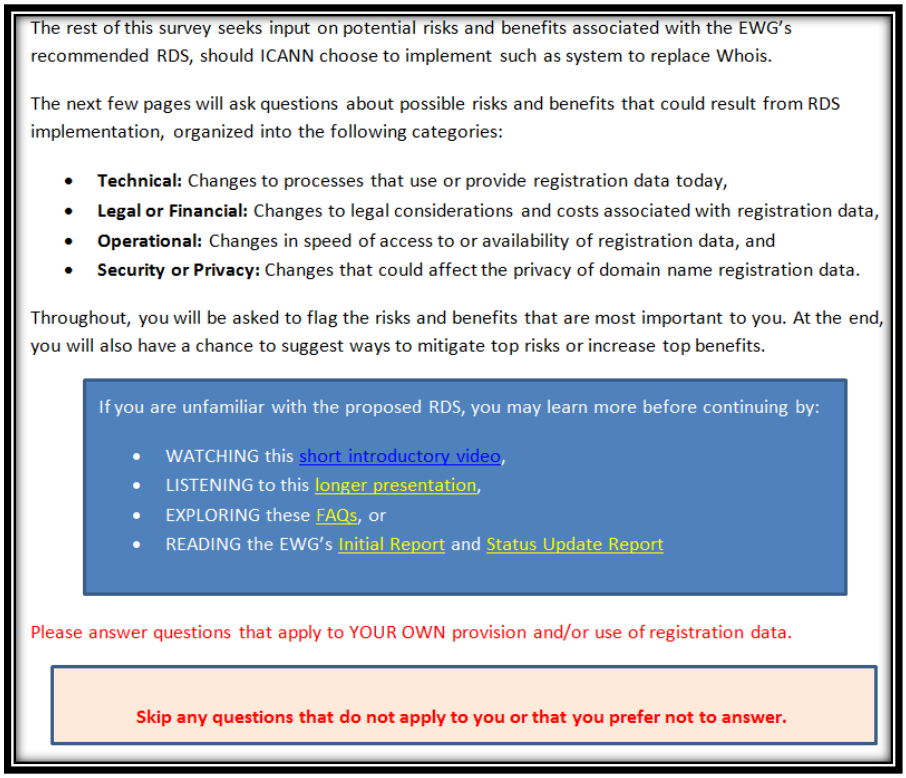
Enquête sur les risques liés au RDS - Résumé des résultats

Le 14 mars, le groupe de travail d'experts sur les services d'annuaire des gTLD (EWG) a invité toutes les parties qui fournissent ou utilisent des données d'enregistrement de noms de domaine gTLD à participer à une enquête sur les risques du RDS, y compris les titulaires de noms de domaine, les bureaux d'enregistrement, les registres et le vaste éventail d'individus, d'entreprises et d'autres organisations consommatrices des données du WHOIS aujourd'hui. Cette enquête à offert aux participants l'occasion d'interpeller l'EWG à propos des risques et des bénéfices que le **service d'annuaire des données d'enregistrement de prochaine génération (RDS)** pourrait représenter.

Ce document résume les risques et les bénéfices du RDS identifiés à travers ce sondage. L'EWG a utilisé les réponses obtenues pour identifier et réduire les risques imprévus et inutiles lors de la préparation de son rapport final (publié le 6 juin 2014). L'EWG a également recommandé que ces réponses soient tenues en compte lors d'une future évaluation complète des risques du RDS proposé.

Conception du sondage

L'introduction ci-dessous a établi le contexte pour ceux qui ne sont pas familiarisés avec le RDS en organisant les risques et les bénéfices en 4 catégories :



The rest of this survey seeks input on potential risks and benefits associated with the EWG's recommended RDS, should ICANN choose to implement such as system to replace Whois.

The next few pages will ask questions about possible risks and benefits that could result from RDS implementation, organized into the following categories:

- **Technical:** Changes to processes that use or provide registration data today,
- **Legal or Financial:** Changes to legal considerations and costs associated with registration data,
- **Operational:** Changes in speed of access to or availability of registration data, and
- **Security or Privacy:** Changes that could affect the privacy of domain name registration data.

Throughout, you will be asked to flag the risks and benefits that are most important to you. At the end, you will also have a chance to suggest ways to mitigate top risks or increase top benefits.

If you are unfamiliar with the proposed RDS, you may learn more before continuing by:

- WATCHING this short introductory video,
- LISTENING to this longer presentation,
- EXPLORING these FAQs, or
- READING the EWG's Initial Report and Status Update Report

Please answer questions that apply to YOUR OWN provision and/or use of registration data.

Skip any questions that do not apply to you or that you prefer not to answer.

Pour chaque catégorie, un exemple des risques et des bénéfices potentiels ont été présentés aux personnes interrogées qui ont été invitées à :

- *sélectionner TOUS les risques techniques qui pourraient potentiellement VOUS affecter*
- *sélectionner les DEUX (2) risques qui, à votre avis, pourraient avoir le plus grand impact*
- *sélectionner les DEUX (2) risques les plus probables*
- *sélectionner PARMI les nouveaux risques introduits, liés au RDS, tout risque n'étant pas encore associé au WHOIS.*

-- Publié le 28 juillet 2014 --

Enquête sur les risques liés au RDS - Résumé des résultats

Les personnes interrogées sont également encouragés à ajouter d'autres risques et bénéfices potentiels. Ce récapitulatif des réponses au sondage identifie les risques et les bénéfices le plus souvent mentionnées, ainsi que ceux qui y viennent s'ajouter.

Présentation de la réponse

Cette enquête sur les risques du RDS a été réalisée en anglais. Cent quatre-vingt-deux réponses partielles ont été reçues depuis le 12 juin 2014. Un peu plus de 100 personnes interrogées ont répondu au sondage complet.

Toutes les réponses, sauf une, ont été soumises avant la publication du rapport Final de l'EWG. Dans ce contexte, ces résultats offrent des commentaires sur le RDS tel qu'il a été proposé dans le rapport mis à jour de l'EWG (11 novembre 2013) et présenté lors de la 48e réunion de l'ICANN à Buenos Aires. Ces résultats ne devraient pas être considérés comme des commentaires sur les propositions finales du RDS détaillées dans le rapport de juin 2014 de l'EWG. Cependant, ces réponses ont aidé l'EWG à comprendre les risques et les bénéfices que les utilisateurs et les fournisseurs de données Whois trouvent potentiellement significatifs, ayant un impact et étant associés à *tout* service d'annuaire des données d'enregistrement de prochaine génération.

