Rapport sur PRISM -Documents déclassifiés de la NSA - Avril 2014

Soumis le 11 août, 2014 - 08:58

Traduction de documents déclasifiés de la N.S.A. - Rapport sur PRISM - Source: NSA Unclassified Report on Prism [1] ; NSA Unclassified Section 702 FISA & Section 215 USAPA [2]

Rapport du Directeur de la NSA du bureau des affaires privées et des libertés civiles

Implantation de l'acte de surveillance des services secrets étrangers - Section 702 - Le 16 Avril 2014

INTRODUCTION

Ce rapport a été rédigé par le bureau des affaires privées et des libertés civiles de la National Security Agency (NSA), dans le but de mettre en évidence les communications entre le public et les fournisseurs de communications. Créé en Janvier 2014, le bureau est également chargé de garantir que la protection des libertés civiles et des données privées a été intégrée dans les activités de la NSA. L'objet de ce rapport est d'aider à l'établissement d'une compréhension commune qui puisse servir de base aux futures discussions sur les libertés civiles existantes et la protection des données privées.

La mission de la NSA est de rendre plus sûre la nation en fournissant des règles politiques et militaires sur les rapports étrangers et en protégeant le réseau d'informations sur la sécurité nationale. La NSA collecte des données étrangères selon la demande du Président, son équipe de sécurité nationale, et leur personnel, à travers les priorités du réseau de services secrets (National Intelligence Priorities Framework - NIPF). La NSA recherche ces renseignements sur les services secrets étrangers à l'aide de la collecte, l'exécution et l'analyse des communications ou des autres données, accessibles par radio, câble et autres moyens électroniques.

L'autorité de la NSA à diriger les collections de signaux des services secrets étrangers et les mesures de contre-espionnage est indiquée dans la Section 1.7(c)(1) de l'ordre exécutif 12333, qui a été amendé.

L'exécution de la mission d'espionnage de la NSA doit être effectuée en conformité avec le quatrième amendement. L'acte de surveillance des services secrets étrangers (Foreign Intelligence Surveillance Act - FISA) de 1978 régularise certains actes des services secrets étrangers, comprenant ceux qui surviennent avec l'aide des fournisseurs de communications US.

Ce rapport décrit la voie par laquelle la NSA assume ses responsabilités durant l'application de la Section 702 du FISA, et par l'amendement du FISA de 2008. Aussi, de nombreuses agences fédérales participent à l'application de la Section 702, ce rapport décrit le processus par lequel la NSA obtient, utilise, échange et conserve les communications des nations étrangères, dans le cadre de la Section 702. Il décrit également les moyens de protection existant pour les données privées et les libertés civiles, créés par ce processus.

Le Bureau des libertés civiles et des données privées (Civil Liberties and Privacy Office - CLPO) de la NSA utilise les principes pratiques d'information juste (Fair Information Practise Principles - FIPP) comme outil initial pour décrire l'existence de libertés civiles et la protection des données privées à la place d'un ensemble effectué sous l'autorité de la Section 702.

Section 702 du FISA

La Section 702 du FISA a été débattue publiquement au Congrès lors de son passage initial en 2008 et d'une manière beaucoup plus conséquente en 2012. Elle accorde à la NSA un statut de base, avec l'obligation de contrôler les communications électroniques des fournisseurs d'accès et de cibler des personnes non US, soupçonnées d'être domiciliées en dehors des USA ; après avoir acquis des informations des services secrets étrangers. La Section 702 ne permet de cibler que les personnes non US domiciliées en dehors des USA ; celà diffère beaucoup des autres sections du FISA. Il ne nécessite pas un avis individuel de la cour de surveillance des services secrets (Foreign Intelligence Surveillance Court - FISC) indiquant qu'il y a une raison probable à croire que la cible est une puissance étrangère ou un agent d'une puissance étrangère. A la place la FISC revoit tous les ans les certifications exécutées par l'avocat général (Attorney General - AG) et le directeur des services secrets nationaux (Director of National Intelligence - DNI) afin de déterminer si ces certifications sont statutairement justifiées. Le FISC détermine également si le nécessaire statutairement appliqué dans les procédures ciblant ou minimisant les connections, dans leur certification, sont conformes statutairement au quatrième amendement. Les procédures de ciblage sont déterminées pour assurer que cette section 702 est utilisée uniquement pour cibler des personnes non US, supposées localisées en dehors des US.

