*Rep-Agency*) du type de DoubleClick ou FocalLink. La notification apparaît à condition que le *browser* soit paramétré correctement de sorte que la boîte de dialogue signalant que le site souhaite envoyer le *cookie* s'affiche en surimpression sur l'écran de l'utilisateur ; dans ce cas de figure on peut considérer que la collecte de données s'opère de manière licite et loyale et qu'en cliquant sur le bouton d'acceptation, le visiteur consent à l'opération ; cela ne veut pas dire pour autant qu'il soit à ce stade éclairé sur la finalité de la collecte et les traitements que cela va permettre. Si par contre le *browser* est paramétré de manière à accepter les *cookies* sans affichage systématique de la boîte d'avertissement, l'utilisateur ne les verra pas passer et la circulation des *cookies* s'opérera alors à son insu.

La boîte de dialogue dont le contenu est standardisé permet d'identifier le nom du fichier qui ira s'inscrire dans le répertoire ad hoc, l'origine du *cookie* (nom de l'URL) et sa durée de vie : la majorité des *cookies* envoyés par les sites de l'échantillon ont une date d'expiration fixée à la fin de l'année 1999, soit près de 20 mois. Deux cas dépassent l'an 2000 (2010 pour l'un, 2020 pour un autre).

---

1. Un "cookie" est un mécanisme que les connexions du "côté serveur" (server-side) peuvent utiliser pour, à la fois, stocker et retrouver de l'information sur le "côté client" (client-side). En pratique, un cookie est un fichier texte qu'un site web place sur l'ordinateur d'un utilisateur lorsque ce dernier visite le site. Le serveur web peut ainsi par la suite, accéder à ce fichier, et le lire, chaque fois que l'utilisateur visite le site. Ce fichier texte contient de l'information concernant l'utilisateur, qui permet ensuite au site web de reconnaître ce dernier et de rappeler ses préférences, par exemple pour vérifier son mot de passe, ou l'orienter sur une page pré-selectionnée à l'intérieur d'un site. Les cookies peuvent également être utilisés pour enregistrer les articles qui vont être achetés dans un magasin électronique (auquel cas, le cookie sert de "panier" jusqu'à la phase finale de la transaction) ou bien, pour personnaliser le site en fonction de l'identité de l'utilisateur. Ils peuvent aussi être utilisés pour collecter des informations sur l'audience du site, notamment en observant le comportement d'un utilisateur à l'intérieur d'un site, ou en pistant ses retours sur le site.

La particularité des *cookies* est qu'afin de suivre notamment la navigation de l'utilisateur à travers les différentes rubriques, les sites peuvent être amenés à en implanter à plusieurs reprises. La fréquence peut être très élevée : dans de nombreux cas elle est supérieure à cinq ; plusieurs sites de l'échantillon en ont proposé l'implantation à plus de dix reprises. Le risque à ce niveau est que, lassés, les utilisateurs d'Internet paramètrent une bonne fois pour toutes leur *browser* de manière à accepter les *cookies* et éviter l'affichage trop fréquent de la boîte d'avertissement.

A l'exception d'un site, dans la totalité des autres cas analysés l'acceptation des *cookies* ne conditionne pas l'entrée et la navigation sur le site ou sur une rubrique. Indirectement cela signifie qu'il n'existe pas à ce niveau de relation de subordination entre la fourniture de données personnelles et l'accès à un site Internet.

Un serveur Web peut également envoyer de l'information qui est stockée par le navigateur de l'utilisateur (c'est ce que l'on appelle les *cookies*), et restituée lors d'une connexion ultérieure au serveur. Ce système permet de savoir qu'un visiteur est déjà passé par là, sans que pour autant son identité soit connue : il faut pour l'identifier procéder à des recoupements avec d'autres informations. Ainsi, rapprochées du fichier identité incorporé dans le browser et transmis à un serveur, les informations inscrites dans les *cookies* permettent de constituer des profils intéressants d'utilisateurs. Il peut être noté toutefois que certains navigateurs permettent, avec une aisance variable et souvent insuffisante, de bloquer l'utilisation de ces *cookies*.

Les formulaires

Proposant pour la plupart des services commerciaux, la totalité des sites de l'échantillon soumettent à leurs visiteurs des formulaires qu'ils doivent remplir pour s'inscrire, s'abonner, participer à un groupe de discussion hébergé sur le site, faire part de suggestions et *a fortiori*, bien entendu, pour réserver un service ou commander un article et engager la procédure d'achat.

Les données le plus fréquemment collectées concernent le nom, l'adresse, le numéro de téléphone personnel ou professionnel et l'adresse e-mail de l'utilisateur ; des données d'identification complémentaires sont parfois demandées sur l'âge, le sexe, le statut matrimonial, l'emploi occupé et dans quelques cas les revenus, la taille et le secteur d'activité de l'entreprise ou les centres d'intérêt personnels (sports pratiqués, habitudes de lecture, …). Les formulaires de commandes exigent tous le type et le numéro de carte de crédit ainsi que la date d'expiration ; ils proposent également une distinction entre l'adresse de livraison et l'adresse de facturation. Ces données sont collectées dans des contextes d'inscription, de participation volontaire à une enquête ou de paiement qui font qu'elles restent dans l'ensemble pertinentes.

Bien qu'a priori l'information soit collectée à travers les *cookies* quelques sites demandent à leurs utilisateurs de leur préciser le système d'exploitation de leur micro-ordinateur et la version du *browser* avec lequel ils se connectent sur Internet, la vitesse de transmission du modem. Certains sites comportent des questionnaires en ligne en relation avec leur activité et peuvent être amenés à solliciter des données précises concernant par exemple pour les constructeurs de matériels informatiques ou les éditeurs de logiciels les caractéristiques de l'ordinateur utilisé, pour les agences de voyages les préférences de services à bord des compagnies aériennes (emplacement du siège, repas).

La collecte automatique de données

Ainsi qu'on le sait, les deux composants technologiques de base présents au sein des *browsers* (Java ou ActiveX) ont comporté à une époque de graves anomalies qui menaçaient la sécurité des données et des fichiers personnels présents sur les micro-ordinateurs des utilisateurs ; plus particulièrement, dans les versions 2 et 3 de Navigator, il était possible pour un site *Web* mal intentionné de capturer l'adresse *e-mail* de ses visiteurs à leur insu. Ces problèmes sont a priori réglés aujourd'hui. Quelques sites américains, pour dissiper tout soupçon, prennent l'engagement explicite dans leur "*privacy policy statement*" qu'ils ne collectent pas l'adresse *e-mail* autrement que lorsqu'elle est fournie volontairement par les visiteurs.

Toutefois des moyens de collecte automatique existent encore à travers d'une part l'adresse IP qui contient notamment le nom de domaine auquel un utilisateur appartient et son fournisseur d'accès ; seuls deux sites de l'échantillon font référence à cette collecte de données de nature plutôt technique et peu identifiantes. Il est possible d'autre part de collecter les données du formulaire d'identification que l'utilisateur d'un PC est invité à renseigner dans les options de configuration de son *browser* et qui correspondent en réalité à sa carte de visite personnelle : ce formulaire comporte plusieurs onglets et de nombreux champs, tous étant bien sûr facultatifs, pour le nom de l'utilisateur, son adresse *e-mail*, son adresse professionnelle et personnelle, ses différents numéros de téléphone ou de fax, sa fonction et même une zone en texte libre. Si le *browser* n'est pas configuré de telle sorte qu'une boîte de dialogue s'affiche lorsqu'un site souhaite accéder à cette information, le transfert des données présentes s'opère alors automatiquement à l'insu de l'utilisateur. Cela dit rien n'oblige un utilisateur à personnaliser son *browser*, pas même à mentionner son adresse *e-mail*. Aucun des sites étudiés ne fait référence à ce mode de collecte de données personnelles.

Enfin, il est encore un procédé très simple de collecter une adresse électronique, sans qu'un visiteur en soit nécessairement conscient, qui consiste à exploiter l'en-tête de courriers électroniques ou de formulaires divers qu'il va transmettre via *e-mail*. En tout et pour tout, seul un site français, qui offre une prestation de gestion de portefeuille de titres boursiers, mentionne ce risque par l'activation d'une boîte de dialogue du *browser* qui s'affiche préalablement à la transmission par le visiteur d'un formulaire de demande d'informations.

Qualité et pertinence des données

Données collectées et finalités

Dans l'ensemble les données collectées par les sites de l'échantillon semblent pertinentes par rapport aux finalités.

