RFC 6462 : Report from the Internet Privacy Workshop

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 janvier 2012

Date de publication du RFC : Janvier 2012

https://www.bortzmeyer.org/6462.html

Après une très longue période d'ignorance quasi-complète des problèmes de protection de la vie privée, l'IETF a évolué et on n'entend plus gère ses participants écarter d'un revers de main ces questions, en disant « Nous, on fait juste de la technique, tout ça, c'est de la politique, ça ne nous concerne pas. » De nos jours, au contraire, la prise de conscience est nette et l'IETF a désormais une activité structurée autour de la notion de vie privée, activité qui se traduit par un programme dédié <http://www.iab.org/activities/programs/privacy-program/> et une liste de diffusion <https://www.ietf.org/mailman/listinfo/ietf-privacy>. Faut-il aller plus loin ? C'était une des questions posées lors de l'Atelier « "*Internet Privacy Workshop 2010*" <http://www.iab.org/activities/workshops/internet-privacy-workshop-2010/> », atelier qui s'est tenu du 8 au 9 décembre 2010 à Cambridge et dont ce RFC est le compte-rendu. (L'auteure travaille pour une ONG qui lutte pour les libertés sur l'Internet.)

Pas de décisions à attendre tout de suite, donc. On en est à un stade d'exploration. L'atelier de Cambridge était coorganisé par l'IETF, le MIT et le W3C pour voir ce que les SDO pouvaient faire en terme de protection de la vie privée. On est loin d'un accord unanime (et le résumé du RFC dit bien qu'aucun des organismes présents n'a de position officielle sur ces questions) mais au moins quelques pistes de travail émergent. L'IETF étant chargé de produire des spécifications concrètes, une bonne partie de l'atelier a porté, non pas sur des discours généraux sur la vie privée, mais sur les tâches envisageables.

La question de la protection de la vie privée sur l'Internet est immense et couvre beaucoup de domaines très différents. Certains problèmes apparaissent de manière récurrente, le "*fingerprinting*" (la détermination d'une identité à partir de traces numériques qui n'étaient a priori pas conçues pour cela), la fuite d'informations, la difficulté à distinguer les partenaires primaires (à qui on a donné directement de l'information) des tiers (qui ont eu de l'information sans qu'on interagisse explicitement avec eux), le manque d'informations des utilisateurs sur les avantages et inconvénients d'une meilleure protection, etc. (Notons que le RFC mentionne les faiblesses des utilisateurs, mais pas l'aggressivité avec laquelle les capitalistes collectent et revendent de l'information privée.) Le RFC note que la vie privée n'est pas

un absolu et que, par exemple, la protéger peut influer négativement sur l'utilisabilité d'un service. Bref, il y a pour l'instant davantage de défis que de solutions (section 1).

Plus précisement, de quoi a-t-on parlé pendant l'atelier (les supports présentés sont disponibles en ligne <http://www.iab.org/activities/workshops/internet-privacy-workshop-2010/slides/>) ? La section 2 résume tout cela. D'abord, une discussion technique (section 2.1). Commençons par l'adresse IP. Elle donne souvent bien trop d'informations (il est trivial de remonter d'une adresse IP à un utilisateur, ce qui explique pourquoi elle est considérée comme une donnée personnelle <http://www.cnil.fr/dossiers/internet-telecoms/fiches-pratiques/article/ladresse-ip-est-une-do>). Certains protocoles offrent des risques particuliers comme certaines techniques de mobilité, qui permettent de suivre un utilisateur à la trace.

C'est d'ailleurs dans le cas de l'adresse IP qu'on trouve un des rares exemples d'une technologie IETF spécialement développée pour répondre à des craintes concernant la vie privée : les adresses IP temporaires du RFC 4941 [1], qui sont partiellement aléatoires, et regénérées de temps en temps, pour éviter le suivi de l'utilisateur.

Autre mécanisme bien connu pour empêcher le suivi par l'adresse IP : le routage en oignon, surtout connu grâce à Tor. Ce service route les paquets à travers plusieurs nœuds distincts, chiffrant leur contenu à chaque fois. Seuls les premiers et derniers nœuds voient le message en clair. Observer le trafic ne permet de trouver, au pire, que l'origine (si on espionne au début), ou bien que la destination (si on espionne à la fin).