Les procédures de minimisation ont pour but de réduire l'impact sur les données des personnes US en réduisant l'acquisition, la rétention et la dissémination des données non publiques disponibles d'une personne US qui ont été légalement, mais accidentellement acquises dans le cadre de la Section 702, visant une personne non US soupçonnée d'être domiciliée en dehors des US. Sous ces certifications, le AG et le DNI donnent des directives pour les communications électroniques des fournisseurs d'accès, qui nécessitent que les fournisseurs d'accès "fournissent immédiatement au Gouvernement toutes les informations... ou toute l'assistance nécessaire pour accomplir l'acquisition [de données des services secrets étrangers] de telle manière à protéger le secret de cette acquisition..." L'acquisition des communications par le Gouvernement, sous l'autorité de la Section 702, doit être effectué conformément à un contrôle judiciaire et avec les connaissances des fournisseurs d'accès.

La NSA ne peut pas, intentionnellement, sous l'autorité de la Section 702, cibler n'importe quel citoyen US, n'importe quelle personne US, ou n'importe qui, au moment de l'acquisition, domicilié à l'intérieur des US. Les règles interdisent également l'usage de la Section 702 pour acquérir intentionnellement n'importe quelle communication par lesquelles l'envoyeur ainsi que tous les destinataires sont connus au moment de l'acquisition et localisés à l'intérieur des US. De même, les règles interdisent l'usage de la Section 702 conduisant à "inverser la cible" (c.a.d la NSA ne doit pas intentionnellement cibler une personne soupçonnée demeurer en dehors des US si le but d'une telle acquisition est de cibler une personne soupçonnée demeurer à l'intérieur des US). Toutes les acquisitions par la Section 702 doivent être menées de manière à respecter le quatrième amendement. Les procédures de ciblage approuvées par le FISC permettent à la NSA de cibler

une personne non US soupçonnée demeurer en dehors des US.

Existence de mesures de protection des données privées et des libertés civiles : Chacune des trois branches du gouvernement fédéral surveille l'utilisation des autorités de la Section 702 par la NSA. La NSA doit fournir la transparence à ses partenaires (Congrès, DOJ, ODNI, DOD, le Président des services secrets et le FISC) à travers des discours réguliers, des rapports succints et des rapports d'incidents. Au final, le DOJ et l'ODNI établissent des compte-rendus périodiques avec l'utilisation de l'autorité de la NSA et des rapports sur ces compte-rendus. Beaucoup plus récemment, à la direction de la Présidence, le Gouvernement a fourni une transparence supplémentaire au public à propos du programme en déclassifiant les avis du FISC et des documents en rapport. Aussi, la surveillance du FISA est tenue secrète pour les cibles de la surveillance, il y a des exceptions. Par exemple, si le Gouvernement tente d'utiliser les résultats de la surveillance du FISA, incluant la surveillance avec Section 702, en test et d'autres actions sur une personne dont les communications ont été collectées, le Gouvernement doit informer cette personne que les communications de cette personne ont été acquises légalement. Ces mesures de protection implémentent la transparence des principes pratiques d'information juste (Fair Information Practice Principle - FIPP).

COMMENT LA NSA APPLIQUE LA SECTION 702 DU FISA

ENTRAINEMENT

Avant qu'un analyste ait le droit d'accéder à toutes données des signaux des services secrets de la NSA, l'analyste doit, auparavant, avoir été formé aux lignes de conduite légales et politiques qui dirigent la manipulation et l'usage de ces données. Une formation supplémentaire est requise pour l'accès aux données de la Section 702. Cette formation annuelle nécessaire comprend un scénario d'entraînement, obligatoire, ainsi qu'un test de compétence final. L'analyste doit passer ce test avant que l'accès lui soit accordé. De plus, si il se produit un incident dû à une erreur ou un acte d'incompréhension, l'analyste doit être à nouveau formé avant de continuer d'avoir accès aux données acquises selon la Section 702.