Il faut par contre observer qu'il est assez rare que l'utilisateur soit informé de la finalité simultanément au processus de collecte, cette remarque s'applique particulièrement en ce qui concerne les fichiers de *cookies* : la boîte de dialogue s'affiche de façon impromptue au cours de la navigation et ne contient aucune indication quant à la finalité du *cookie* ; il faut se déplacer pour cela dans une zone de service du site, où le cas échéant la *cookie policy* sera explicitée. Dans ce cas les trois finalités qui sont le plus souvent déclarées sont assez neutres :

- la reconnaissance automatique du visiteur lorsqu'il se connecte, ce qui évite d'avoir à lui demander de s'identifier ; c'est donc là un principe de confort ergonomique favorable à l'utilisateur ;

- l'analyse de la navigation, la détection des rubriques les plus visitées, afin de faire évoluer au mieux le contenu du site en fonction des attentes des utilisateurs ;

- la conservation dans le panier des articles sélectionnés au cours de la session d'achat jusqu'à la réalisation de la transaction de paiement proprement dite au cours de la vacation, ou au cours d'une nouvelle vacation si la précédente a été interrompue pour une raison ou pour une autre.

Il est curieux cependant qu'aucun des sites n'explique sincèrement qu'un des objectifs des *cookies* est somme toute de pouvoir réaliser de la communication publicitaire -- *one to one* -- en ciblant précisément les visiteurs en fonction de leur profil individuel. Peut-être certains considèrent-ils qu'ils n'ont rien à voir avec ces traitements, étant donné qu'ils sont généralement assurés par des agences spécialisées et que leur site n'est qu'un support. Si telle était leur attitude elle serait pour le moins discutable. Par ailleurs, il est manifeste que d'autres sites réalisent leurs propres études d'impacts : un site explique ainsi qu'il procède à des études anonymes lui permettant de dire à ses clients annonceurs que "*12 000 personnes ont cliqué sur la bannière publicitaire X ou Y aujourd'hui et parmi elles 35 pour cent nous ont indiqué précédemment qu'elles s'intéressaient au sport" ;* le paradoxe est que nulle part ce site n'explique qu'il opère des traitements d'analyse des *clickstream* et qu'au moment où le traitement proprement dit est opéré les données en entrée ne sont pas anonymisées, seuls les résultats en sortie le sont.

On a plus de chance par contre de trouver une explication des finalités acceptable et associée au processus de collecte lorsqu'on est en présence de questionnaires. Les opérateurs de site font en effet l'effort de préciser en tête du questionnaire que les informations demandées ont pour but par exemple d'enregistrer une participation à un concours ou de réaliser des études de fréquentation à caractère socio-démographiques ; ils précisent également que les données seront traitées de façon agrégée et anonyme ; pour faire comprendre cela, on trouve généralement une illustration du type : "*40 pour cent de nos membres appartiennent à la classe d'âge de 20 à 30 ans*".

Informations facultatives et informations obligatoires

Dans près des deux-tiers des sites certaines des informations demandées à travers les divers formulaires d'inscription, les formulaires de *feed-back* et surtout à travers les questionnaires sont facultatives ; plusieurs sites ont adopté une pratique satisfaisante pour la compréhension du visiteur qui consiste à séparer nettement les informations facultatives en les regroupant dans un pavé distinct ; cette formule a le mérite d'être plus claire que celle, assez fréquente, qui consiste à marquer d'un astérisque les champs d'informations qui entrent dans cette catégorie. D'autres sites procèdent de manière inverse et affichent les libellés correspondant à des champs d'information obligatoires en caractères gras ou les font précéder de la mention "*Required* ". Parmi les données facultatives on trouve assez souvent l'adresse *e-mail* et le numéro de téléphone, l'âge et le sexe, la profession, certaines préférences et habitudes personnelles ; dans quelques cas, notamment dans une galerie commerciale japonaise, la fourniture de réponse aux questions facultatives permet aux visiteurs d'acquérir en échange des points-cadeaux ; dans un autre cas, de participer à un concours, dans un autre encore, celui d'une librairie *on line,* la précision par les visiteurs de leurs genres de lecture préférés leur donne droit à un service mensuel gratuit d'information (transmission dans la boîte-aux-lettres électronique) sur les parutions récentes correspondant aux goûts personnels qui ont été cochés dans le questionnaire.

Les informations obligatoires quant à elles correspondent en général aux données d'identification et de paiement indispensables pour s'abonner ou réaliser une transaction ; à ce titre

certaines des données sont contrôlées par des tables et fiabilisées *on line* comme par exemple le remplissage correct des zones d'adresse, les codes postaux et les données concernant les cartes de crédit ; ces contrôles sont opérés soit directement par le site lui-même soit par une connexion instantanée sur un serveur d'autorisation.

La collecte de données sensibles

L'étude permet d'observer qu'au moins trois sites collectent des informations à caractère sensible. Deux de ces sites sont des librairies en ligne. L'une propose facultativement à ses visiteurs de cocher sur une longue liste quels sont leurs thèmes de lecture préférés ; la liste comporte des sujets qui indirectement peuvent révéler les inclinations sexuelles des visiteurs qui les sélectionnent ("*gay studies*", "*lesbian studies*") ou leur religion ("*Eastern religion*", "*judeo-christian book"*). Ce site ne comporte aucune disposition particulière de confidentialité à l'égard de ces données. L'autre librairie est par contre plus prudente et spécifie que les données sensibles qu'elle pourrait être amenée à collecter (numéro de sécurité sociale, nom de jeune fille de la mère, salaire, détention de portefeuille d'actions, données médicales, données concernant les enfants) seront traitées avec un soin très particulier (*extra care*), qu'elles ne sortiront pas de l'entreprise et que les personnes peuvent exercer un *opt-out* pour éviter que ces données soient partagées avec diverses entités à l'intérieur même de l'entreprise *business units*.

Le troisième site est celui d'une agence de voyage australienne qui dans le cadre de l'enregistrement de ses membres collecte des données que l'on pourrait qualifier d'indirectement sensibles et qui ont trait à l'expression de préférences de service lors de l'enregistrement d'une réservation aérienne. Ces préférences (SSR : *Special Services Requirement*) ont été codifiées et normalisées au plan international sous l'égide de IATA dans une table appelée AIRIMP et sont couramment utilisées par les agences de voyage dans le monde entier lors de la création du PNR (*Passenger Name Record*) ; elles comportent près d'une centaine de codes sur 4 caractères alphabétiques dont certaines qui définissent les exigences alimentaires (repas pour diabétique, repas végétarien, repas musulman, repas cacher,…) et l'état de santé du passager ("*Blind passenger"*, "*Deaf passenger"*, "W*heelchair in cabin"* …) sont proposées sur le site Internet étudié afin d'être prises en compte lors du processus de réservation en ligne.

LES TRAITEMENTS DE DONNEES PERSONNELLES SUR LES SITES COMMERCIAUX EN LIGNE

Nature des traitements de données

La quasi-totalité des sites de l'échantillon indiquent clairement qu'ils procèdent à des traitements de données personnelles ; deux catégories de traitements doivent être distinguées, les traitements de ciblage marketing et les traitements de données navigationnelles (*clickstream data*) :

- Les traitements marketing sont destinés à établir le profil des visiteurs des sites qui se sont inscrits et qui ont fourni pour cela un certain nombre de données permettant de les identifier ; il est précisé de façon assez systématique que ces traitements déboucheront sur des offres commerciales ciblées qui seront faites aux visiteurs selon trois moyens de communication : le courrier postal, le courrier électronique et plus rarement le téléphone. Moins de cinq sites pratiquent le *host-mailing* : ils expliquent ainsi qu'ils pourront être amenés à réaliser eux-mêmes une campagne commerciale pour le compte de partenaires extérieurs, dont on précise toujours qu'il s'agit de sociétés sérieuses et scrupuleusement sélectionnées.

- Les traitements des données navigationnelles permettent de croiser deux sources d'information :

  – les données d'identification et de profil des visiteurs telles qu'elles ont pu être collectées lors de l'enregistrement initial des utilisateurs sur le site ;

  – les données générées soit à partir de logiciels d'analyse des logs[2] présents sur les plates-formes serveurs, soit à l'aide des *cookies* et qui vont permettre de suivre pas à pas les rubriques consultées par les utilisateurs et les articles placés dans le panier d'achat.

Trois sites seulement reconnaissent qu'ils procèdent à ce type de *matchings* qui à l'évidence permettent d'affiner les profils et surtout de déterminer quelles sont les zones des sites les plus fréquentées par telle ou telle catégorie d'utilisateurs ; dans une logique de marketing *one-to-one*, cette information est bien entendu à très haute valeur ajoutée pour les agences publicitaires, les acheteurs d'espace et les

2. Le "logiciel d'analyse de fichier journal" (Log Analysis Software) est un logiciel "côté serveur" utilisé par un site Web pour analyser des données relatives aux utilisateurs collectées par l'intermédiaire des cookies en les rapprochant d'informations collectées par le serveur dans un "fichier journal standard du serveur". Les données du journal qui sont obtenues lorsqu'un utilisateur se connecte à un site web, incluent l'adresse IP, la date de connexion, le type de transaction, le nombre des fichiers transférés vers le navigateur de l'utilisateur, le protocole utilisé, la page par laquelle l'utilisateur a accédé au site, ainsi que le type de navigateur utilisé. Le "logiciel d'analyse de fichier journal" peut être utilisé pour un analyse approfondie de la fréquentation du site Web.

annonceurs. Ce petit nombre de sites qui pratiquent en la matière une relative transparence, ont pour caractéristiques communes d'être tous les trois d'origine nord américaine et d'adhérer au label TRUSTe. Ces sites expliquent dans leur "*privacy statement*" qu'ils se financent essentiellement à partir de revenus publicitaires et que de leur capacité à fournir des données de ciblage pointues dépend la gratuité d'accès pour les visiteurs. Ces sites affirment également ne pas réaliser de rapprochements entre les identités individuelles et la navigation ; dont acte. Il faut toutefois convenir que rien techniquement n'empêche de réaliser ce traitement dans la mesure où les *cookies* placés par ces sites contiennent un *user ID* permanent qu'il est aisé de rapprocher des données d'identification et de profil collectées lors du processus d'enregistrement du visiteur.