Mais Tor n'est pas parfait : le contenu des messages peut donner des indications sur l'origine ("*cookies*", par exemple, pour une requête HTTP). Si on veut vraiment être anonyme, utiliser Tor ne suffit pas : il faut aussi couper bien des choses sur son navigateur, à commencer par Flash et JavaScript, et certains peuvent considérer cela comme un problème. Comme souvent en sécurité, rien n'est gratuit. Protéger sa vie privée peut nécessiter des sacrifices.

Les participants à l'atelier ont également planché sur le mode "*private browsing*" qu'offrent certains navigateurs. C'est un mode dans lequel le navigateur ne stocke pas localement les identifiants de session (comme les "*cookies*"). Son but n'est pas de protéger contre un suivi de l'utilisateur par le serveur mais de protéger contre d'autres utilisateurs du même poste client. L'expérience indique que beaucoup d'utilisateurs ne comprennent pas la différence et croient que le "*private browsing*" leur procure une navigation sans flicage. C'est un exemple d'un autre problème courant en sécurité : les utilisateurs ne comprennent pas les risques.

Enfin, dernière discussion technique, sur les propositions "*Do Not Track*", qui permettent à un utilisateur d'indiquer clairement aux sites Web qu'il ne veut **pas** être suivi à la trace. Pour l'instant, ce ne sont que des propositions, sans accord technique ou politique.

Après ces discussions techniques, l'atelier s'est demandé quel pouvait être le rôle des SDO dans cette histoire. Dans le passé, il n'y a pas eu d'appproche systématique de la vie privée dans les protocoles IETF. Cela ne veut pas dire que rien n'a été fait : certains RFC ont été entièrement conçus pour résoudre un problème de vie privée (comme le RFC 4941 pour IPv6 ou le RFC 3323 pour SIP). Certains services particulièrement sensibles ont bénéficié de davantage d'efforts, par exemple l'indication de présence (RFC 2778) ou bien sûr la géolocalisation (RFC 3693). Un protocole comme ALTO (RFC 5693)

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc4941.txt

a également vu ses problèmes de vie privée étudiés dès le début. Le cas d'ALTO est difficile car le protocole est d'autant plus efficace que l'utilisateur révèle beaucoup de choses sur lui (en demandant à l'oracle « Je veux télécharger le fichier `Serge Reggiani - Les Loups Sont Entrés Dans Paris.mp3` de taille 4732679 octets et de MD5 `2d79e0d7e25c8c10c9879cefcef4102a` et voici la liste complète des pairs BitTorrent qui l'ont » par rapport au plus discret mais moins efficace « je voudrais savoir si le pair `2001:db8:1::1` est plus ou moins rapide que le `2001:db8:67e::34a:1ff3` »).

La protection de la vie privée a pas mal de rapports avec la sécurité (la section 8 discute du rapprochement de ces deux concepts) et la sécurité est un bon exemple d'une préoccupation transverse (elle affecte tous les protocoles) qui était largement ignorée au début de l'IETF et a vu son rôle de plus en plus pris en compte. L'IETF a ainsi bâti une culture de la sécurité. Ainsi, depuis le RFC 1543, tous les RFC doivent inclure une section "*Security Considerations*" pour exposer l'analyse sécurité du protocole. Elle peut être vide mais elle doit être présente avec une mention expliquant pourquoi les auteurs du RFC ont consciemment laissé la section vide. Cette obligation bureaucratique n'est évidemment pas suffisante et l'IETF a ajouté une direction de la sécurité <`http://trac.tools.ietf.org/area/sec/trac/wiki/SecurityDirectorate`>, un RFC dédié pour guider les auteurs de RFC (RFC 3552), de nombreux tutoriels pour auteurs de RFC aux réunions physiques, etc. La même méthode peut-elle être appliquée à la vie privée ? (Le RFC 2828, qui rassemble la terminologie IETF sur la sécurité, contient des termes liés à la protection de la vie privée.)