Distribution géographique des personnes interrogées

- Représentation globale, y compris l'Amérique du Nord (68 %), l'Europe (35 %), l'Asie (20 %), l'Amérique latine (14 %), l'Afrique (12 %) et l'Océanie (10 %)[1]
- Equitablement réparties entre les UTILISATEURS et les FOURNISSEURS de données d'enregistrement :
    - quatre vingt quatre pour cent des données d'enregistrement obtenues à travers le système WHOIS.
    - 63 % correspond aux données d'entrée et 24 % recueille, conserve ou transmet des données Whois
    - les UTILISATEURS de ces données incluent les titulaires de nom de domaine (45-57 %), les utilisateurs d'Internet individuels (50 %), les utilisateurs commerciaux d'Internet (50 %), le personnel technique d'Internet (40 %), les chercheurs d'Internet (41 %), les chercheurs OpSec (36 %), les détenteurs de la propriété intellectuelle (27 %), d'autres chercheurs (14 %), les agences d'application de la loi (5 %) et environ 20 autres.
    - les FOURNISSEURS des données incluent les personnes physiques (65 %), les personnes morales (59 %), les bureaux d'enregistrement (14 %), les opérateurs de registre (9 %), les fournisseurs de services d'enregistrement fiduciaire (5 %) et des tierces parties (5 %).

Risques techniques du RDS

- Possibles **effets techniques négatifs** le plus souvent invoqués (104 réponses) :
    1. je risque de ne plus accéder de façon anonyme et publique à toutes les données d'enregistrement (69).

[1] Remarque : Il est permis de donner plusieurs réponses ; le total dépasse 100 %

2. l'accréditation nécessaire pour accéder aux données sécurisées pourrait être difficile à obtenir (65).
3. mes pratiques en matière d'accès aux données d'enregistrement pourraient devoir changer (62).

- Risques identifiés comme les plus importants / les plus probables : les numéros 1 et 2 cités précédemment.
- Au-delà des risques expressément énumérés, des risques opérationnels supplémentaires ont été identifiés :
  - le nouveau RDS peut avoir un impact sur les parties qui fournissent le Whois historique et inversé (8)
  - L'accès automatisé ne plus être disponible (6)
  - Il est impossible d'obtenir des informations sur des criminels, des partenaires commerciaux ou des candidats (3)
  - Le délai d'exécution pour l'obtention de données ou l'enregistrement pourrait augmenter (2)
  - Les droits de la vie privée peuvent être violés (2)
  - Source unique de défaillance / risques techniques SAC061 (2)
  - Information en masse pour l'application de la loi et les spammeurs, deux groupes qui risquent de faire l'objet d'abus
  - Les données publiquement accessibles disparaîtront
  - [Connexions] Je peux les utiliser mais elles doivent être modifiées au départ et après en raison de la rotation
  - Transfert / migration
  - Question inter juridictionnelle introduite
  - Aucun examen public des données aux bureaux d'enregistrement connus pour être tolérants de fausses données
  - Les modifications apportées aux données d'enregistrement peuvent exiger des certificats SSL
  - Rompt le modèle délégué de DNS
  - Je perds la visibilité de la journalisation sur qui accède à mes données personnelles dans certaines circonstances
  - Je perds la possibilité de contrôler directement ou de limiter l'accès à mes renseignements
  - Le développement, l'assurance qualité, la révision et mise à jour des coûts, avec aucun revenu pour les compenser

  Remarque générale : tous ces risques techniques ont été identifiés par les personnes interrogées, mais un grand nombre sont en fait couverts par d'autres types de risques considérés ailleurs dans cette enquête.

Bénéfices techniques du RDS

- Possibles **effets techniques négatifs** le plus souvent invoqués (89 réponses) :

1. les données d'enregistrement auxquelles j'aurai accès pourraient être plus exactes (58).
2. l'accès aux données d'enregistrement pourrait être plus uniforme et cohérent (56).
3. je pourrais avoir un meilleur accès aux données sécurisées dont j'ai vraiment besoin (41).

- Bénéfices identifiés comme ayant plus d'impact ou étant plus probables : les numéros 1 et 2 cités précédemment
- Outre les bénéfices répertoriés explicitement, des prestations techniques supplémentaires ont été identifiées :
  - amélioration de l'exactitude des données (grâce à la gestion des contacts et à la validation) (8)
  - mes données pourraient être accessibles pour ceux ayant le droit légal plutôt que d'être publiées pour que tout le monde puisse les voir
  - je peux identifier plus facilement les récidivistes et les cyber squatteurs en série avant que je commence une action en justice ou que je dépose une plainte UDRP, pour économiser l'argent et les ressources de mes clients
  - je devrai fournir toujours le port 43 Whois et ce n'est pas grand-chose
  - les données d'enregistrement accédées seraient vraisemblablement plus applicables, utiles et significatives
  - le transfert de domaine entre les titulaires de noms de domaine sera plus facile (les données WHOIS resteront les mêmes, aucune analyse de sortie Whois ne sera plus nécessaire)
  - impact négatif en raison de la grande échelle des données réduites - Exemple : moins de courrier indésirable

Risques juridiques ou financiers du RDS

- Possibles **effets juridiques et financiers négatifs** le plus souvent invoqués (102 réponses) :
  1. le nombre de données d'enregistrement disponible publiquement pourrait diminuer (68).
  2. le coût total pour obtenir des données d'enregistrement risque d'augmenter (66).
  3. la journalisation des accès ou les notifications du RDS pourraient compromettre les enquêtes en cours (61).
- Risques identifiés comme ayant plus d'impact ou étant plus probables : le numéro 1 cité précédemment
- Au-delà des risques expressément énumérés, des risques juridiques et financiers supplémentaires ont été identifiés :
  - les fraudeurs de marques ou les spammeurs pourrait être plus difficiles à retrouver. (3)
  - le temps nécessaire pour accéder aux données pourrait être retardé (3)
  - sans un accès public à toutes les données, les innovations à valeur ajoutée risquent de devenir moins rentables.
  - trop de nouveaux TLD conduisent à une augmentation des coûts et à beaucoup d'enregistrements de mauvaise foi.