Cessions de données à des tiers

Deux familles de sites peuvent être distinguées à cette étape : les sites qui explicitement et catégoriquement déclarent à travers leur "*privacy statement*" qu'ils n'entendent céder aucune donnée personnelle à des tiers en dehors de statistiques agrégées et anonymes ; et ceux qui, dans des termes généralement prudents, expliquent qu'ils peuvent être amenés à fournir à des filiales ou à des partenaires extérieurs des données personnelles en vue d'envoi de sollicitations commerciales. Tous les sites qui pratiquent des cessions de données à des tiers mettent en avant le respect de la vie privée en offrant la possibilité aux personnes de s'en extraire.

Les possibilités d'opt out

La moitié des sites analysés offrent aux visiteurs la possibilité de refuser que leurs données personnelles fassent l'objet de traitements commerciaux et de transmission à des tiers. Le visiteur a la possibilité d'exprimer son refus de quatre manières différentes :

- par cochage d'une case ad hoc, généralement située sur le formulaire d'inscription, ce qui apparaît somme toute le moyen le plus simple et le plus naturel pour la personne d'exercer son droit au retrait ;

- par courrier, dans ce cas on remarque que tous les sites ne font pas l'effort de rappeler leur adresse postale à l'endroit même où figure cette indication ; il est généralement demandé aux personnes à ce niveau de préciser leur nom et leur adresse exacte afin que leur requête puisse être prise en compte ;

- par e-mail libre ;

- par téléphone, quelques sites seulement indiquent alors un numéro vert.

Il est très difficile sur quelques sites qui déclarent offrir une possibilité d'*opt-out*, sans en préciser les modalités, de trouver comment ce droit s'exerce. En réalité, après une recherche plutôt longue, on découvre au détour d'une explication dans le "*privacy statement*" que le visiteur dispose, à travers les *e-mail* commerciaux qu'il va recevoir d'une possibilité d'envoyer une réponse en retour pour se soustraire à ce type d'envoi. Il s'agit donc *d'un opt-out* différé.

Il est très important de noter que les dispositions d'*opt-out* telles qu'elles sont proposées dans les sites appartenant à l'échantillon ne s'exercent qu'à l'égard de démarches commerciales ou d'opérations publicitaires dont le visiteur est susceptible de faire l'objet ; seuls les sites du monde de la presse incluent

dans l'*opt-out* les enquêtes de satisfaction qui pourraient être adressées aux abonnés par *e-mail* . De plus, la procédure d'*opt-out* ne distingue pas selon que le démarchage est initié par le site lui-même ou par des tiers qui auraient eu communication d'un fichier de prospects. Dans aucun des sites analysés les utilisateurs n'ont la possibilité d'exercer un *opt-out* par rapport au traitement des données navigationnelles ou celles relatives à leur comportement d'achat. Un seul site très particulier offre une procédure d'*opt-out* non commerciale, pourrait-on dire : il s'agit d'un site canadien permettant à ses abonnés de poster une recherche d'emploi ; pour des raisons évidentes de confidentialité, les candidats ont la possibilité de transmettre, via une zone en texte libre, une liste d'entreprises auxquelles ils ne souhaitent pas que leur demande soit transmise. Indirectement et même si cela est complexe, cet exemple témoigne de la capacité des sites à gérer des demandes d'*opt-out* différenciées.

Un seul site fait référence à une procédure de recueil du consentement de ses visiteurs préalablement à l'utilisation de données personnelles : il s'agit du cas bien particulier d'un très grand site technologique américain qui offre à ses visiteurs de nombreux systèmes de *feed-back* ; cela l'amène ainsi à récupérer toutes sortes d'informations et de réflexions sur lesquelles les opérateurs du site considèrent qu'ils disposent d'un droit d'usage sans limite et irrévocable, ce qui peut être discutable. Dans le cas où ces textes seraient publiés, le site s'engage cependant à ne faire référence nominativement à leurs auteurs qu'après notification préalable ou recueil de leur consentement.

Enfin une mention spéciale doit être faite en ce qui concerne la possibilité d'exercer un *opt-out* global et centralisée auprès des agences qui exploitent la communication publicitaire sur Internet. Cette possibilité est effectivement offerte par l'agence DoubleClick entre autres ; concrètement, l'activation de la procédure nécessite de se connecter au site de l'agence et de sélectionner la rubrique "*privacy*" : à cet endroit l'utilisateur peut lire une déclaration générale de l'entreprise concernant ses pratiques en matière de protection de la vie privée et choisir l'*opt-out.* A partir de ce moment-là, le numéro d'identification spécifique à DoubleClick et contenu dans le *cookie* est effacé et remplacé par la mention ID = OPT OUT. Quasiment personne ne connaît l'existence de cette procédure, sur 17 millions de *cookies* implantés il y a environ un an, DoubleClick déclarait ne recevoir à l'époque guère plus de 5 à 10 *opt-out* par jour ; cela s'explique probablement par le fait qu'aucun des sites *Web* qui commercialisent leur espace publicitaire via une agence du type de DoubleClick ne font référence, par hyper-lien par exemple, à l'existence de cette possibilité.

TRANSPARENCE DES SITES EN MATIERE DE PROTECTION DE LA VIE PRIVEE

L'étude des sites permet dans une certaine mesure d'apprécier leur niveau de mise en pratique du principe de transparence de la politique en matière de protection de la vie privée. On a recherché à ce niveau à identifier à quel corpus de règles les sites faisaient référence et en quels termes ils le faisaient ; d'emblée il ressort qu'aucun des sites ne fait référence à l'un ou l'autre des instruments internationaux suivants : OECD Guidelines, Council of Europe Convention, United Nations Guidelines, EU Directive. Trois catégories de sites peuvent être ici distinguées suivant qu'ils se réfèrent à une loi nationale, à une politique interne, à un code de déontologie sectoriel.

La référence aux lois nationales

On observe que dans l'ensemble les sites européens font référence à leur loi nationale respective en matière de protection des données ; quelques sites cependant omettent encore de le faire. La référence figure le plus souvent sous une rubrique de service qui traite du droit d'accès et de rectification des données personnelles, une rubrique FAQ (Frequently Asked Questions), un contrat d'abonnement (presse), ou encore à travers le "*privacy statement*" lorsqu'il y en a un, ce qui n'est pas toujours le cas chez les sites européens.

A défaut de loi nationale sur la protection des données, les deux sites américains exerçant dans le secteur du *Credit Reporting* se réfèrent à une réglementation sectorielle dans le domaine du crédit (FCRA: *Fair Credit Reporting Act* – 1970, amendé Sept. 30,1996) qui comporte un ensemble de dispositions sur le droit d'accès et de rectification des données, leur durée de conservation, et des restrictions quant à leur transmission à des tiers ; l'un des deux sites propose un hyper-lien permettant d'accéder au texte complet de la loi. On doit bien noter cependant que la référence à cette loi concerne la protection de la vie privée des consommateurs dont les données sont présentes dans les fichiers, bien plus que celle des clients abonnés au site Web qui accèdent à ces données ; les contrats d'abonnement à ces sites sont très élaborés ; ils révèlent en cela la sensibilité toute particulière de la société américaine à l'égard des *Credit Bureaus* ; ainsi en s'abonnant au site, les clients du système qui à la fois consultent et enrichissent la base de données des *consumer credit reports,* s'engagent à appliquer les obligations instituées par le FCRA ; des clauses spécifiques du contrat les rappellent, notamment l'obligation de respect des finalités ("*legitimate business*" et l'obligation de divulgation des sources à la demande.

Un site canadien spécialisé dans les offres d'emplois protège la confidentialité des informations personnelles stockées dans ses bases de données en invoquant les lois nationales applicables au *copyright* ; il rappelle les sanctions prévues à l'égard des actes de piratage et encourage, moyennant une récompense de $500, la dénonciation de toute utilisation frauduleuse, reproduction et redistribution des données.