Le W3C a également procédé à un effort semblable. Un de ses premiers grands efforts a été P3P, un mécanisme pour permettre aux sites Web d'exprimer de manière formelle leur politique de gestion des données personnelles. P3P est un langage riche, qui permet d'indiquer des politiques complexes. Mais il a été très peu adopté en pratique. Opinion personnelle : comme pour la neutralité du réseau <`https://www.bortzmeyer.org/neutralite.html`>, tout le monde prétend que l'information du consommateur résout tous les problèmes, qu'il suffit d'annoncer sa politique et que le marché choisira. Mais personne ne veut le faire réellement. P3P permettait d'exprimer les politiques de protection des données personnelles en des termes simples et non ambigus et c'était évidemment intolérable pour les e-commerçants, qui préfèrent infliger à l'utilisateur des "*privacy policies*" de vingt pages écrites en langage légal.

Après ce tour d'horizon du travail effectué et des acteurs en place, l'atelier s'est attaqué aux défis (section 3). Quels sont les grands problèmes à résoudre ?

D'abord, la trop grande facilité à identifier un utilisateur donné par les informations que donne le logiciel qu'il utilise : adresse IP, champs de la requête HTTP comme `User-Agent:` ou `Accept-Language:`, "*cookies*" (RFC 6265), et plein d'autres paramètres font qu'on peut identifier un utilisateur ou une machine bien trop souvent. C'est ce qu'on nomme le "*fingerprinting*" et c'est bien démontré par le Panopticlick <`http://panopticlick.eff.org/`>.

Comme dans toute réunion de "*geeks*", les participants à l'atelier ont évidemment pris plaisir à explorer en détail des techniques de "*fingerprinting*" particulièrement rigolotes comme d'envoyer du code JavaScript qui va transmettre au serveur la liste des polices installées dans le navigateur (elle est souvent unique).

Capturés par un simple script WSGI sur le serveur (testez-le en <`https://www.bortzmeyer.org/apps/env`> ; les variables d'environnement dont le nom commence par `HTTP_` sont les en-têtes de la requête HTTP), voici une partie de ce qu'envoie un Firefox typique, depuis une machine Ubuntu :

```
HTTP_ACCEPT_CHARSET: ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_USER_AGENT: Mozilla/5.0 (Ubuntu; X11; Linux i686; rv:8.0) Gecko/20100101 Firefox/8.0
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE: en-us,en;q=0.5
HTTP_ACCEPT_ENCODING: gzip, deflate
```

Cette combinaison d'options et de numéros de version est probablement unique, ou en tout cas rare sur le Web, et identifie donc assez bien une machine (sans même avoir besoin de "*cookie*"). Une telle combinaison a par exemple déjà été utilisée pour confondre un agresseur <http://reflets.info/le-pur-fail-agenceh-hadopi-eurorscg/> agissant pour le compte de l'industrie du divertissement.

Ces informations n'étaient **pas** prévues pour cet usage (par exemple, les adresses IP étaient prévues pour router les paquets, pas pour identifier une machine ou une personne). Mais remplacer ces informations par des mécanismes qui empêchent ou limitent le "*fingerprinting*" ne sera pas trivial. D'autant plus que pas mal de gens se sont habitués à les utiliser dans ce but et qu'il sera de plus en plus difficile de revenir en arrière. Ainsi, le "*fingerprinting*" est souvent utilisé pour détecter des fraudes, ou pour fournir du contenu adapté (et le RFC, qui est gentil et évite les sujets qui fâchent, ne cite pas les applications répressives du "*fingerprinting*", pour identifier l'auteur d'un délit abominable, comme de partager des œuvres d'art). Il y aura probablement beaucoup de désaccords sur le compromis entre vie privée et service « amélioré » grâce au "*fingerprinting*".

Au minimum, l'IETF et le W3C vont essayer de documenter les points qui, dans les protocoles courants (TCP, HTTP, SIP), facilitent le "*fingerprinting*".

Un problème proche est celui de la fuite d'informations (section 3.2) : des mécanismes conçus pour des motifs tout à fait honorables transmettent néanmoins plus d'information qu'ils ne le devraient. Ainsi, le champ `Referer:` dans une requête HTTP permet de savoir d'où vient un visiteur Web (ce qui est utile) mais révèle également des choses comme les ID de session (lorsqu'ils sont mis dans l'URL), les termes de recherche utilisés <https://www.bortzmeyer.org/je-parle-a-mon-moteur-de-recherche.html>, etc. Voici un exemple vu dans le journal de mon blog (les informations trop sensibles ont été modifiées). On voit les termes de recherche utilisés dans Google :

```
192.0.2.70 - - [16/Dec/2011:17:08:53 +0000] "GET /1383.html HTTP/1.0" 200 3291 "http://www.google.fr/url?sa=
```