- le manque de transparence des propriétaires de sites Web (en particulier pour les sites commerciaux avec des transactions monétaires ou des entrées de données à caractère personnel) peut devenir un risque pour les consommateurs.
- il peut s'avérer difficile de confirmer les informations sur les autres domaines du titulaire lors de la confirmation d'éligibilité dans le domaine limité.
- la défaillance ne serait pas localisée. Un seul objectif pour des « attaques » juridiques, au DOS, contrôle ou autres.
- je pourrais être tenu de fournir des informations inexistantes (par ex. adresse réelle, oui, il y a des gens sans domicile fixe qui ont enregistré des noms de domaine)
- la création d'un monopole sur les données Whois va étouffer l'innovation et centraliser trop de pouvoir sur l' « annuaire téléphonique » de l'Internet en un seul endroit.
- dans certaines situations, il y a des parties des données que je voudrais partager, même avec des personnes qui pourraient autrement être fiables.
- je veux que mes données Whois soient disponibles pour toutes les parties intéressées telles qu'elles sont aujourd'hui
- les registres dans l'Union européenne et dans d'autres endroits ayant des lois de protection des données ne seront pas en mesure d'exporter des données vers le RDS, ce qui va éroder considérablement son utilité.
- la charge des coûts et les inconvénients juridiques potentiels affectant les titulaires de nom de domaine, les bureaux d'enregistrement et les opérateurs de registre peuvent avoir un bénéfice minimal pour les parties concernées et des bénéfices maximaux pour d'autres.

Bénéfices juridiques ou financiers du RDS

- Possibles **effets juridiques et financiers positifs** le plus souvent invoqués (68 réponses) :
  1. l'amélioration de la qualité des données d'enregistrement pourrait réduire des inefficacités qui s'avèrent coûteuses (42).
  2. les procédures d'exécution contractuelle liées aux obligations en matière de données seraient plus robustes (35).
  3. je pourrais plus facilement obtenir un accès légal aux données d'enregistrement sécurisées (35).
- Bénéfices identifiés comme les plus importants / les plus probables : les numéros 1 et 2 cités précédemment
- Au-delà des bénéfices expressément énumérés, des bénéfices juridiques et financiers supplémentaires ont été identifiés :
  - mon risque d'avoir une grande quantité de données personnelles (y compris les données commerciales impliquant des individus) diminuera considérablement.
  - établir facilement des connexions entre les propriétaires du domaine et découvrir des réseaux
  - je pourrais tenir responsable le fournisseur de l'ICANN/RDS pour le manque de transparence et devenir moins responsable.

Enquête sur les risques liés au RDS - Résumé des résultats

Risques opérationnels du RDS

- Possibles **effets opérationnels négatifs** le plus souvent invoqués (87 réponses) :
    1. mon accès aux données d'enregistrement pourrait être entravé par des défaillances du RDS (68).
    2. mon accès aux données sécurisées pourrait être retardé suite à des retards dans l'accréditation (66).
    3. mon accès aux données d'enregistrement pourrait être ralenti par des goulots d'étranglement du RDS (65).
    4. les données d'enregistrement fournies par le RDS pourraient ne pas être synchronisées avec les mises à jour les plus récentes (56).
- Risques identifiés comme les plus importants / les plus probables : les numéros 2 et 3 cités précédemment
- Au-delà des risques expressément énumérés, des risques opérationnels supplémentaires ont été identifiés :
    - les réponses aux requêtes de relais de communication et de révélation d'identité des services d'enregistrement fiduciaire et d'anonymisation pourraient être plus longues (49).
    - notre entreprise serait à risque en vertu des décisions de politique du RDS.
    - l'accès contrôlé du public ne permet pas aux consommateurs d'avoir suffisamment de transparence pour savoir à qui on paie les services ou quand est-ce qu'on saisit des renseignements personnels
    - violation des données
    - peut avoir augmenté la difficulté/retard pour s'occuper des sujets liés au spam/attaques/questions liés au réseau provenant de sources extérieures.
    - Les données fermées pour le niveau d'accréditation peuvent ne pas satisfaire une exigence réelle.
    - les règles arbitraires empêcheront les besoins d'accès valide.
    - JE veux que TOUTES les parties puissent accéder à MES donnés à l'aide de la technologie actuelle établie.
    - les sites pirates qui opèrent par l'intermédiaire de programmes d'affiliation de réseau seront plus facilement à l'abri de l'application de la loi, des fournisseurs de services, et des consommateurs qui ont été dupés.
    - il sera nécessaire de mettre en œuvre et de maintenir les nouveaux processus et systèmes quand le statu quo n'est pas rompu.
    - perte du délai supplémentaire, des revenus et de l'occasion au contact initial augmenté par le conseiller d'IP non expérimenté qui abuse ou tire indûment du profit du nouveau système.

Bénéfices opérationnels du RDS

- Possibles **effets opérationnels positifs** le plus souvent invoqués (61 réponses) :
    1. les réponses des services d'enregistrement fiduciaire accrédités aux requêtes de relais de communication et de révélation d'identité pourraient être plus courtes (49).

-- Publié le 28 juillet 2014 --

2. je pourrais avoir un accès haut débit plus fiable aux données d'enregistrement (40).
3. l'accès authentifié en temps réel aux données sécurisées pourrait être plus rapide qu'aujourd'hui (39).
4. le temps de réponse du RDS pourrait être plus uniforme et plus prévisible que celui du WHOIS (35).

- Bénéfices identifiés comme les plus importants / les plus probables : les numéros 2 et 4 cités précédemment.
- Outre les bénéfices répertoriés explicitement, des bénéfices opérationnels supplémentaires ont été identifiés :
  - les RDS agrégés peuvent mieux soutenir les fonctionnalités telles que WhoWas et le Whois inversé (7)

Risques du RDS en matière de sécurité ou de confidentialité

- Possibles **effets négatifs sur la sécurité et la confidentialité** le plus souvent invoqués (70 réponses) :
  1. mes données d'enregistrement risquent d'être plus vulnérables à des attaques extérieures (40).
  2. mes données d'enregistrement risquent de faire l'objet d'une utilisation impropre par l'opérateur du RDS (40).
  3. je pourrais devoir fournir une identité vérifiable pour enregistrer un nom de domaine gTLD (24).
- Risques identifiés comme les plus importants / les plus probables : les numéros 1 et 2 cités précédemment
- Au-delà des risques expressément énumérés, des risques supplémentaires à la sécurité et à la confidentialité ont été identifiés :
  - les « utilisateurs individuels d'Internet » sont souvent des titulaires de droits et devraient avoir la possibilité d'accéder à un enregistrement correspondant pour enquêter sur les infractions en ligne (5)
  - je suis préoccupé du fait que les utilisateurs individuels qui devraient avoir accès puissent être exclus
  - fournir un numéro de téléphone ou une adresse email valides est essentiel pour que les titulaires de droits puissent enquêter sur l'utilisation abusive
  - mes requêtes de données d'enregistrement risquent de faire l'objet d'une utilisation impropre par l'opérateur du RDS.
  - je pourrais devoir choisir entre l'un ou l'autre des droits de compromis que j'ai comme personne morale et personne physique lors de l'enregistrement de mon nom de domaine alors que je peux clairement prendre en charge les deux. En conséquence, on pourrait me demander de renoncer à ces droits au titre d'une catégorie de droits, bien que j'aie légalement droit aux bénéfices des deux.
  - mes données personnelles risquent de devenir plus disponibles comme administrateur de noms de domaine