La présence de "Privacy Policy Statements"

Les trois-quarts des sites Web de l'échantillon étudié ont une politique de protection de la vie privée à destination de leurs visiteurs et accessible *on line*. On peut observer qu'il n'y a pas à proprement parler de conjonction entre le fait que les sites aient pris la peine de se doter d'une politique spécifique et le fait qu'il existe plus largement au plan national des dispositions légales en matière de protection des données : 11 sites d'origine européenne sur 19 affichent leur propre politique ; en toute logique la proportion est de 22 sur 23 pour les sites américains. Aucun des sites ne cherche explicitement à tirer avantage en terme d'image et de recherche de confiance chez les visiteurs du fait qu'il se soit doté de "*privacy statement*". Dans le cadre de l'évaluation de la transparence des politiques, on s'est plus particulièrement intéressé à l'accessibilité de cette information, aux garanties offertes et aux possibilités de recours mises à disposition des utilisateurs.

Accessibilité des "Privacy Policy Statements"

On retire un sentiment assez partagé quant à la facilité avec laquelle les visiteurs peuvent accéder aux "*Privacy Statements*" sur les sites *Web :* l'opération est aisée pour un peu plus de la moitié des sites considérés mais elle s'avère complexe pour au moins une dizaine d'entre eux et nécessite un temps de navigation relativement long avant de les découvrir ; pour certains sites il faut même être assez avancé dans un processus d'inscription ou dans une transaction, c'est à dire avoir commencé à transmettre des données personnelles, pour voir apparaître un lien avec les dispositions du site concernant les données et la vie privée. La procédure la plus aisée est bien entendu lorsque figure le titre de rubrique *privacy* sur la *homepage* des sites, c'est le cas le plus fréquent et l'utilisateur intéressé peut satisfaire sa curiosité très rapidement. On observe enfin que seulement cinq sites ont référencé le terme *privacy* dans le catalogue des mots-clés de leur moteur de recherche interne.

Typologie des politiques

Il n'était pas dans les moyens de l'étude de procéder à une analyse juridique approfondie du contenu des "*privacy statements*" postés par les différents sites retenus dans l'échantillon. On peut toutefois les classer en trois grandes catégories :

- *Les dispositions incluses dans des sections FAQ* : il s'agit généralement de rubriques assez sommaires (de un à cinq paragraphes) traitant souvent partiellement de la question ; certains se focalisent sur les *cookies*, d'autres sur la capture de l'adresse *e-mail*, ou la procédure d'*opt-out*, d'autres enfin sur les protocoles sécurisés de transmission de données. Une des traits communs à ces sites est peut-être qu'ils sont récents sur le *Web* ou qu'ils éludent un peu vite la question au prétexte qu'ils peuvent faire référence à la loi nationale du pays où ils sont établis. Le seul cas un peu exceptionnel dans ce groupe, est celui de Netscape où l'on ne trouve pas moins de quatre ou cinq pages de questions-réponses assez techniques autour des enjeux de la protection de la vie privée. Mais ce site possède aussi une rubrique dans ses CGU (Conditions Générales d'Utilisation – Trad. : *TOS : Terms Of Service*) qui définit précisément les pratiques de collecte des données et les conditions d*'opt-out*.

- Les "*Privacy Statements*" en forme de lignes directrices : il s'agit là souvent de rubriques à part entière, généralement accessibles dès la *homepage*. En terme de volume, ces lignes directrices varient entre une page et dix pages denses, la moyenne pouvant être estimée

autour de 3 ou 4 pages. Elles se distinguent de prime abord par leur contenu : certains sites adoptent un profil résolument favorable aux visiteurs : pas d'exportation de *cookies* (sur les sites notamment qui s'adressent aux enfants), analyse de trafic limitée aux statistiques de *login*, durée de conservation réduite, référence au droit d'accès, procédure d'*opt-out*, non-communication des données à des tiers. A l'autre extrême l'échantillon comporte une catégorie de sites qui exposent dans le détail des pratiques de collecte et de traitement de données que l'on pourrait qualifier de résolument extensives, sans pour autant qu'ils obèrent la possibilité d'exercice des droits individuels.

A l'évidence l'affichage de "*Privacy Statements*" est plutôt une pratique nord américaine. Les sites qui l'ont adopté ont généralement une bonne antériorité sur le monde en ligne, ils font partie des architectes du Web et sont proches de la technologie, ils gèrent une activité stratégique sur Internet. C'est eux qui postent les dispositions les plus détaillées et qui somme toute poussent le principe de transparence assez loin, il faut bien le reconnaître. Ce sont ces sites qui offrent également des liens divers à la fois internes pour des questions techniques ou pour l'un d'entre eux avec des organismes extérieurs comme l'EFF (*Electronic Frontier Foundation*) ou l'EPIC (*Electronic Privacy Information Center*). Tous les sites qui déclarent adhérer à TRUSTe font partie de ce groupe. Les sites des deux *Credit Bureaus* présents dans l'échantillon ont aussi des dispositions sur la vie privée très détaillées, mais cela procède en partie d'une autre logique (FCRA).

- *Les dispositions contractuelles* : il s'agit là de sites dont les dispositions concernant la vie privée sont intégrées sous forme de clauses dans des conditions contractuelles ; ces conditions encadrent généralement une inscription à un forum de discussion, à un service de *push* d'information, un abonnement à l'édition électronique d'un journal, un achat *on line.* Elles se présentent sous deux formes :

  – Dans une version concentrée, tout d'abord, généralement sous la forme d'un ou deux paragraphes en haut ou en bas d'un formulaire où le visiteur s'apprête à saisir des données personnelles ; les sites français de l'échantillon notamment utilisent plus volontiers cette formule et font en quelques mots une double référence à la loi nationale et au droit d'accès et de rectification.

  – Sous une forme détaillée à travers des CGU ; les dispositions concernant la vie privée cohabitent alors avec d'autres domaines du droit : droit commercial applicable, responsabilité civile, indemnisation, copyright. Elles décrivent les données collectées, les traitements et les cessions éventuelles à des tiers que le site *Web* pourrait ou au contraire s'interdit de faire. Les restrictions que s'impose un site prennent ici l'apparence d'un véritable engagement sur des enjeux consistants en matière de vie privée ; c'est notamment à travers une clause de ce type qu'un site de l'échantillon, spécialisé dans le tourisme et affilié au CRS (*Computer Reservation System*) américain SABRE, s'engage à ne pas communiquer à des tiers non parties à la transaction les données relatives aux réservations aériennes passées par les clients du site.

***Les insuffisances de contenu des* "privacy statements"**

Au total et malgré un choix sélectif des sites de l'échantillon, le bilan que l'on peut faire du contenu des "*privacy statements"* est assez contrasté. On peut observer qu'environ un bon tiers des sites ne sont pas très explicites quant aux données collectées, plus de la moitié n'abordent pas la question des *clickstream data* et des traitements dont elles font l'objet. Un tiers encore n'offrent pas de possibilités

d'*opt-out* ni de droit d'accès, près d'un quart enfin ne font figurer aucune adresse physique permettant au visiteur de savoir à qui il a affaire et d'exercer un recours éventuel par des voies de transmission traditionnelles.

Les références à des codes de conduite

Trois sites parmi l'échantillon font référence à des codes de conduite professionnels spécifiant un certain nombre de garanties et d'engagements en matière de protection de la vie privée des consommateurs : les trois sites en question sont des sites commerciaux, l'un canadien, l'autre américain, et l'autre français ; ils s'appuient tous trois sur le code de conduite de leur association nationale des professionnels du marketing direct. Notre propos n'est pas de porter un jugement sur le fait que ces codes de conduite sont adéquats ou pas ; on s'est plutôt attaché à vérifier si les dispositions contenues dans ces codes sont correctement mises en pratique par les sites Web qui s'en réclament. L'analyse nous conduit à faire les observations suivantes :

- Le site canadien est un serveur commercial ; il se réfère explicitement (avec hyper-lien) au code d'éthique de la CDMA (*Canadian Direct Marketing Association : Code of Ethics & Standard of Practice)* qui a été récemment amendé de manière à intégrer des dispositions spécifiques concernant le commerce en ligne. Ce code contient notamment des dispositions assez protectrices concernant le recueil du consentement du consommateur pour la transmission d'offres commerciales par *e-mail*, et l'obligation d'information en matière de traitement des *clickstream data*. Autant il apparaît très clairement que ce deuxième principe est remarquablement bien traité par le site en question à travers un FAQ très détaillé sur les *cookies*, autant le premier apparaît, à la lumière de l'étude, complètement passé sous silence et aucun dispositif d'*opt-out* n'est proposé.