Le contrôle sur les données privées repose normalement sur la possibilité de distinguer les récepteurs primaires des données des tiers (section 3.3). Ainsi, si je me connecte sur SeenThis <https://www.bortzmeyer.org/seenthis.html>, ce site est récepteur primaire de mes données et je ne suis pas surpris qu'il récolte des informations sur moi. Il s'agissait d'un choix conscient et informé de ma part. Mais l'examen du code source de ce site montre qu'il fait appel au service Google Analytics et donc, sans l'avoir demandé, sans même le savoir, je transmets également des données à Google, un tiers qui peut alors récolter des données sans que je l'ai choisi.

Le cas ci-dessus est relativement simple. Mais dans le Web d'aujourd'hui, on trouve d'autres cas où la distinction entre destinataire primaire et tiers est moins évidente. Un utilisateur qui met un "*widget*" amusant sur une page peut le considérer comme primaire alors que le navigateur (par exemple pour retourner les "*cookies*") le traitera comme un tiers, et l'inverse existe également.

Enfin, le dernier grand défi est celui de l'information de l'utilisateur (section 3.4). La plupart du temps, le flicage de ce dernier se fait discrètement, sans qu'il se rende compte de l'immense quantité de données qui est collectée à son insu. La seule information disponible est composée de « "*policy statements*" » écrits dans un jargon juridique délibérement confus, conçu pour protéger le patron de l'entreprise et pas pour informer l'utilisateur. Le RFC note que des informations cruciales (comme la durée de conservation des données) en sont souvent absentes. Opinion personnelle : c'est pour cela que les mécanismes du marché - l'entreprise publie sa politique et le consommateur est libre de continuer ou pas - ne fonctionnent pas et qu'il faut des lois comme la loi I&L. Le marché suppose une information parfaite et des acteurs symétriques, ce qui n'est pas du tout le cas ici.

Le problème est d'autant plus sérieux que, si le technicien se doute bien de tout ce que le site Web peut apprendre sur son visiteur, l'utilisateur ordinaire n'a souvent pas pas idée de la quantité de traces numériques qu'il laisse.

Il est donc nécessaire de travailler à une meilleure information. P3P était un bon effort dans ce sens. Mais comme c'était un langage riche, il était difficile de traduire une politique P3P de manière claire pour l'utilisateur. Les efforts actuels portent plutôt sur un nombre limité d'icônes qui pourraient devenir largement connues (un panneau « danger, ici votre vie privée est menacée »...) Un exemple est le projet Common Terms <https://www.iis.se/en/internet-for-alla/internetfonden/commonterms>.

La section 4 étudie ensuite les défis liés au déploiement des bonnes pratiques. D'abord (section 4.1), le problème que les mesures techniques sont génériques, alors que les menaces effectives sont souvent spécifiques à un contexte donné. La vie privée n'est pas un concept binaire. Il y a d'autres stades que « complètement privé » et « public ». Mais il est très difficile de traiter cette complexité par des mesures techniques.

Par exemple, les solutions situées en couche 3 comme les adresses IP temporaires du RFC 4941 résolvent certes certains problèmes (le serveur qui reconnaît un visiteur récurrent uniquement sur son adresse) mais ne protège pas du tout contre un FAI ou un État qui essaie d'associer une adresse à un utilisateur. Selon la menace envisagée, ces adresses temporaires sont donc efficaces... ou pas du tout.

Il ne faut donc pas évaluer les solutions techniques en leur demandant de résoudre tous les problèmes possibles. Il ne serait pas raisonnable pour l'IETF d'exiger de ses protocoles qu'ils empêchent complètement toute atteinte à la vie privée. Il faut plutôt dire clairement quels sont les risques et qui (le programmeur, l'utilisateur, la loi) est chargé de les traiter.

Autre problème délicat de déploiement de solutions de protection de la vie privée : la tension entre l'utilisabilité et la protection (section 4.2). Comme souvent en matière de sécurité, il va falloir faire des choix douloureux. Les tenants du Roi Marché ont beau jeu de faire remarquer que les utilisateurs, lorsqu'ils ont le choix, vont vers les services qui violent le plus leur vie privée (Facebook, Google, etc) en échange d'applications sympas et qui brillent. La principale faiblesse de cet argument est qu'il suppose que l'utilisateur est parfaitement conscient des risques, et de ce qui peut lui arriver, ce qui est très optimiste.