- perte d'enregistrements à cause des exigences supplémentaires ; les sociétés en formation peuvent ne pas avoir des identités commerciales, etc. mais ont encore besoin d'un domaine.
- les attaquants externes auront désormais une grande cible rouge clignotante.
- mon identité personnelle peut être associé par la force à un domaine détenu et contrôlé par une personne morale, pas par moi personnellement
- les organisations et les personnes malveillantes tireront profit de la capacité de cacher leurs informations dans les données sécurisées, ce qui rendra plus difficile au personnel de sécurité et de conformité d'enquêter à ce sujet avec succès.
- je ne peux pas enregistrer un domaine de manière anonyme
- révéler mes motifs pour accéder aux données. Ils sont légitimes, mais ce sont mes affaires, pas celles de l'ICANN.
- les données d'enregistrement devraient être moins accessibles par sécurité, marque et d'autres acteurs d'application de la loi du secteur privé.
- mes données d'enregistrement seront plus vulnérables à des tierces parties, y compris ceux qui s'occupent des fonctions de sécurité pour des entreprises privées et qui voudront plus d'accès aux informations personnelles et sensibles à travers plusieurs TLD génériques.
- possibilité d'être nommé dans un procès en raison de la disponibilité de mon nom avec la compagnie
- offrir un accès à plusieurs niveaux d'application de la Loi est un moyen de leur accorder un accès supplémentaire, et c'est un moyen de contourner les ordonnances du Tribunal et les citations à comparaître. Ce n'est pas le genre d'occasion, ou de processus dans lequel l'ICANN devrait s'impliquer.
- les décisions de politique concernant les données d'enregistrement pourraient être prises par une seule entité.
- l'accès des tiers pourrait enfreindre la législation locale, la conservation des données ou la vie privée et présenterait un risque pour le client à mon insu.
- l'accès des tiers ou le compromis des données stockées pourrait créer un gros outil pour l'utilisation abusive de mes données ou de celles de mon client.
- le nouveau système pourrait devenir un nouveau vecteur d'attaque.

Bénéfices du RDS en matière de sécurité ou de confidentialité

- Possibles **effets positifs sur la sécurité et la confidentialité** le plus souvent invoqués (55 réponses) :
  1. mes données d'enregistrement pourraient être mieux protégées contre des utilisations impropres (37).
  2. mes données d'enregistrement pourraient être sécurisées de manière plus uniforme (31).
  3. je pourrais publier un identifiant de contact (Contact ID) réutilisable à la place de mon nom (29).

4. une plus petite partie de mes données d'enregistrement pourrait être disponible de manière anonyme et publique (27).

- Bénéfices identifiés comme les plus importants / les plus probables : les numéros 2 et 3 cités précédemment.
- Au-delà des bénéfices expressément énumérés, des bénéfices supplémentaires à la sécurité et à la confidentialité ont été identifiés :
  - les règles de validation, d'authentification et d'autorisation seront appliquées de manière cohérente et peuvent être facilement vérifiées (7) ;
  - je serais plus disposé à mettre à jour mon information de contact pour qu'elle soit exacte, puisqu'elle serait inaccessible pour les harceleurs ;
  - il faudrait exiger une certification légale au lieu d'une certification physique
  - faciliter l'accès ouvert aux entités légales.

Opinions supplémentaires

Les personnes interrogées ont présenté trente commentaires sur les **risques inévitables**, sur la base des risques préalablement déclarés :

1. il y aura une diminution de l'accès aux données d'enregistrement disponibles.
2. les risques 5a, 5b et 9b (modifications apportées aux pratiques, réduction de l'accès public en libre disponibilité) sont inhérents au RDS.
3. toute entité contrôlant un point d'accès central unique pour récupérer des données d'enregistrement retiendra toujours trop de pouvoir sur un bien public.
4. la question de l'accès illimité aux données, même par ceux qui ont des identificateurs et des mots de passe, est une question que la communauté doit pouvoir mieux comprendre. le fait que le RDS ne vérifie probablement pas les recherches trop indiscrètes faites par des acteurs étatiques et par des tierces parties est un risque majeur.
5. si l'architecture s'avère défaillante, nous ne pourrons pas accéder rapidement à l'information. Ou si l'accréditation nécessaire pour accéder aux données prend trop longtemps.
6. capacité à obtenir des informations de manière efficace et opportune (pour aider les clients qui poursuivent des investigations sur un site web pirate).
7. capacité à protéger les consommateurs des achats et / ou de la saisie de données personnelles sur des sites pirates (en raison du manque de transparence sur la propriété du site).
8. le stockage et l'approvisionnement centralisés du Whois pour tous les enregistrements dans n'importe quelle sorte de base de données (plutôt que chez les bureaux d'enregistrement et les registres) accroît le risque de violation des données.
9. un système comme celui-ci sera un aimant pour ceux qui souhaitent pirater des bases de données, ce qui pourrait entraîner la répétition du ralentissement du service et des interruptions.
10. je crois que l'on pourrait trouver quelqu'un fournissant des informations correctes au moment de l'enregistrement mais comment seront-elles tenues à jour ?
11. la conformité avec les dispositions de l'ICANN n'est pas la seule raison pour fournir l'accès au WHOIS. Dans la pratique, le registre devra toujours fournir l'accès WHOIS des ports 43 et 80, ce qui accroît et le coût et le risque.
12. le RDS brise un principe fondamental de l'Internet : la décentralisation du pouvoir et du contrôle. Et cela du fait d'introduire un ensemble de questions inter-juridictionnelles de manière déficiente du point de vue technique.
13. il ignore ces problèmes : 1) comment faire pour trouver un serveur Whois pour une zone ; 2) les domaines « privés » qui sont ouverts pour l'enregistrement « public » ; 3) la base installée, les outils et les pratiques existants.