IDENTIFICATION ET TACHES D'UN SELECTEUR

Le prochain processus dans la Section 702 est, pour un analyste de la NSA, d'identifier une personne non US, localisée en dehors des US, qui est à même de communiquer des informations, désignées dans la certification, aux services secrets étrangers. Par exemple, une telle personne pourrait être un individu appartenant à une organisation terroriste étrangère ou qui facilite les activités des membres de cette organisation. Les personnes non US ne sont pas ciblées à moins que la NSA ait une raison de croire qu'elles sont à même de communiquer des informations, précisées dans la codification, aux services secrets étrangers ; les personnes US ne sont jamais ciblées.

Une fois que l'analyste de la NSA a identifié une personne ayant des communications avec des services secrets étrangers, qui est la cible appropriée selon l'autorité du FISC, et selon les certifications de la Section 702, cette personne est considérée comme une cible. Les tentatives de l'analyste de la NSA vont déterminer comment, quand, avec qui et où la cible a communiqué. Alors, l'analyste identifie quels ont été les modes spécifiques de communication utilisés par la cible et obtient un identifiant unique associé à la cible, par exemple un numéro de téléphone ou une adresse mail. Cet identifiant unique est appelé sélecteur. Le sélecteur n'est pas un "mot-clé" ni un terme particulier (par exemple, "nucléaire" ou "bombe") ; mais doit être un identifiant de communication spécifique (par exemple une adresse mail).

Ensuite, l'analyste de la NSA doit vérifier qu'il y a une connexion entre la cible et le sélecteur ; et, que la cible est supposée être une personne non US et localisée en dehors des US. Il n'y a pas de test pour être un étranger à 51% ou 49%. De plus, l'analyste de la NSA devra tester de multiples sources et devra prendre une

décision basée sur la totalité des informations disponibles. Si l'analyste découvre n'importe quelle information indiquant que la personne est une cible localisée aux US ou que la cible peut être une personne US, une telle information doit être prise en compte. Dans d'autres mots, si il y a des informations conflictuelles sur la localisation de la personne ou son status en tant que personne non US, ce conflit doit être résolu avant que la personne soit ciblée avec succès.

Pour chaque sélecteur, l'analyste de la NSA doit renseigner les informations suivantes :
(1) les informations des services secrets étrangers, qui ont été acquises sous l'autorité de la certification,
(2) les informations sur une personne, permettant de conclure que le sélecteur est associé à une personne non US,
(3) les informations sur une personne, permettant de conclure que celle-ci est non US et localisée en dehors des US.

Cette documentation doit être relue et approuvée (ou réfutée) par 2 analystes senior de la NSA, qui ont satisfait les formations additionnelles nécessaires. Ces analystes senior devraient demander d'avantage de documentation ou de clarification ; mais, également, devraient vérifier que tout le nécessaire a été intégralement effectué. La NSA recherche toutes les soumissions, revues et processus d'approbation à travers les documentations et la détermination des analystes senior de la NSA a été retenue pour d'avantage d'éléments de points de vue de la NSA, autant que de points de vue externes du DOJ et de l'ODNI. Au delà de cette approbation, le sélecteur doit être utilisé comme base pour demander à un fournisseur d'accès de fournir les communications associées à un sélecteur donné. C'est généralement ce à quoi fait référence le terme de "TACHES D'UN SELECTEUR".

Existence de mesures de protection des données privées et des libertés civiles : La NSA forme ses analystes à travers diverses choses de manière à assurer que les analystes comprennent parfaitement leurs responsabilités et les moyens de sonder spécifiques de cette autorité. Si l'analyste échoue à connaître ces standards d'entraînement, l'analyste ne pourra pas avoir la possibilité d'utiliser les outils proposés sous l'autorité de la Section 702. Si l'analyste échoue à pratiquer les entraînements standards, l'analyste perd la possibilité d'utiliser les outils proposés sous l'autorité de la Section 702 et la possibilité de retrouver toute donnée précédemment acquise sous cette autorité. La NSA nécessite que tout analyste soit autorisé et entraîne dans la recherche et la surveillance du sélecteur, en utilisant le Section 702, afin de documenter les 3 informations nécessaires à l'usage de cette autorité ; à savoir que :
- la cible identifiée par le sélecteur soit en relation avec des services secrets étrangers ;
- la cible soit une personne non US ;
- la cible soit supposée être localisée en dehors des US.
Cette documentation doit être revue, validée et approuvée par un analyste senior qui a reçu l'entraînement additionnel. Ces mesures de protection comprennent les spécifications du FIPP, son audit et sa minimalisation.