- Le site américain est celui d'un des deux *Credit Bureaus* sélectionnés dans l'échantillon ; il déclare adhérer à la DMA (*Direct Marketing Association)*[3] et fournit un lien avec le site de cette organisation. Les principes de la DMA américaine sont sensiblement différents et de prime abord moins contraignants que ceux établis par l'association voisine du Canada. Ils sont dans l'ensemble correctement appliqués par le *Credit Bureau* à son site Web, qui par ailleurs n'utilise pas la technique des *cookies*. Deux réserves cependant doivent être formulées : les traitements opérés à partir des fichiers de *login* ne sont pas suffisamment détaillés ; d'autre part, alors que les principes de la DMA insistent particulièrement sur la nécessité de faire figurer la notice d'information sur les pratiques de collecte et de traitement de données sur la page même où l'information est collectée, il ressort de l'étude du site que cette suggestion n'est pas correctement mise en pratique ; de plus la formulation de l'opt-out *on line* est fortement encouragée par la DMA alors que le site n'offre qu'une possibilité par courrier sans que cela non plus soit rappelé sur les supports de collecte. On note cependant qu'une fois l'*opt-out* enregistré par le *Credit Bureau*, il devient définitif alors que sa durée de vie n'est que de 5 ans selon les standards de la DMA.

3. C.f. The DMA's Marketing Online Privacy Principles and Guidance.

- Le site français est un grand magasin spécialisé dans la vente de livres et de CD. Il déclare sur son site être adhérent au code professionnel national du Syndicat des Entreprises de Vente par Correspondance (SEVPCD). Ce code de bonne conduite rappelle un certain nombre de dispositions de la loi française en matière de protection des données et développe toute une déontologie quant au traitement des demandes de radiation des fichiers, quant à l'information préalable des prospects, l'exposé des finalités, la mise à disposition des données à des tiers, etc. Un rapide examen permet de noter que le site n'est pas parfaitement conforme aux suggestions, ne serait-ce que par rapport à l'article 3.4 qui stipule que les traitements doivent être régulièrement déclarés à l'autorité nationale (CNIL) ; or, le site Web de ce magasin n'a pas à ce jour fait l'objet d'une démarche spécifique allant dans ce sens, le magasin en question considérant qu'il est en règle dans le cadre d'une déclaration globale réalisée au niveau du groupe pour toute son activité de marketing direct.

LES TECHNOLOGIES DE SECURITE ET DE CONTROLE DES DONNEES

La sécurisation des paiements

Sécurité des systèmes

Sur les 34 sites de l'échantillon qui vendent effectivement des produits ou des services à travers leur site *Web*, une très forte majorité recourt au protocole de paiement SSL *(Secure Socket Layers*) implémenté sur des serveurs sécurisés. Ce point est aisément vérifiable dans la mesure où tout le processus d'achat se déroule sur le *browser* de l'utilisateur, l'icône de sécurité en position verrouillée. Quelques sites se sont dotés de dispositifs additionnels :

- un site italien par exemple utilise le système de certification de Verisign ;
- tous les sites français utilisent l'architecture nationale centralisée de télé-autorisation des paiements par cartes ; on assiste ainsi au cours d'un processus de paiement *on line* à un reroutage de la connexion sur un des centres informatiques ad hoc qui fournit alors à l'opérateur du site un numéro d'autorisation et valide la transaction ; le système est fait de telle sorte que les établissements financiers n'ont pas la connaissance du contenu du panier des achats, ce qui n'est probablement pas le cas avec les systèmes de cartes de paiement *co-branded* entre VISA et AOL ou Yahoo !

Un site spécialisé dans la vente de CD offre la possibilité de transmettre le numéro carte de crédit via un *e-mail* crypté à l'aide du système PGP[4]; il peut être déclenché au moment du paiement.

Sécurité des procédures

Quelques sites proposent des solutions simples à mettre en œuvre et de nature à renforcer la confidentialité des paiements *on line*. Deux ou trois sites demandent par exemple au visiteur de préciser, soit lors de l'inscription, soit lors du paiement le nom de jeune fille de la mère ; cette collecte d'information peut apparaître curieuse ou disproportionnée : en réalité elle sert à authentifier un client qui aurait égaré un mot de passe et qui souhaiterait pourtant accéder à son compte (*customer account*). On notera que cette procédure n'a rien d'exceptionnel, elle est notamment appliquée par les grands opérateurs de carte de crédit dans le cadre des déclarations de perte faites au téléphone.

Un autre site, spécialisé dans la gestion et la valorisation de portefeuilles boursiers prodigue des conseils basiques mais non moins pertinents à ses visiteurs qui souhaiteraient préserver une certaine

4. PGP est un logiciel qui utilise le chiffrement pour protéger le secret des correspondances électroniques et les données stockées sur un disque dur d'ordinateur. Cela peut aussi être utilisé pour "signer électroniquement" des données à fin de rapporter la preuve de leur authenticité et/ou de leur intégrité.

confidentialité à leur navigation ; il recommande par exemple de fermer le browser à la fin de leur vacation et de vider le répertoire cache à la fin de la vacation afin d'éliminer toute trace des informations financières personnelles qui ont été affichées.

Enfin trois sites proposent un système qui devrait être fortement encouragé pour tout le commerce électronique grand public : il s'agit d'une option laissée au libre choix du client consistant à demander au site de conserver son ou ses numéros de cartes de paiement dans un portefeuille personnel qu'il héberge. De la sorte, lorsque le client revient sur le site pour faire un achat, il n'a qu'à choisir une des ses cartes qu'on lui propose avec seulement les quatre derniers chiffres. Ainsi un numéro de carte n'aura circulé qu'une seule fois sur le réseau lors de l'exécution du premier achat. Ces sites déclarent prendre des précautions particulières de stockage de la base de données des numéros cartes sur un *non-networked computer*.

L'exercice du droit d'accès

L'exercice du droit d'accès appliqué par les visiteurs des sites Internet peut être vu à la fois comme un moyen de contrôler les informations personnelles collectées mais aussi de s'assurer qu'elles sont tenues à jour et le cas échéant de demander à ce qu'elles soient corrigées. Plus de la moitié des sites étudiés offrent un droit d'accès individuel et pour un quart seulement ce droit peut s'exercer *on line,* c'est à dire que la demande et la réponse sont exécutables en temps réel au cours d'une connexion et d'un dialogue entre le *browser* et la plate-forme serveur. Cette procédure n'étant techniquement pas très compliquée à mettre en œuvre, on peut s'étonner du fait qu'elle ne soit pas plus généralisée. Il est enfin manifeste que les sites américains de l'échantillon sont ceux qui ont la propension la plus faible à offrir à leur visiteur la possibilité d'exercer leur droit d'accès.

Les systèmes de contrôle des données (PETs)

On a recensé dans l'inventaire une série d'instruments technologiques qui peuvent être mis à la disposition des utilisateurs d'Internet afin de protéger la confidentialité de leurs données personnelles ou de leur navigation. Ces technologies, principalement OPS (*Open Profiling Standard*) et P3P (*Platform for Privacy Preferences*) sont encore en gestation et c'est probablement ce qui explique qu'un seul des sites de l'échantillon recourt explicitement à l'une de ces solutions. Il s'agit d'une librairie *on line* américaine qui exploite le système Firefly. Ce système s'appuie sur une technologie dite de *collaborative filtering* à laquelle, il faut bien le reconnaître, n'adhèrent aujourd'hui guère plus d'une trentaine de sites. On doit noter que cette société vient d'être rachetée très récemment par Microsoft. Concrètement le système offert à ce jour fonctionne sur le principe d'un tiers de confiance : l'utilisateur d'Internet délivre sur le site de Firefly ses informations personnelles (identification + centres d'intérêts) et définit pour chacune un statut privé ou public, cela constitue son passeport. Lorsqu'il se connecte sur un site adhérent au réseau Firefly il n'a plus qu'à saisir son mot de passe Firefly et le site récupère automatiquement les données publiques de son passeport. Le visiteur bénéficie des engagements de confidentialité définis dans le "*Privacy Statement"* de Firefly (droit d'accès, droit de rectification on line, recueil du consentement préalable pour la transmission de l'adresse *e-mail* à des tiers, interdiction de recherche inversée -- *reverse searches* -- pour identifier le titulaire d'une adresse *e-mail*, droit de réponse, recours). Enfin le visiteur en retire un avantage en terme de contenu puisque le site, sur la base de son profil et de la définition de ses préférences va pouvoir désormais lui transmettre des informations ciblées ; dans le cas de la librairie *on line* de

l'échantillon, cela se traduit par l'affichage d'une page d'accueil personnalisée et par la transmission par courrier électronique d'information sur les nouveautés et sur les auteurs. Il est curieux toutefois que le site ne mette nulle part en valeur son utilisation de Firefly, si ce n'est une minuscule icône en bas d'un écran.

RECOURS ET RESPONSABILITES

Les voies de recours proposées

On a recensé à travers le dernier chapitre de l'inventaire, les différents mécanismes nationaux fondés sur la loi ou sur l'autorégulation susceptibles de contraindre les sites *Web* à appliquer leurs obligations en matière de traitement de données personnelles et de protection de la vie privée ; certains de ces instruments constituent également une voie de recours possible permettant aux visiteurs des sites *Web* qui s'estimeraient lésés d'introduire une instance.