14. le nouveau mécanisme impose l'existence de beaucoup de données cachées. Cela conduira à une augmentation du risque pour le public quant aux domaines [problématiques] car ceux-ci ne feront pas l'objet de mesures. Il y aurait aussi une perte de preuves pour l'application de la loi.
15. le système actuel exige un volume important de données. Ces données vulnérables sont faciles à saisir lors de leur soumission ou de leur stockage par ceux ayant une réputation éthique douteuse ainsi que par ceux ayant l'intention de commettre des actions illégales.
16. puisque des êtres humains sont concernés, l'échec fait partie du système.
17. la centralisation du contrôle sur qui peut accéder aux données d'enregistrement des noms de domaine, ainsi que l'exigence d'une validation de la personne ou de l'entité accédant aux données d'enregistrement des noms de domaine, implique un risque de monopole inévitable, réduit la possibilité d'application de la loi et la capacité d'identifier des comportements abusifs sur Internet des responsables des enquêtes sur la sécurité. Ces risques semblent inévitables [dans les deux modèles].
18. un ralentissement général du processus d'enregistrement de domaines sera inévitable si les données d'enregistrement doivent dorénavant être validées.
19. le RDS propose d'étendre l'accès sécurisé aux organismes d'application de la loi de tous les pays ou de la plupart d'entre eux. Par conséquent, son but est tout simplement d'exposer les titulaires de noms de domaine individuels aux enquêtes des organismes étrangers, auxquels ils n'ont aucune obligation d'obéir ni de raison légitime de se soumettre. Le RDS est donc intrinsèquement défectueux.
20. tout mécanisme d'enregistrement anonyme fera l'objet d'abus. Forcer les « méchants » à s'enregistrer sous un DBA et avec une boîte postale représente, au moins, une petite barrière pour accéder à l'enregistrement de noms de domaines à des fins illégales.
21. l'ouverture de l'accès et le blocage de la réplication en masse s'opposent aux intérêts de gain abusif sur l'enregistrement de noms de domaine, alors il est inévitable que tout nouveau RDS établi par l'ICANN « trouve une solution » à ces « problèmes » avec le Whois actuel.
22. il est clair que les auteurs du rapport sont fortement centrés sur la protection de la confidentialité d'un nombre relativement petit de titulaires de noms de domaine avec des besoins spéciaux quant à la confidentialité. Néanmoins, les cas légitimes de ce type sont extrêmement peu nombreux... Les modifications proposées feront obstacle au travail des « faiseurs de bien » et il en résultera un écosystème de domaines plus propice aux abus, qui sera probablement rempli de données inexactes et inutiles.
23. les données à grande échelle représentent évidemment un grand risque qui ne peut pas être totalement évité.
24. toute centralisation des données présente le risque inévitable d'un point unique d'échec : les pirates informatiques, les cybercriminels et les entités malintentionnées telles que les gouvernements voyous ou les gouvernements qui commettent des abus contre les droits civils et les droits de l'homme n'auront besoin que d'aller voir à un seul lieu pour obtenir des informations privées.
25. toute restriction de l'accès public à l'information sur l'identité du propriétaire d'un domaine rend plus difficile la lutte contre le courrier indésirable ou contre les programmes malveillants.
26. compte tenu du terrible bilan de l'ICANN quant aux opérations et à la conformité il résulte complètement invraisemblable que cela puisse fonctionner.
27. mes données d'enregistrement seront situées dans un autre pays dont la juridiction ne me fait pas confiance.
28. il semblerait que le nouveau système du RDS améliorera sensiblement la confidentialité des données d'enregistrement et favorisera la liberté d'expression ce qui constitue, à mon avis, la base et le charme de l'Internet. Mon seul souci en termes de risques inévitables concerne les opérateurs et les employés ainsi que les personnes et les organisations qui auront ou pourraient avoir un accès illimité et / ou non réglementé à toutes les données d'enregistrement.
29. le service centralisé est risqué et inutile et il met l'ICANN dans des situations légales épineuses qui peuvent être évitées. Cherchons d'autres solutions possibles.
30. quels que soient le type ou la structure de théâtre kabuki pouvant accompagner le lieu où le RDS sera créé ou ce qu'il pourrait au minimum offrir uniquement aux organismes d'application de la loi (LEA) et aux marques commerciales (TM) pour servir leurs intérêts, ce RDS sera perçu comme une source de données dont les gouvernements abuseront.

Enquête sur les risques liés au RDS - Résumé des résultats

Treize personnes interrogées ont donné des réponses détaillées et leurs arguments sur les **risques acceptables** :

1. le risque est acceptable si l'on tient compte des solutions techniques existantes à l'heure actuelle (l'informatique à haute performance, la distribution basée sur le nuage et la technologie de basculement pour augmenter la disponibilité, etc. (5)).
2. tant que cela sera développé avec les techniques généralement acceptées pour garantir la disponibilité et la sécurité, les préoccupations devraient être atténuées.
3. les sites non-commerciaux (qui n'ont pas de fonctionnalité de commerce électronique ou des contraintes pour la saisie des données) présentent moins de risques pour les consommateurs et pour ceux qui s'efforcent de protéger les consommateurs (entreprises, organismes d'application de la loi, etc.). Il serait donc acceptable d'avoir moins de transparence sur ces sites-là.
4. la capacité de travailler avec une législation variable en matière de confidentialité est un risque acceptable qui pourrait avoir un effet sur l'activité des entreprises.
5. le risque d'une violation de la sécurité des données à accès sécurisé est acceptable, puisque le risque est toujours moins grand que celui de la base de données Whois publiquement accessible utilisée actuellement.
6. le risque lié aux données à grande échelle peut être rendu acceptable grâce à une conception soigneuse et à la supervision opérationnelle. Le manque d'accès à l'information requise par le niveau d'accès sécurisé peut être amélioré par une analyse minutieuse des besoins des parties prenantes.
7. l'ICANN recevrait des « redevances »plus réduites suite à la mise en œuvre du RDS. Le RDS proposé réduira le volume d'enregistrements actuel du marché à cause de sa méthode contraignante qui oblige le client à fournir une énorme quantité de données avant de pouvoir procéder à un achat initial

Les personnes interrogées ont suggéré vingt-quatre manières de **réduire ou de modifier les risques** :