ACCES AUX COMMUNICATIONS OBTENU SOUS L'AUTORITE DE LA SECTION 702

Une fois que l'analyste senior a approuvé le sélecteur comme étant conforme, les fournisseurs d'accès sont légalement tenus d'assister le gouvernement en lui fournissant le relevé des communications. Auparavant, le fait de surveiller sous cette autorité a été porté à la connaissance des fournisseurs d'accès. La NSA reçoit des informations sur un sélecteur surveillé par 2 méthodes différentes.

Pour la 1ère de ces méthodes, le gouvernement fourni aux fournisseurs d'accès une liste de sélecteurs par l'intermédiaire du FBI. Les fournisseurs d'accès sont tenus de fournir à la NSA les communications entrantes et sortantes de ces sélecteurs. Ceci fait, généralement, référence au programme PRISM.

Pour la 2ème de ces méthodes, les fournisseurs d'accès sont tenus d'assister la NSA dans l'interception légale des communications électroniques entrantes et sortantes de ces sélecteurs. Cette assistance par les fournisseurs d'accès fait généralement référence à la collecte en amont. Les procédures de ciblage de la NSA, approuvées par le FISC, comprennent le nécessaire additionnel tel que les outils permettant d'éviter

l'acquisition de la totalité des communications domestiques. Par exemple, dans certaines circonstances, les procédures de la NSA nécessitent l'utilisation du filtrage du protocole Internet (IP) afin de s'assurer que la cible est localisée en dehors des US. Le processus d'approbation de la surveillance d'un sélecteur est majoritairement le même entre PRISM et la collecte en amont.

Une fois que la NSA a reçu les communications d'un sélecteur surveillé, la NSA doit suivre les procédures additionnelles approuvées par le FISC et connues en tant que procédures de minimisation. Ces procédures nécessitent que l'analyste de la NSA revoit au minimum un échantillon des communications acquises, pour tous les sélecteurs, sous l'autorité de la Section 702, avec les bases nécessaires afin de déterminer de manière probante qu'elles sont valides.

L'analyste de la NSA doit vérifier un échantillon des communications reçues de sélecteurs pour s'assurer qu'elles sont, en réalité, associées à une cible des services secrets étrangers et que l'individu ou l'entité ciblée n'est pas une personne US et n'est pas localisée aux US. Si l'analyste de la NSA découvre que la NSA a reçu des communications qui ne sont pas associées à la cible visée ou que l'utilisateur du sélecteur est une personne US ou localisée aux US, le sélecteur doit être alors "non surveillé". En tant que règle générale, dans l'éventualité où la cible est une personne US ou dans les US, tous les autres sélecteurs associés à cette cible doivent aussi être "non surveillés".

Existence de mesures de protection des données privées et des libertés civiles : En rapport avec cet entraînement intensif, l'analyste est nécessaire pour revoir les collectes afin de déterminer qu'elles sont associées avec le sélecteur ciblé et ont été rapidement fournies aux services secrets étrangers après que la surveillance ait démarré et au minimum dans l'année. Cette revue permet à la NSA d'identifier les problèmes potentiels avec les collectes et fournissent des données chiffrées supplémentaires. Au final, la NSA dispose de mesures techniques pour alerter l'analyste de la NSA si il apparaît qu'un sélecteur a été utilisé depuis les US. Ces mesures de protection comprennent le FIPP général indiquant des spécifications, la minimisation, le chiffrage et l'analyse, la qualité des données et la sécurité.

COLLECTE ET ANALYSE, PAR LA NSA, DES COMMUNICATIONS OBTENUES SOUS L'AUTORITE DE LA SECTION 702

Les communications transmises à la NSA sous l'autorité de la Section 702 sont conservées dans dans les systèmes et les bases de données de la NSA. Une certaine source de données, par exemple, peut être contenue dans les communications telles que le texte des e-mails et les enregistrements de conversations ; alors qu'une autre source de données peut inclure les meta-data, cad les informations contenant les bases des communications, telles que l'heure et la durée d'un appel téléphonique, ou l'expéditeur et le destinataire des e-mail.