Il ressort de l'analyse qu'à peine dix sites sur les 50 étudiés dans l'échantillon proposent à leurs visiteurs ou clients des possibilités de recours en cas de désaccord. Quatre niveaux de recours doivent être distingués :

- Un recours par *e-mail* pour traiter tout problème qui pourrait survenir dans une livraison par exemple, dans la qualité du produit ou dans la facturation. Appliquant un standard mondial en matière de vente à distance, la plupart des sites ont une politique de retour. D'une manière générale étant donné que tous les sites donnent leur adresse *e-mail*, on peut considérer que ce moyen de communication peut être systématiquement utilisé par les visiteurs pour faire part de leurs questions ou de leurs désaccords avec telle ou telle pratique.

- Un recours financier : un site commercial italien, prend l'engagement de dédommager un client à hauteur de US$50 en cas d'une utilisation frauduleuse de sa carte de paiement à la suite d'un achat online qu'il a effectué sur le site et dans la mesure où l'institution qui a délivré la carte maintient à la charge du client une part de responsabilité.

- Un recours devant un arbitre : le site d'une banque française comporte une page dédiée aux voies de recours amiable possible via son service clientèle pour régler tout différend pouvant survenir avec un client. Cette offre est large et ne s'adresse pas seulement aux désaccords éventuels qui pourraient résulter de l'utilisation de son site *Web*.

- Un recours devant les tribunaux : quelques sites enfin, les journaux en ligne notamment, font figurer dans leur contrat une clause d'attribution de juridiction qui désigne l'institution judiciaire compétente pour traiter un différend entre les deux parties.

Les responsabilités en matière de respect de la vie privée

Les sites de l'échantillon qui acceptent de se considérer explicitement comme responsables de l'application de leur "*Privacy Policy Statements*" sont fort peu nombreux ; ils sont sept en tout et pour tout et encore convient-il de remarquer que cette spécification de responsabilité ne concerne assez souvent que la limitation des transmissions de données à des tiers.

Cela pose bien évidement la question de la valeur de ces engagements. Cette étude des sites *Web* ne permet pas à ce niveau d'apporter une réponse à cette interrogation. Toutefois la connaissance de certaines pratiques conduit à relativiser la portée des déclarations des opérateurs de site, et même dans certains cas, celle de leurs engagements contractuels.

Des exemples récents montrent en effet que certains sites, contraints à rechercher toutes les sources possibles d'équilibre économique, n'hésitent pas à se lancer dans des opérations marketing contraires à leurs engagements vis à vis de leurs abonnés. Le cas le plus connu est celui d'une campagne de *phoning* qu'un grand fournisseur de service avait envisagé de lancer au cours de l'été l'année dernière. Ce projet supposait la cession à des firmes de marketing direct d'une liste de numéros de téléphone personnels de plusieurs centaines de milliers d'abonnés du service alors que contractuellement la collecte de ces numéro était destinée exclusivement à permettre de prévenir les abonnés en urgence en cas d'utilisation frauduleuse de leur accès et de leur moyen de paiement. Dans le même temps le fournisseur de service modifiait discrètement et unilatéralement ses *Terms Of Service* afin de rajouter le numéro de téléphone parmi la liste des données qu'il s'autorisait à transmettre à des tiers à des fins de prospection commerciale. Manifestement cette opération révélait une double entorse aux principes établis : c'était à la fois un détournement de finalité et une absence d'information directe et loyale des personnes concernées[5]. Dans ce cas précis il est révélateur que ce ne sont autres que la pression du marché, c'est à dire la colère des membres, leurs menaces de désabonnement et les sarcasmes de quelques leaders d'opinion, qui ont poussé ce grand opérateur à renoncer à appliquer ce plan.

5. C.f. Serge Gauthronet : "*Les services en ligne et la protection de la vie privée – Rapport n° 2 – Etudes de cas*" - Commission des Communautés Européennes – ETD/96/B-3000/142 - Bruxelles - Décembre 1997 – (à paraître).

CONCLUSION

La conclusion la plus saillante que cette étude permet de tirer est celle d'un décalage marqué entre d'une part le monde des institutions et des organisations diverses qui développent une pensée et des instruments de protection des données et celui d'autre part du monde des sites *Web*. Ces derniers, quelle que soit leur sincérité et leurs bonnes intentions à l'égard de leurs visiteurs, donnent en effet aujourd'hui l'impression, dans leur grande majorité, de méconnaître les enjeux en matière de protection de la vie privée et de flux transfrontaliers et surtout de manquer d'orientations précises et homogènes applicables sur les réseaux en ligne.

Aussi il a paru utile de dégager des suggestions de portée générale qui correspondent à quelques bonnes pratiques que l'on a pu relever ou *a contrario* que l'on peut déduire des insuffisances et des carences qui persistent à travers les sites analysés.

Sans prétendre à l'exhaustivité, ni voir une quelconque intention de priorité dans leur classement autre que celle qui découle de la chronologie de ce rapport, on peut donc formuler, dans l'esprit à la fois d'une bonne application des principes de l'OCDE et de la promotion d'un environnement de confiance pour le commerce électronique, les dix séries de suggestions jointes en annexe 1.

ANNEXE 1

SUGGESTIONS POUR UN DESIGN *PRIVACY FRIENDLY* DES SITES *WEB*

1. Cookies

- Le visiteur d'un site Web doit être informé de la finalité de la collecte et des traitements de données relatifs aux *cookies* au moment où ceux-ci sont placés dans le fichier correspondant de son *browser*.

- La durée de conservation des *cookies* et plus largement de toute information personnelle doit être définie et non excessive ; une durée de vie d'un ou deux ans semblerait acceptable ; des durées plus longues peuvent être admises en fonction de la durée du contrat liant un utilisateur et un service en ligne sur lequel il se connecte régulièrement : dans ce cas la durée de conservation doit être proportionnelle à la durée pendant laquelle la prestation est fournie, plus une période d'environ un an pour régler les contestations éventuelles liées à la facturation ou à des fins de reconquête du client.

- L'implantation de *cookies* en rafale provoquant un effet de saturation chez le visiteur devrait être résolument déconseillée.

- Lorsqu'un utilisateur a formulé une première fois son refus d'acceptation d'un *cookie*, le site Web devrait cesser définitivement ses tentatives d'implantation.

- Aucun lien de subordination ne devrait exister entre le fait d'accepter un *cookie* ou plus largement de transmettre des informations personnelles et la possibilité de naviguer librement à travers les pages et les rubriques publiques d'un site Web.

- L'information sur les finalités des *cookies* doit être sincère et complète : elle doit permettre notamment de distinguer les finalités et les traitements de données selon que les *cookies* sont implantés par les sites eux-mêmes ou par des agences de publicité.

- L'information doit également comporter des indications précises sur l'existence de *matchings* entre les données d'identification (voir suggestion numéro8) et les données navigationnelles issues des *cookies*.

2. Messages électroniques (E-mail)

- Toute transmission de message de demande d'informations à un site dévoile indirectement l'adresse *e-mail* de l'émetteur ; dans le cadre d'une obligation de conseil, il est de la responsabilité des sites d'en avertir leurs visiteurs.

3. Formulaires

- Les informations facultatives collectées à travers les différents formulaires (inscriptions, enquêtes, feed-back, paiement) doivent être clairement séparées des informations obligatoires et regroupées dans un bloc distinct.

- Si des données sensibles sont collectées de manière légitime, le site doit s'engager à respecter à leur égard le plus haut niveau de sécurité et de confidentialité.

4. Cession de données à des tiers et opposition (opt-out)

- Tout site qui collecte des données personnelles doit offrir à ses visiteurs une possibilité d'*opt-out* en ligne.

- Les possibilités d'*opt-out* doivent pouvoir s'exercer directement et simultanément à la collecte au moyen d'un cochage de case sur les formulaires de collecte même.

- L'exercice de l'*opt-out*, dans les cas où cela s'impose, doit distinguer à quels traitements il s'applique : aux traitements commerciaux réalisés par le site lui-même, aux traitements d'analyse navigationnelle, aux extractions de listes destinées à des tiers et aux *matchings* dont ces listes pourraient faire l'objet par la suite.

- L'*opt-out* doit pouvoir s'exercer également en direction des agences de publicité qui réalisent des ciblages *one-to-one* ; à cette fin les sites Web doivent pouvoir soit s'engager à recueillir cet *opt-out* et à le transmettre à l'agence, soit fournir un hyper-lien qui permette de se connecter directement sur la bonne page du site publicitaire afin que l'utilisateur puisse lui-même exécuter la procédure.

- Tout site qui, après s'être engagé à ne fournir aucune donnée personnelle à des tiers, souhaite néanmoins le faire, doit obtenir le consentement préalable de la personne concernée. Une modification unilatérale des *Terms Of Service* n'est en aucun cas suffisante.

5. Education/Information

- Tout site Web se référant à l'application d'un instrument international ou régional de protection des données est encouragé à faire expressément référence à cet instrument et à fournir un hyper-lien avec le site de l'organisation concernée.