1. prendre des mesures pour améliorer l'exactitude
2. les risques de goulots d'étranglement du RDS devraient être gérables par une supervision rigoureuse de l'opérateur du RDS.
3. les capacités du Whois / WhoWas inversé pourraient être intégrées au RDS
4. la réduction des données librement accessibles pourrait être améliorée grâce à une analyse rigoureuse des éléments de données actuellement publics et supprimer seulement l'accès public à ceux pour qui le besoin de cette suppression puisse être objectivement établi.
5. la conception d'un processus d'accréditation simple permettant d'obtenir une information d'identification permanente.
6. il est nécessaire de justifier l'identification de l'utilisation d'un nom. La réponse devrait être donnée seulement sur la base des plaintes reçues. Si la demande est valable, une réponse peut être donnée.
7. le titulaire du nom de domaine reçoit-il un avis du fait que l'information a été demandée et, si c'est le cas, peut-il identifier la partie requérante ?
8. les principaux risques du RDS peuvent être évités rien qu'en mettant en œuvre les aspects de validation dans le paradigme actuel. Si l'on souhaite la mise en conformité de toutes les données d'enregistrement conformément à un format spécifique, cela peut se faire au moyen de la politique de l'ICANN plutôt qu'avec un nouveau RDS.
9. peut-être un moyen de délimiter les sites commerciaux et les sites non-commerciaux pourrait fournir davantage de transparence vis-à-vis des sites commerciaux et réduirait les risques.
10. certains risques pourraient au moins être réduits en utilisant une approche fédérée où chaque registre stockerait sa propre information.
11. repenser l'ensemble du schéma et collecter un minimum de données de contact. Appliquer des principes de proportionnalité, de confidentialité planifiée et de confidentialité par défaut.
12. exiger des délais raisonnables pour répondre aux contacts, après quoi les domaines peuvent être suspendus en attendant la réponse.
13. stocker moins de données.

-- Publié le 28 juillet 2014 --

14. l'accès au Whois peut et doit rester anonyme et ouvert à tous les utilisateurs d'Internet.
15. les délais de traitement de la validation des enregistrements doivent être réduits autant que possible afin que les administrateurs de domaine puissent exploiter leurs domaines de manière efficace, avec un temps d'attente minimal lié aux procédures de validation.
16. l'idéal serait de permettre au consommateur de choisir le fournisseur de validation : les fournisseurs seraient ainsi encouragés à réduire et maintenir leurs coûts et leurs délais de traitement afin d'être compétitifs.
17. centraliser la validation au moyen d'un petit groupe ou forcer la validation par l'intermédiaire d'un fournisseur spécifique sont des actions qui réduiront la motivation pour que le processus reste rapide et rentable.
18. permettre à tous d'enregistrer des noms de domaine (non seulement à ceux qui sont censés avoir besoin de la protection d'une organisation) de manière totalement anonyme, sans fournir aucune donnée d'enregistrement. S'il n'y a presque pas de données d'enregistrement, il n'y aura donc aucun problème concernant l'accès public à ces données.
19. éliminer l'anonymat de l'enregistrement.
20. certains risques peuvent être facilement modérés au moyen d'une approche par étapes dans la mise en œuvre du RDS, par exemple, en rendant facultative toute demande d'information supplémentaire pendant un certain temps alors que l'on rend disponibles les données de l'infrastructure du WHOIS existante. Cela signifie que le système RDS pourra être développé et que tous les bogues / toutes les problématiques pourront être facilement résolus sans avoir d'impact sur système existant et, qu'une fois établi et qu'il y aura eu le temps suffisant pour résoudre les problèmes d'intégration, les bureaux d'enregistrement / registres pourront faire la transition. Je suggérerais une période appropriée pour que les données supplémentaires soient facultatives et environ 3 ans pour le chevauchement des services : cela permettrait d'avoir le temps suffisant pour changer les systèmes et éduquer les clients de manière adéquate.
21. éliminer tous les « enregistrements fiduciaires », appliquer l'exactitude des données d'enregistrement, demander aux registres de restreindre l'accès en masse, rendre obligatoire l'accès ouvert à toutes les données d'enregistrement du Whois mais limité par le nombre de requêtes, et interdire aux registres et aux bureaux d'enregistrement la vente des données d'enregistrement en masse.
22. éliminer les mesures incitatives financières destinées aux bureaux d'enregistrement ou autres pour la vente de services d'enregistrement privés. À l'heure actuelle, c'est la vache à lait, autant que l'étaient les numéros de téléphone non publiés pour les compagnies téléphoniques. Garantir que les bureaux d'enregistrement n'ont aucune « intention cachée » lorsqu'ils offrent des services d'enregistrement privés ou de type fiduciaire. Assurer que les titulaires de noms de domaines qui ont un besoin légitime d'enregistrements privés ou de type fiduciaire paient des frais suffisants pour démontrer qu'ils ont effectivement besoin de ce genre de service et que le montant payé soit versé à une association d'utilité publique (ce qui assurerait que l'ICANN n'a pas non plus de raison d'encourager les enregistrements privés ou fiduciaires).
23. la consultation des données demandées s'avère être meilleure que l'établissement d'un niveau d'accès sécurisé.
24. afin de réduire le risque d'abus dans l'accès aux données d'enregistrement privées, cet accès devrait être approuvé par des documents juridiques signés par un juge ou par une autre autorité judiciaire.
25. surmonter les perceptions de Snowden, Kafka et Orwell sur l'abus en masse par excès de zèle, faisant en sorte que tous les accès et les demandes au système soient transparents à 100 % pour le public.
26. vaincre la résistance aux changements en bloc, concevoir une méthode pour augmenter les bénéfices et pour réduire les inconvénients pour les titulaires de noms de domaine, pour les bureaux d'enregistrement et pour les registres, telle que l'utilisation d'un système de validation centralisé par les registres.

Treize personnes interrogées ont suggéré des voies permettant de transformer **les risques en des bons compromis pour obtenir des bénéfices** :

1. les bénéfices potentiels dépendent de la modalité de mise en œuvre (2).