Les analystes de la NSA peuvent accéder aux communications obtenues sous l'autorité de la Section 702 dans le but d'identifier les services secrets étrangers. Ils peuvent accéder à l'information via des "requêtes", permettant de sélectionner la date, des chaînes de caractères alpha-numériques, ou la combinaison des 2. Les procédures de minimisation du FISC surveillent que les requêtes sont bien effectuées sous l'autorité de la Section 702 et tente de réduire les informations dérivées. Les analystes de la NSA ayant un accès aux informations dérivées de la Section 702 sont entraînés pour établir des requêtes correctes de telle manière que la requête permette de renvoyer des informations des services secrets étrangers valides et de réduire la probabilité d'obtenir des informations non pertinentes sur une personne US. L'accès des analystes de la NSA à chaque base de donnée est contrôlé, monitoré et surveillé. Il y a, par exemple, des tests automatisés qui déterminent si un analyste a complété tous les entrainements majeurs nécessaires pour retourner les informations répondant à une requête. Parallèlement et périodiquement, des tests de requêtes des analystes de la NSA sont menés.

Depuis Octobre 2011 et la persistance des procédures de minimisation de la Section 702 des autres agences gouvernementales, les procédures de minimisation de la Section 702 de la NSA ont permis au personnel de la NSA d'utiliser des identifiant de personnes US pour effectuer des requêtes sous l'autorité de la Section 702

lorsqu'une telle requête permet de retourner des informations sur les services secrets étrangers. la NSA distingue bien les requêtes sur le contenu des communication de celles sur les meta-data des communications. Les analystes de la NSA doivent fournir des justifications et recevoir une approbation supplémentaire avant que le contenu d'une requête sur l'identifiant d'une personne US ne soit utilisé. Concrètement, les analystes de la NSA devraient effectuer des requêtes, selon la Section 702, sur l'identifiant d'une personne US moins fréquemment que les requêtes, selon la Section 702, sur les meta-data. Par exemple, la NSA effectue une requête sur l'identifiant d'une personne US lorsqu'il est urgent de sauver la vie, telle qu'une prise d'otages. La NSA nécessite de conserver des enregistrements des requêtes sur une personne US et ces enregistrements sont disponibles à l'analyse par le DOJ et l'ODNI en tant que processus externes sous cette autorité. Au total, les procédures de la NSA interdisent à la NSA d'effectuer des requêtes sur les données entrantes de l'identifiant d'une personne US.

Existence de mesures de protection des données privées et des libertés civiles : Avec l'entraînement et les contrôle d'accès, la NSA poursuit l'audit et garde la trace de toutes les requêtes sous l'autorité de la Section 702. Les routines d'organisation du personnel du Signal Intelligence Directorate de la NSA revoie une partie de ces requêtes comprenant celles sur l'identifiant de personne US afin d'assurer que toutes ces requêtes ne sont seulement effectuées que quand elle sont appropriées. Le personnel du DOJ et de l'ODNI fournissent des renseignements supplémentaires assurant que la NSA recherche des données de manière appropriée. Ce mesures de protection comprennent la sécurité du FIPP, le chiffrage, l'audit et la qualité des données.

DISSEMINATION DES COMMUNICATIONS OBTENUES SOUS L'AUTORITE DE LA SECTION 702 PAR LES SERVICES SECRETS DERIVES DE LA NSA

La NSA génère uniquement des rapports sur les signaux des services secrets lorsque l'information concerne des services secrets spécifiques, concernant les rapports et informations sur une personne US. La dissémination des informations concernant une personne US figurant dans n'importe quel rapport des services secrets de la NSA est expréssément interdite tant qu'une telle information est nécessaire pour comprendre les informations des services secrets étrangers ou pour évaluer son importance, contient une preuve évidente de crime ou indique des menaces de mort ou de dommages corporels. Même, si une ou plusieurs de ces conditions sont appliquées, la NSA devrait inclure le minimum d'informations nécessaire sur une personne afin de comprendre le crime ou la menace. Par exemple, la NSA "masque" volontairement la véritable identité des personnes US par l'utilisation de la phrase "en tant que personne US" et par la suppression des détails pouvant conduire à les identifier avec succès dans ce contexte. Le contenu des rapports de la NSA peut être demandé pour que la NSA fournisse la véritable identité d'une personne US dissimulée et référencée dans un rapport des services secrets si il est légitime de connaître cette identité. Selon la politique de la NSA, la NSA peut être autorisée à révéler l'identité seulement sous certaines conditions et où des contrôles additionnels spécifiques ont été mis en place pour exclure la disséminations des informations futures, et des approbations supplémentaires ont été demandées à l'une des sept positions indiquées de la NSA. En plus, ensemble, le DOJ et l'ODNI revoient la plus grande variété possible de dissémination d'informations concernant les personnes US, obtenues sous l'autorité de la Section 702, en tant que partie de leurs processus de surveillance.