- Tout site Web opérant à partir d'un pays qui dispose d'une loi nationale en matière de protection des données doit y faire référence formellement et dans le cadre de la politique générale d'information et d'éducation des utilisateurs, fournir un hyper-lien avec le site de l'autorité administrative responsable de la bonne application de ladite loi. Il y a à cet égard une nécessité pressante que chaque autorité de protection des données existant dans le monde soit présente sur le Web à travers des sites pertinents, documentés et interactifs.

- Tout site Web se réclamant d'un instrument professionnel ou sectoriel doit fournir un hyper-lien avec le texte du code auquel il est fait référence et avec le site de l'organisation professionnelle responsable de sa bonne application.

6. Transparence des sites

- Quel que soit l'instrument international ou national dont ils se réclament, les sites doivent, parce qu'ils opèrent à l'échelle mondiale, se doter de "*privacy statements*" accessibles en ligne par leurs visiteurs.

- Les "*privacy statements*" accessibles en ligne doivent au minimum être explicites quant aux données collectées, quant à leur justification, quant à l'utilisation des *clickstream data* et des traitements dont elles font l'objet et quant aux possibilités d'*opt-out*.

- La mention faisant référence aux "*privacy statements"* doit figurer explicitement et de manière visible sur le *homepage* de chaque site concerné.

- Tout site implanté dans un pays où la loi nationale exige une déclaration préalable des traitements doit mentionner le numéro de récépissé délivré par l'autorité compétente.

- Tout site se réclamant de l'application d'un code de bonne conduite sectoriel doit le mettre en œuvre scrupuleusement dans la totalité de ses dispositions.

7. Sécurité

- Les sites commerciaux qui offrent des procédures de paiements *on line* doivent obligatoirement mettre à niveau leur plate-forme serveur de manière à intégrer aussitôt qu'ils sont disponibles et éprouvés les moyens les plus sécurisés.

- Les sites commerciaux qui offrent à la vente des produits ou des services achetables pour de petits montants doivent accepter les moyens de paiement anonymes.

- Dans le cadre de leur obligation de conseil à leurs visiteurs, les sites qui traitent des données confidentielles doivent alerter leurs visiteurs quant aux risques de divulgation de leurs données qui existent localement sur leur micro-ordinateur (historique des consultations, fichier cache).

- En l'absence pour l'instant de sécurité absolue en matière d'authentification des paiements et de transmission de données sur le réseau, les sites commerciaux qui acceptent les paiements *on line* à l'aide de cartes bancaires peuvent configurer leur système de telle sorte à ne réclamer qu'une seule fois les coordonnées de la carte à la condition impérative de stocker cette information dans des fichiers hautement sécurisés, sur des ordinateurs non-connectés au réseau *(non-networked computers)*.

8. Droits individuels

- Tous les sites pratiquant le commerce électronique doivent offrir à leurs clients des procédures de recours par *e-mail.*

- Tous les sites collectant des données personnelles doivent fournir à leurs visiteurs identifiés la possibilité d'exercer leur droit d'accès *on line ;* à défaut ce droit doit pouvoir s'exercer *off line* et dans ce cas l'adresse postale du site doit figurer en bonne place.

- Le droit d'accès doit pouvoir s'exercer de manière complète et ne pas être limité aux seules données fournies par les visiteurs du site. Si des données sont collectées ou générées par ailleurs, si par exemple des profils de navigation ou d'achat sont constitués, les visiteurs exerçant leur droit d'accès doivent également avoir communication de cette information et notamment du segment comportemental dans lequel ils sont classés.

- Au cas où l'information demandée à travers l'exercice du droit d'accès ne serait matériellement pas possible à transmettre, le site doit motiver sa réponse dans des formes précises et intelligibles à un non-initié.

9. Technologies protectrices de la vie privée (Privacy Enhancing Technologies)

- Les sites Web doivent s'engager à mettre en œuvre sur leur plate-forme serveur, aussitôt qu'elles seront disponibles et éprouvées, les solutions techniques de protection des données personnelles intégrées aux *browsers (PETs),* dès lors que ces solutions apportent une réponse aux suggestions ci-dessus et permettent aux utilisateurs de définir et rectifier au coup par coup la délivrance de leur données personnelles en fonction des différentes catégories de destinataires possibles.

10. Responsabilité

- Tous les sites Web collectant des données personnelles doivent formellement admettre le principe de leur responsabilité pleine et entière par rapport à la sécurité, à la confidentialité et à tous les engagements pris de façon déclarative ou contractuelle quant à ces données et à leurs traitements.

ANNEXE 2

ETUDE RELATIVE A DES PRATIQUES EN MATIERE DE PROTECTION DE LA VIE PRIVEE EFFECTUEE SUR UN ECHANTILLON DE SITES WEB SITUES DANS DIVERS PAYS MEMBRES DE L'OCDE

Méthodologie de constitution de l'échantillon

Compte tenu des conditions de réalisation de l'étude et du délai imparti (1 mois), il n'a pas été possible de construire un échantillon de sites Web statistiquement significatif et représentatif au plan mondial.

La démarche suivie a donc été résolument différente et s'est démarquée des initiatives passées ou en cours sur le même sujet, notamment, l'étude de l'EPIC qui avait ciblé les 100 *hot sites* ou celle en cours de la FTC aux Etats-Unis qui annonce un travail de diagnostic sur 1.200 sites Web.

Le parti a été pris de s'intéresser à des sites commerciaux qui affichaient des pratiques convenables en matière de protection des données dans un triple objectif :

- montrer qu'il n'y a pas d'antinomie entre commerce en ligne et protection de la vie privée;
- recenser et mettre en avant les bonnes pratiques qui seraient identifiées ;
- analyser les carences et proposer le niveau ad hoc qui devrait pouvoir être généralisable.

Cette démarche a soulevé un problème de qualification préalable des sites et un niveau minimum a été défini pour qu'un site soit accepté dans l'échantillon. Vu les contraintes de délai, certains sites très visités, cités par le "Top 100 web sites" (100hot Web Sites, Web21) ont été inclus dans l'échantillon ainsi que des sites proposés par des spécialistes (experts ou autorités de protection des données) des pays Membres de l'OCDE qui présentaient un intérêt particulier au regard de la collecte et du traitement des données personnelles.

La démarche de constitution de l'échantillon a pris en compte trois familles de critères :

Critère n°1 : des sites commerciaux

Ont été ciblés les sites commerciaux du secteur privé qui pratiquent le commerce en ligne ou qui collectent des données personnelles en ligne, quel que soit le type de biens ou de services proposés.

Critère n° 2 : des sites implantés dans les diverses zones de l'OCDE

Bien qu'en majeure partie les sites commerciaux soient encore d'origine nord américaine, l'intérêt de cette étude était d'observer en quoi les dispositions de protection des données des différents pays Membres de l'OCDE étaient ou n'étaient pas reflétées dans la conception des sites et dans le protocole relationnel avec les clients. Il était donc impératif de diversifier les sources d'observation et d'incorporer dans l'échantillon des sites commerciaux ayant une implantation d'origine dans différents pays Membres de l'OCDE.

En consequence, ont été retenus 50 sites selon le schéma de répartition géographique suivant :

Etats-Unis :	23 sites
Canada	5 sites
Union Europeenne dont : - Allemagne 1 - Danemark 1 - Espagne 2 - Finlande 2 - France 6 - Italie 2 - Royaume-Uni 2	16 sites
Japon	2 sites
Australie	3 sites
Mexique	1 site

Critère n°3 : des sites proposant des biens ou des services diversifiés

La plupart des secteurs commerciaux, même les plus inattendus, sont présents sur Internet, mais il était illusoire de prétendre tous les couvrir à travers notre étude. Aussi l'observation a été concentrée sur quatre principales catégories de sites :

- Des sites commerciaux pour lesquels Internet est un facteur de réussite spectaculaire ou est en passe de devenir le principal vecteur de distribution. Ces sites à fort trafic, étaient les plus susceptibles d'avoir pris des dispositions en matière de protection de la vie privée concernant leurs clients ; en particulier, ont été retenus trois secteurs :

  – la vente de matériel informatique
  – la vente de logiciels
  – la vente de livres et de disques.

- Des sites à fortes potentialités commerciales sur le Web et traditionnellement enclins à développer des politiques sophistiquées de marketing direct ; ont ainsi été retenues trois activités :

- le tourisme
- le transport et la billetterie aérienne
- la finance.

- Des sites proposant des produits ou services dont le contenu peut être plus ou moins directement révélateur de la situation personnelle des visiteurs ; ont été sélectionnées trois séries de sites commerciaux :

  - la presse et les magazines en ligne
  - les sites de jeu
  - les sites de services Internet, comme les services "e-mail"et la publicite en ligne.

- Des sites grand public liés au commerce de détail (et généralement intégrés dans des *mall*) ; ont été retenus les deux secteurs suivants :

  - le textile, l'habillement et les accessoires
  - l'equipement sportif et les jouets.