2. tout risque associé à une réduction de l'accès aux données (actuellement libres et publiques) peut être diminué si la communauté assure une plus grande exactitude de toutes les données qui nécessitent un accès sécurisé. La réduction de l'accès sans une augmentation de l'exactitude serait un défaut majeur dans tout nouveau système proposé (2).
3. bien qu'une base de données regroupée puisse accroître les risques liés à la sécurité, cela peut être amélioré au moyen d'une conception et une surveillance appropriées, ainsi que par un service disponible partout montrant des résultats sous un format cohérent qui pourrait justifier de tels risques.
4. un accès à plusieurs niveaux en échange de l'amélioration des données (par ex., plus complètes et plus exactes) pourrait être un compromis possible.
5. le RDS proposé présente un certain nombre de bénéfices qui dépassent les risques. Un accès facile aux données exactes des titulaires de noms de domaine est critique pour la protection des droits de propriété intellectuelle en ligne. Un système de RDS qui améliore l'accès et l'exactitude de ces données serait extrêmement avantageux pour les titulaires des droits de propriété intellectuelle et pour leurs conseillers dans la lutte contre la contrefaçon de la propriété intellectuelle et d'autres abus commis par les titulaires de noms de domaine et d'autres utilisateurs d'Internet.
6. si les coûts et les délais de validation peuvent être contrôlés et maintenus à un niveau minimal, les bénéfices du système proposé pourraient être un échange équitable pour les bénéfices proposés du système. Si les coûts ne sont pas contrôlés, ils dépasseront les bénéfices.
7. l'amélioration de la qualité des données dans la base de données du Whois est très importante et elle vaut vraiment la peine. Relier les titulaires de noms de domaine de manière cohérente à leur portefeuille de noms de domaine complet est aussi très important et intéressant, puisque cela assurerait que lorsqu'une inexactitude dans les données de point de contact pour un domaine serait identifiée et corrigée, elle serait corrigée partout.
8. l'accès programmatique amélioré (sans limitations arbitraires ou mal conçues) serait aussi extrêmement utile.
9. un accès uniforme, fiable et utilisable des données correctes est un atout clair, puisque les risques peuvent être minimisés grâce à une conception et à une consultation soigneuses.

Vingt-cinq personnes interrogées ont proposé les **commentaires supplémentaires** ci-dessous à la fin de l'enquête.

1. la proposition manque de caractéristiques concrètes pour améliorer l'exactitude des données dans la pratique (la capacité de contact des titulaires de noms de domaine) de manière significative par rapport au niveau de base du contrat d'accréditation des bureaux d'enregistrement 2013 (RAA 2013) et, pour les engagements d'intérêt public (PIC) des nouveaux gTLD. Il faut l'expliquer dans le détail. De manière similaire, une base de données plus riche fournissant des services améliorés tels que des données historiques pourrait aider à justifier la restriction de l'accès public à cette ressource.
2. un bénéfice consiste à nous permettre d'identifier des titulaires de noms de domaine qui essaient de cacher leur identité pour pouvoir continuer à exercer des activités malveillantes et à distribuer des logiciels malveillants.
3. la capacité des utilisateurs et des outils des tierces parties pour se servir du système du Whois actuel afin d'accéder et de sauvegarder l'information du Whois à des propos historiques est critique. Tout système de RDS proposé doit assurer cette fonctionnalité. Cela peut se faire directement au moyen du RDS lui-même ou indirectement en continuant à habiliter les outils / clients des tierces parties à le faire.
4. donner un contrôle monopolistique de ce bien public à une seule entité se traduit par une perte pour le monde avec un petit bénéfice qui ne pourrait pas être atteint par d'autres moyens moins centralisés.
5. pourquoi y a-t-il autant de nouveaux gTLD ? Cette décision est un désastre pour les propriétaires de marques parce qu'elle conduit à une augmentation des coûts de protection de la propriété intellectuelle. Dès à présent, nous sommes confrontés à de très nombreux enregistrements de mauvaise foi, bien que les périodes d'enregistrement prioritaire pour beaucoup de nouveaux gTLD n'aient même pas encore commencé. Si vous êtes une petite entreprise, vous pourriez ne pas disposer du budget nécessaire pour

vos enregistrements afin d'éviter des enregistrements de mauvaise foi. D'autre part, les coûts de recours en justice sont élevés.

6. le fait d'avoir un Whois vérifié est d'une importance capitale en raison de l'anonymat de l'Internet. Nous cherchons des fraudeurs et les données inexactes ne sont plus acceptables.
7. je soutiens pleinement les efforts visant à rendre plus exactes les données du WHOIS. Ce serait un changement positif SI une base de données centralisée et fermée ne rendait pas plus difficile l'obtention de l'information, qu'elle ne ralentissait pas le processus d'obtention d'information, qu'elle n'imposait pas un plafond à la quantité d'information pouvant être obtenue, qu'elle ne créait de longs processus pour que les compagnies puissent obtenir leur accréditation pour accéder à l'information ou que cela ne créait pas de problèmes de transparence pour les utilisateurs du web. Une bonne partie de mes soucis se rapporte au fait que la communauté de la cyber sécurité soit effectivement capable de protéger les consommateurs des sites web pirates qui peuvent tirer profit d'une base de données fermée.
8. la proposition d'un accès public vs. un accès sécurisé pour certains éléments des données est bonne. Ce serait utile d'avoir davantage de détails sur les raisons de divulgation acceptables, sur l'évaluation de ces candidats, et sur la manière dont les utilisateurs de cet accès sécurisé sont tenus pour responsables, etc., afin de pouvoir faire des commentaires là-dessus.
9. d'une manière générale, tout mouvement pour centraliser des données augmente fortement les risques de piratage évident et secret, de furetage des gouvernements invisible et injustifiable, de modes de défaillance à grande échelle et d'interférences politiques. Bien que certains des objectifs du RDS soient utiles, ils ne dépassent pas les risques tout à fait prévisibles. Les risques les plus grands du RDS sont la possibilité d'être obligés de payer pour pouvoir accéder à l'information publique du WHOIS et/ou la perte de l'accès public à l'information essentielle de gestion du réseau, y compris l'attribution des blocs d'adresses IP, l'emplacement physique et l'utilisation frauduleuse des messageries. Toute proposition qui ne protège pas l'accès public libre et la disponibilité continue de ces informations devrait être éliminée aussi rapidement et définitivement que possible.
10. je ne suis pas encore sûr de la manière dont nous pouvons garantir « l'exactitude » des données d'enregistrement, parce que les données du premier jour (sur l'enregistrement) sont une chose et la « vérification périodique » est une autre, ce qui est le plus important à mon avis. Je crois que nous pouvons avoir à externaliser cela à « l'organisme » dans chaque site (pays ou ville peut-être) pour qu'il s'occupe de la vérification, mais cela peut susciter à nouveau des remises en question sur l'exactitude et la norme.
11. il existe deux groupes d'individus auxquels le registre moyen voudrait empêcher d'accéder en masse aux données du Whois, à savoir les spammeurs et les organismes d'application de la loi. Fournir des informations en masse à l'un quelconque de ces deux groupes pourrait endommager irrémédiablement la réputation du registre. Un système RDS centralisé oblige le registre à mettre sa réputation entre les mains d'une tierce partie.
12. il faut accepter que toutes les parties n'aient pas le même protectionnisme en vertu de la législation locale et que les demandes transfrontalières de données peuvent ne pas aboutir à cause de questions politiques externes. Le RDS provoquerait la perte d'une ressource vitale dans la lutte contre la cybercriminalité organisée.
13. comme titulaire individuel d'un nom de domaine, j'utilise actuellement une fonction de anonymisation / enregistrement fiduciaire disponible dans mon bureau d'enregistrement pour protéger mon identité individuelle d'un accès fortuit et inutile du public en général, ce que je trouve utile comme une précaution contre le harcèlement personnel anonyme. Je voudrais que ces fonctions de confidentialité soient obligatoirement disponibles de manière régulière dans tous les bureaux d'enregistrement, pour assurer un marché d'enregistrement tout à fait compétitif avec tous les bureaux d'enregistrement et pas tout juste avec un sous-ensemble volontaire de bureaux d'enregistrement.
14. le risque qui m'inquiète le plus est celui du coût de la validation de mes données d'enregistrement et l'authentification dont j'aurai besoin pour accéder à des données sécurisées. Je me soucie aussi des délais de traitement et du ralentissement général que ces procédures pourraient susciter.
15. le RDS est une excellente idée. Il aiderait à résoudre beaucoup de problèmes s'il est mis en œuvre de manière appropriée. Je suis impatient de recevoir des commentaires. Toutefois, cette enquête en particulier n'est pas bien conçue.