Un bon exemple de ce compromis est donné par Tor. Celui-ci fournit une bonne protection mais complique et ralentit (en raison du nombre d'étapes de routage) la navigation. Résultat, il reste peu utilisé, en bonne partie parce que les utilisateurs font un calcul coût/bénéfice (peu informé, d'ailleurs) et décident que leur vie privée n'est pas assez importante pour justifier ce coût.

Avec Tor, le coût de la protection est élevé. Mais même des mesures bien plus légères ont des coûts. Supprimer l'en-tête `Referer:` des requêtes HTTP améliore certainement la protection. Mais certains sites Web proposent une vue différente selon la valeur de ce champ et, en le supprimant, on se prive de ce service. Reste à savoir qui va décider du compromis, et sur quelles informations : comment exposer ce choix (« "*Do not send Referer headers*" ») dans une interface utilisateur, de manière qui permette un choix raisonné ? Alors même que l'effet de ce choix va dépendre des sites (dans la plupart des cas, le `Referer:` est inutile au client Web.)

Ces problèmes d'utilisabilité sont cruciaux. Le RFC cite l'exemple de SIP, où un mécanisme normalisé de protection des requêtes contre l'écoute existe (RFC 3261, section 23) mais il n'est pas utilisé en pratique car trop contraignant.

Dernier obstacle au déploiement de techniques respectant davantage la vie privée, la difficulté à trouver les bonnes motivations (section 4.3). Les différents acteurs impliqués ne feront pas d'effort s'ils n'ont pas une motivation pour cela. Cela peut être la crainte du gendarme, la conviction que cela leur apportera plus de clients ou simplement le souci d'utiliser les meilleures techniques (ces trois motivations sont rarement présentes en même temps). La crainte du gendarme est discutée en section 4.3.1. Traditionnellement, beaucoup de services proposés sur l'Internet sont gratuits et la possibilité de vendre les données personnelles des utilisateurs est l'une des voies les plus évidentes pour gagner de l'argent. Comme l'illustre un dessin célèbre <http://www.ethannonsequitur.com/facebook-you-customer-product-pigs.html>, « soit l'utilisateur est le client, soit il est la marchandise ». Dans un tel contexte, il n'y a pas de motivation économique à respecter la vie privée, bien au contraire. Les diverses autorités de régulation ont fini par froncer les sourcils, ce qui a mené les fournisseurs de ces services à publier de longues politiques d'utilisation des données sur leur site. Comme le note le RFC, ces politiques, écrites sans effort pédagogique, visent plutôt à protéger le fournisseur du service qu'à informer correctement et complètement l'utilisateur. Le RFC note à juste titre que ces problèmes ne se corrigeront pas tout seuls et qu'une approche régulatrice est nécessaire (cf. le rapport de la FTC de 2010 <http://www.ftc.gov/opa/2010/12/privacyreport.shtm> sur l'importance d'avoir des politiques publiques mieux écrites).

Le RFC soutient que cette tendance doit continuer : sans forte pression des régulateurs, de la loi, le patronat Internet va toujours essayer de concéder le moins de vie privée possible aux utilisateurs. Un exemple d'une telle pression est la directive européenne qui parle des cookies <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML>, indiquant qu'ils ne doivent pas être utilisés sans le consentement des utilisateurs.

Le cas de P3P, déjà cité, est un bon exemple de ce problème des motivations (section 4.3.2). L'idée de base était que les logiciels du côté du client allaient pouvoir lire et comprendre les politiques de protection de la vie privée et automatiquement réagir (par exemple en n'envoyant pas de "*cookies*" aux sites dont la politique était trop peu protectrice de la vie privée). C'est une idée très états-unienne : les acteurs libres s'informent mutuellement de leurs pratiques et décident ensuite librement, en adultes majeurs, informés et consentants, de poursuivre ou pas la relation. Si on croit qu'il y a égalité (d'information, de moyens de traitement, de pouvoir) entre le patron de Facebook et M. Michu, utilisateur de Facebook, cela peut marcher. Sinon, on préfère l'approche européenne où certaines pratiques sont interdites, qu'il y ait ou pas consentement de la marchandise, pardon, de l'utilisateur.