Existence de mesures de protection des données privées et des libertés civiles : Comme indiqué au-dessus, la NSA dispose d'une politique, de moyens techniques et de personnel sur place, capable d'attester que les données sont conservées en accord avec les procédures approuvées du FISC. Les processus automatiques pour effacer les collectes à la fin de la période de rétention s'appliquent autant pour les informations des personnes US ou que pour celles des personnes non US. Les informations devraient seulement être "non surveillées" dans des instances spécifiques constantes en rapport avec les procédures de minimisation et la politique de la NSA. Ces mesures de protection comprennent la minimisation du FIPP et les mesures de spécification..

CONSERVATION DES COMMUNICATIONS NON REVELEES, OBTENUES SELON L'AUTORITE DE LA SECTION 702

Le temps maximum, pendant lequel le contenu ou les metadata de communications spécifiques seront retenus, est établi dans les procédures approuvées de minimisation du FISC. Le contenu ou les metadatas non encore évalués par PRISM ou les données téléphoniques collectées selon la Section 702, sont conservées pas plus de cinq ans. Les données entrantes collectées depuis l'activité internet sont conservées pas plus de deux ans. La NSA respecte ces mesures de rétention dans ses processus automatisés.

Les procédures de la NSA spécifient également plusieurs instances pendant lesquelles la NSA doit détruire les données collectées sur un personne US rapidement avant leur reconnaissance. En général, ceci comprend toute instance pendant laquelle les analystes de la NSA reconnaissant que de telles collections ne sont pas clairement autorisés à proposer l'acquisition ne comprenant pas des preuves évidentes de crime. Au final, en l'absence d'exceptions limitées, la NSA doit détruire toute communication acquise lorsque tout utilisateur dont le compte surveillé a été trouvé sachant qu'il est localisé aux US pendant la période d'acquisition.

Existence de mesures de protection des données privées et des libertés civiles : La NSA dispose de moyens politiques, techniques de cohntrôles et de personnel sur place pour s'assurer que les données sont conservées en accord avec les procédures approuvées du FISC. Les processus automatique pour effacer kes collectes à la fin de la période de rétention s'appliquent autant sur les informations des personnes US que sur celles des personnes non US. Il n'existe pas de procédures manuelles pour détruire les informations des personnes US pour lesquelles les analystes de la NSA ont reconnu une preuve évidente de crime. Ces mesures de protection comprennent les procédures du minimisation et de sécurité du FIPP.

GESTION ORGANISATIONNELLE, CONFORMITE ET SURVEILLANCE

La NSA est sujette à des rapports de conformité internes et de surveillance extenes rigoureux. Comme beaucoup d'autres antités règlementées, la NSA dispose d'un programme de conformité d'entreprise, dirigé par le Directeur de Conformité de la NSA, dont la position est statutairement nécessaire. Le programme de conformité de la NSA est utilisé pour fournir des précisions dans les activités de la NSAafin d'assurer qu'elles sont accomplies en accord avec la loi et les procédures, comprenant, dans ce cas, les certifications de la Section 702 et accompagnant les procédures de ciblage et de minimisation de la Section 702 et les procédures additionneles recquises du FISC. En tant que structure conforme d'entreprise, la NSA dispose d'éléments conformes par l'intermédiaire de ses différentes organisations. La NSA recherche également à détecter des incidents non conformes le plus tôt possible. Losrque des éléments non conformes surviennent, par rapport à la manière dont la NSA émet des collects approuvées par le FISC, la NSA organise des actions correctives ; et, en parallèle, la NSA doit transmettre des rapports d'incidents non conformes à l'ODNIet au DOJ puis des rapports ultérieurs au FISC et au congrès, si celà est nécessaire.