16. franchement, ce système semble être aussi inconsidéré que les services de « confidentialité du WHOIS » actuellement disponibles. Leur utilisation revient tout simplement à porter atteinte à la transparence d'une organisation et, en conséquence, à sa réputation en ligne. Merci de m'avoir écouté.
17. je n'y vois pas de bénéfice mais beaucoup de risques d'utilisation frauduleuse ou de vol des données. Idéalement, il faudrait éliminer l'obligation de fournir des données d'enregistrement au bureau d'enregistrement : s'il n'y a pas de données d'enregistrement, il n'y a donc pas de risque d'abus ou de vol.
18. ce qui m'inquiète, c'est de pouvoir faire face à plusieurs sortes d'attaques en réseau / courriers indésirables / intrusions / attaques par inondation de données, etc. Il est ABSOLUMENT essentiel qu'il existe un contact valide capable de résoudre effectivement les problèmes du réseau qui lui sont présentés. Cela signifie que le contact doit avoir en même temps l'autorité et la capacité technique pour assurer que son domaine n'est pas la source de l'abus. Le système actuel, particulièrement les domaines se cachant derrières les enregistrements fiduciaires, N'assurent PAS que le bureau d'enregistrement / l'enregistrement fiduciaire aborderont (ou pourront résoudre) les problèmes en temps opportun. Si les enregistrements fiduciaires vont être autorisés, alors il faut que ce soit ABSOLUMENT clair que quiconque figure dans des listes publiquement accessibles aux recherches / requêtes est responsable du comportement du registre qu'ils sont en train de protéger, y compris la capacité totale de fermer le domaine en cas d'utilisation abusive des réseaux.
19. le risque le plus important concerne la manière dont sera géré l'accès à l'information « sécurisée », en ce sens que cela suppose des frais ou que les processus d'accréditation pour y accéder soient trop compliqués. Si c'est coûteux ou compliqué, cela entravera sérieusement des opérations essentielles, le contact avec les propriétaires de domaines, la recherche et d'autres nombreux champs de gestion des domaines et de recherche.
20. je pense que le processus proposé est une solution à la recherche d'un problème et qu'il est alimenté par des arguments fallacieux de personnes ayant des visions politiques dogmatiques.
21. je ne crois pas que les exigences en matière de confidentialité des personnes physiques comparées aux personnes morales et aux entreprises commerciales / corporations aient fait l'objet d'un examen attentif. Les individus ou les personnes physiques étant titulaires de noms de domaines doivent pouvoir être contactés d'une manière ou d'une autre pour permettre de résoudre des problèmes affectant des tiers ; cependant, il faut leur permettre toujours d'avoir le droit à l'anonymat, sauf en cas de requête légale. En revanche, les personnes morales n'ayant que des restrictions limitées (telles que les centres d'accueil pour femmes ou certaines organisations politiques à risque) NE DOIVENT PAS être anonymes. Il est absolument inapproprié que les entreprises commerciales en particulier agissent de manière anonyme ; les données DOIVENT être accessibles de façon publique et anonyme. Deuxièmement, il doit y avoir un processus permettant de dépouiller des entités de leur anonymat s'il a été démontré qu'elles ne remplissent pas les conditions requises pour cet anonymat.
22. nous supportons trop souvent les spammeurs et les réseaux zombies qui se servent de données fausses pour cacher la propriété des domaines. L'information du Whois peut et doit être claire et bien définie. Ce n'est pas une difficulté majeure d'obtenir des services d'hébergement d'autres entités, mais savoir clairement qui est responsable des serveurs du DNS pour un domaine donné est utile du point de vue opérationnel.
23. à mon avis, la confidentialité est beaucoup plus importante que l'accès public aux données d'enregistrement.
24. s'il n'y a pas de bénéfices, veuillez arrêter de faire ce que vous faites. Si cela fonctionne, laissez-le tel qu'il est. N'oubliez pas qu'il y a un certain nombre de titulaires de noms de domaine qui SOUHAITENT VRAIMENT que leurs données Whois soient accessibles comme elles le sont à l'heure actuelle ; ceux qui ne le souhaitent veulent pas sont libres d'utiliser la POB ou la protection de confidentialité offerte par le bureau d'enregistrement.
25. le RDS c'est beaucoup trop à la fois, c'est une mauvaise idée. Cela représente un fardeau pour ceux qui en bénéficient le moins, sans avoir un coût réel pour ceux qui en bénéficient le plus.

Enquête sur les risques liés au RDS - Résumé des résultats

Enfin, environ 5 des 182 personnes interrogées ont bourré la plupart ou tous les champs de texte au format libre avec des réponses qui ne répondaient pas directement aux questions ; ils ont plutôt fait une déclaration disant que le RDS était une mauvaise idée ou qu'il n'avait pas de bénéfices.

-- Publié le 28 juillet 2014 --