Donc, P3P permettait d'automatiser ce processus d'information et de décision. Microsoft a pris une décision importante en choisissant, dans Internet Explorer 6, de n'envoyer des "*cookies*" aux tiers que si ceux-ci avaient une politique P3P. Comme n'importe quelle politique, même outrageusement prédatrice, était acceptée par Internet Explorer, la plupart des sites Web se sont pliés à cette décision et ont copié/collé la première politique P3P qu'ils trouvaient (souvent l'exemple pris sur le site du W3C). Cette expérience menée grâce à Internet Explorer (les autres auteurs de navigateurs n'ont fait aucun effort et n'ont jamais intégré P3P) a permis de mettre en évidence une limite de P3P : le site qui publie sa politique peut mentir (« Nous ne vendons pas vos données personnelles »). Aucun mécanisme légal ou autre ne l'en empêche. (Voir par exemple l'article « "*Token Attempt : The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens*" <http://www.cylab.cmu.edu/research/techreports/2010/tr_cylab10014.html> ».)

Le cas illustre bien la question des motivations : pour qu'ils reçoivent des "*cookies*" d'Internet Explorer, les sites devaient publier du P3P. Alors, ils l'ont fait (motivation technique). Il n'y avait pas de pression légale ou régulatrice pour dire la vérité dans ces politiques P3P, alors ils ne l'ont pas fait (pas de motivation légale). Les clients (en partie à cause de l'absence de gestion de P3P par les navigateurs) ne donnaient pas la préférence aux sites publiant du bon P3P, alors les sites n'ont pas cherché à l'améliorer (pas de motivation commerciale).

Il sera intéressant de voir si cela marche mieux en sens inverse : pour la géolocalisation, le RFC 4119 et le RFC 6280 fonctionnent de manière opposée à P3P, en permettant aux **utilisateurs** d'indiquer leurs choix en matière de protection des données personnelles. Ils sont normalement plus motivés que les entreprises capitalistes pour cela.

Bien sûr, on est ici très loin des questions techniques que se posent normalement les SDO. Mais la compréhension de ces enjeux économiques et légaux est nécessaire, si on veut que les futures techniques de protection de la vie privée aient plus de succès que P3P.

Conclusion, en section 5, quel est le plan d'action pour les SDO ? Pour l'IETF, la synthèse est que cela va être compliqué. L'IETF normalise des protocoles dans les couches basses, sans présupposer d'un usage particulier, alors que les menaces pour la vie privée sont très dépendantes du contexte. Il va donc être difficile de trouver des réponses générales, dans les protocoles IETF. Cela ne veut pas dire qu'il ne faut rien faire. Le travail a déjà commencé autour d'une série de recommandations pour les auteurs de RFC (rassemblées dans le "*Internet-Draft*", `draft-morris-privacy-considerations`, qui a évolué depuis et a été publié en RFC 6973).

Les participants à l'atelier étaient tous d'accord sur la nécessité de poursuivre également le travail technique, par exemple sur les leçons apprises de Tor, ainsi que sur les capacités (plus fortes que prévues) de "*fingerprinting*" des protocoles existants.

Et le W3C ? Il est probablement mieux placé pour améliorer la protection de la vie privée, puisque les normes du W3C sont plus proches de l'utilisateur, et utilisées dans un contexte plus spécifique. Contrairement à l'IETF, le W3C peut se restreindre au Web.

L'annexe A résume quels sont les documents bruts disponibles pour ceux qui veulent approfondir leur connaissance des travaux de cet atelier :

— Les minutes des discussions <`http://www.iab.org/activities/workshops/internet-privacy-worksh minutes/`>,
— Les présentations <`http://www.iab.org/activities/workshops/internet-privacy-workshop-2010/ slides/`>,
— Et les article soumis <`http://www.iab.org/activities/workshops/internet-privacy-workshop-201 papers/`> (l'annexe C du RFC en contient la liste) comme le « "*Thoughts on Adding "Privacy Considerations" to Internet Drafts*" » d'Alissa Cooper (l'auteure du RFC <`http://www.cdt.org/personnel/alissa-cooper`>) et John Morris.