Ces organisations, en rapport avec le Conseil Général de la NSA, l'Inspecteur Général de la NSA et le plus récent Directeur des Libertés Civiles et des Données Privées, ont des rôles critiques afin d'attester que toutes les actions menées par la NSA sont en accord avec les lois, la politique et les procédures qui dirigent les activités des services secrets. De plus, chaque analyste individuel de la NSA a la responsabilité d'assurer que ses activités personnelles sont complètement conformes. Tout particulièrement, cette responsabilité comprend les rapports sur toute situation pendant laquelle l'analyste a pu dépasser l'autorité afin d'obtenir, analyser et rapporter les informations des services secrets sous l'autorité de la Section 702.

Conformité : La NSA emet des rapports pour tous les incidents, il a pu être effectué des requêtes sur les données de la Section 702, sur lesquelles un analyste a pu commettre des erreur typographiques ou de dissémination. Le personnel de la NSA est obligé de rapporter lors que la NSA n'agit pas (ou ne doit pas agir) en accord avec les lois, la politique ou les procédures. Si la NSA n'agit pas conformément aux lois, à la politique ou aux procédures, la NSA devra informer de ceci à travers des rapports internes ou externes sur la surveillance des services secrets, diriger des revues permettant de comprendre l'origine de la cause et effectuer des éventuels ajustements dans ses procédures.

Si la NSA découvre qu'elle a surveillé un sélecteur utilisé par une personne localisée aux US ou une personne US, la NSA doit cesser la collecte immédiatement ; et, dans la plupart des cas, doit aussi effacer toutes les données collectées qui en dépendent et doit supprimer ou revoir tout rapport disséminé, basé sur ces données. La NSA encourage également les rapports spontannés de son personnel ou les recherches de n'importe quelle error basés sur l'entrainement supplémentaire ou tout autre mesure nécessaire. A la suite d'un incident, une série de solutions doit être prise ; la réalisation d'un rapport écrit doit être effectué, demandant le niveau de connaissances que l'analyste a échoué pendant son entrainemente et/ou les tests recquis. Au total, pour rapporter les informartions décrites plus haut, toute violation intentionnelle de la loi sera rapportée au Bureau de l'inspecteur Général de la NSA. Jusqu'à maintenant, il n'y a pas eu de telles instances, qui n'ai été confirmée par le groupe de consultation du Président sur les services secrets et sur les technologies de communication.

Surveillance externe : Selon les procédures de ciblage indiquées dans la Section 702, autant le DOJ que l'ODNI dirigent les rapports sur les routines de surveillance. Les représentants de ces 2 agences visitent la NSA 2 fois par mois. Ils y examinent les fiches techniques de surveillance que la NSA fournit au DOJ et à l'ODNI pour déterminer si la fiche de surveillance est conforme aux documentations standards recquises par les procédures de ciblage de la NSA et founit suffisament d'informations aux consultants pour vérifier les bases de détermination de qui est étranger. Pour les informations satisfaisant les standards, aucune documentation supplémentaire n'est recquise. Pour les informations concernant les revues ultérieures, la NSA fournit au DOJ et à l'ODNI des informations supplémentaires, pendant ou après l'étude sur site. La NSA reçoit les commentaires des équipes du DOJ et de l'ODNI et ajoute ces informations dans les entrainements formels et informels de ses analystes. Le DOJ et l'ODNI revoient également un grande variété d'informations et de rapports disséminés qui comprennent les informations sur la personne US.

Existence de mesures de protection des données privées et des libertés civiles : Les processus de conformité et de surveillance autorisent la NSA à identifier tout problème le plus tôt possible dans les processus permettant de réduire l'impact sur les données privées et les libertés civiles. Ces mesures de protection comprennent la transparence des organisations de surveillance le chiffrage et l'audit du FIPP.

CONCLUSION

Ce rapport, préparé par le bureau des libertés civiles et des données privées de la NSA, fournit une description compréhensive des activités de la NSA liées à la Section 702. Ce rapport informe également sur les mesures de protection des données privées et des libertés civiles.

Liens:
[1] http://fr.scribd.com/doc/219842108/NSA-Unclassified-Report-on-Prism
[2] http://freegovinfo.info/files/NSA-Section-702-FISA-Section-215-USAPA-Fact-Sheets.pdf