Echantillon retenu

Country	Name	URL	Description	Language
Australia	Fairfax@Market	http://www.market.fairfax.com.au/	Classified ads	Engl
Australia	Qantas	http://www.qantas.com.au/	Airline	Engl
Australia	Traveland	http://www.ansett.com.au/traveland.html	Travel services	Engl
Canada	Royal Bank	http://www.royalbank.com/	Bank	Engl Fr
Canada	Globe & Mail Employment service	http://careers.theglobeandmail.com/	Newspaper employment service	Engl
Canada	Mountain Equipment Co-op	http://www.mec.ca/	Outdoor equipment supplier	Engl
Canada	Hudson's Bay Co.	http://www.hbc.ca	Trading	Engl Fr
Canada	CANOE (CANadian Online Explorer)	http://www.canoe.ca	News, entertainment	Engl Fr
Denmark	Lego	http://www.lego.com	Toys	Engl German Danish Fre
Finland	Iltalehti	http://www.itlalehti.fi	Newspaper	Finnish
Finland	VIP Hiusklubi	http://www.hairstore.fi/~vip/	Hair products	Finnish
France	Decathlon	http://www.decathlon.com	Sporting goods	Fre Engl
France	CPR Bourse	http://www.cprbourse.tm.fr/	Financial svcs.	Fre Engl (only welcome)
France	Société Générale	http://www.socgen.com	Banking svcs.	Fre Engl (incomplete)
France	FNAC	http://www.fnac.fr		Fre
France	CNP	http://www.cnp.fr	Insurance / savings inst.	Fre
France	Les Echos	http://www.lesechos.fr	Newspaper	Fre
Germany	Der Spiegel	http://www.spiegel.de	News	German
Italy	Mollificio Lamperti Srl	http://www.lamperti.it/	Coil springs manufacturer	Italian
Italy	Ego	http://www.ego1997.com	Clothing	Engl
Japan	Japan Catalogue (Mitsubishi)	http://www.japan-cata.com	Japanese products	Japanese
Japan	G-Square	http://www.gsquare.or.jp	Info. svc. provider; on-line shopping	Japanese
Mexico	Infosel	http://www.infosel.com.mx/	News service	Spanish
Spain	Banesto	http://www.banesto.es/	Bank	Spanish Engl
Spain	El Corte Inglés	http://www.elcorteingles.es	Retail	Spanish
United Kingdom	Financial Times	http://www.ft.com	Newspaper	Engl
United Kingdom	Economist	http://www.economist.com		Engl
United States	3M	http://www.mmm.com		Engl
United States	Amazon	http://www.amazon.com	Book seller	Engl
United States	ATT	http://www.att.com/	Telecom	Engl
United States	Barnes and Noble	http://www.BarnesandNoble.com	Book seller	Engl
United States	Nashbar	http://www.nashbar.com	Bikes / volleyball eqpt.	Engl
United States	CDNow	http://www.cdnow.com	Music	Engl
United States	CNet	http://www.cnet.com/		Engl
United States	Double Click	http://www.doubleclick.net/	Internet advertising	Engl Jap Span Fre Port Ital Swed
United States	Excite	http://www.excite.com/	Search	Engl Dutch Fre German Swed Jap
United States	First Virtual	http://www.firstvirtual.com/	E-messaging	Engl
United States	Galoob	http://www.galoob.com	Toys	Engl
United States	IBM	http://www.ibm.com/		Engl
United States	Infoseek	http://www.infoseek.com	Search engine	Engl Fre Port Dan Ger

				Spa Ital Jap Dutch Swe
United States	Intel	http://www.intel.com	Microprocessors	Engl (+ others)
United States	McGraw-Hill	http://www.mcgraw-hill.com/index.html	Publishing	Engl
United States	Microsoft	http://www.microsoft.com		Engl
United States	National Credit Information Network	http://www.social-security-number.com/ncihome.htm	Credit reporting	Engl
United States	NBC	http://www.nbc.com	TV	Engl
United States	Netscape	http://www.netscape.com		Engl
United States	Travelocity	http://www.travelocity.com/	Travel services	Engl
United States	HotWired	http://www.hotwired.com		Engl
United States	Yahoo	http://www.yahoo.com	Search engine	Engl Jap Ger Swe Dan Fre Kor
United States	Experian	http://www.experian.com	Credit reporting	Engl

	YES	NO	No answ.
1) DOES THE SITE REFER TO OR UTILISE ANY OF THE FOLLOWING:	**24**		
Specific Laws And Other Legal Instruments			
International Instruments (e.g. EU Directive)			
National Laws			
Contractual Agreements			
Self Regulation And User Empowerment Technologies			
Compliance with Specific Codes of Conduct or Guidelines:			
Government Model Codes			
Industry Codes			
Auditing and Certification			
TRUSTe			
Audits by Accounting Firms			
BBBOnline			
Personal Preference Settings and Labelling			
P3P (formerly OPS)			
PICS			
Personal Data Control Technologies			
Digital certificates			
2) DOES THE SITE SET "COOKIES"?	**31**	**19**	**0**
If so:			
a) Are the cookies being set by the site itself or by an advertising entity?	*Itself: 22. Both: 7.*		
b) What is the [average] expiration date of the cookie(s)?	*End 1999 (20 months)*		
c) How many times does the site attempt to set cookies?	*10 or more (often at each link).*		
d) Can you enter the site if you refuse the cookie?	29	1	1
3) DOES THE SITE ASK VISITORS TO SUPPLY PERSONAL DATA THROUGH THE USE OF REGISTRATION FORMS, ORDER FORMS, MAILING LISTS, QUESTIONNAIRES OR SURVEYS, AND/OR REQUESTS FOR FEEDBACK OR COMMENT?		**3**	
a) What specific personal information is requested?	*Name, address, e-mail.*		
b) Does the site offer free information or services in exchange for personal data?	28	18	4
c) Is the information requested proportional in value to the information or services received or necessary to complete a specific transaction (e.g. home address for delivery)?	32	7	11
d) Is any of the information requested optional?	29	7	14

	YES	NO	No answ.
4) DOES THE SITE HAVE A PRIVACY POLICY?	**38**	**11**	**1**
If so,			
a) Is information about the Privacy Policy available online? (Please print a copy.)	38	2	10
b) Is it easy to find?	28	10	12
i) is it accessible from the homepage?	21	17	12
ii) if not, is it found as a "key word" using the site's search engine?	5	8	37
5) IS NOTICE GIVEN CONCERNING THE TYPES OF PERSONAL INFORMATION COLLECTED?	**28**	**17**	**5**
6) IS NOTICE GIVEN REGARDING THE COLLECTION OF E-MAIL ADDRESSES OR OTHER PERSONAL INFORMATION COLLECTED AUTOMATICALLY FROM A VISITOR'S BROWSER?	**15**	**33**	**2**
7) IS NOTICE GIVEN CONCERNING THE USE OF THE PERSONAL INFORMATION COLLECTED?	**39**	**9**	**2**
8) CAN VISITORS REFUSE AND/OR "OPT-OUT OF" CERTAIN USES OF THEIR PERSONAL INFORMATION?	**26**	**18**	**6**
9) CAN INDIVIDUALS ACCESS THEIR PERSONAL INFORMATION FOR VERIFICATION AND CORRECTION ?	**28**	**17**	**5**
If yes, briefly describe how (i.e. online mechanisms; off-line contact information)			
10) DOES THE SITE OFFER GOODS OR SERVICES FOR PURCHASE?	**34**	**15**	**1**
If so,			
a) Does the site offer a secure electronic payment mechanism?	28	7	15
Mostly secure server.			
b) What specific personal data is requested during the payment process?	*Name, address, e-mail, credit card (# and expiration date).*		
11) DOES THE SITE MENTION THE USE OF SECURITY MEASURES, EITHER AT THE POINT OF PAYMENT, OR AS PART OF A PRIVACY POLICY OR A SEPARATE "SECURITY STATEMENT"? (This could include operational or managerial measures, the use of encrypted data storage or transit, or securing payment).	**27**	**16**	**7**
12) DOES THE SITE DISPLAY A PRIVACY ICON OR TRUSTMARK?	**4**	**43**	**3**
13) DOES THE SITE GIVE INFORMATION ABOUT INTERNAL OR EXTERNAL AUDITING PROCEDURES?	**4**	**41**	**5**
14) DOES THE SITE REFER OR LINK TO A DATA PROTECTION REGISTRATION BODY OR OTHER INDEPENDENT REGULATORY BODY?	**7**	**40**	**3**
	1/4 of European sites; 1/8 for US.		

	YES	NO	No answ.
15) DOES THE SITE CLEARLY GIVE INFORMATION ABOUT RECOURSE IN THE CASE OF DISAGREEMENT? (If so, briefly describe.)	**10**	**34**	**5**
16) IS RESPONSIBILITY FOR COMPLIANCE WITH PROVISIONS OF THE PRIVACY POLICY SPECIFIED?	**7**	**34**	**9**
17) IS A PHYSICAL ADDRESS GIVEN FOR CONTACTING THE SITE?	**36**	**12**	**2**
18) IS AN EMAIL ADDRESS GIVEN FOR CONTACTING THE SITE?	**50**	**0**	**0**