

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article4463>

# Ecoute électronique : les FAI américains contraints d'obtempérer

- Renseignement - International -



Date de mise en ligne : mardi 15 mai 2007

---

Spyworld Actu

---

### **Une nouvelle version de la loi CALEA oblige les FAI à prévoir des équipements de surveillance pour faciliter le travail de la police. Attention aux dérives, prévient l'EFF.**

Aux Etats-Unis, les fournisseurs d'accès à Internet, les câblo-opérateurs, ainsi que certaines universités, avaient jusqu'au 14 mai pour installer des équipements permettant d'aider les services de police et les agences fédérales de renseignement à surveiller les habitudes de surf des internautes.

Les fournisseurs d'accès devront désormais se soumettre à la nouvelle interprétation de la loi [Communications Assistance for Law Enforcement Act](#) (Calea) de 1994, étendue par la [Federal Communications Commission](#) (FCC).

Dans sa version initiale, la loi autorisait les autorités de police à effectuer des écoutes téléphoniques d'un individu à partir d'un terminal mobile, qui a finalement conduit à une augmentation considérable de ce type de pratiques d'espionnage.

Il y a cinq ans, la FCC est parvenue, à force de pressions, à étendre l'application de cette loi aux connexions à Internet. Cette extension a finalement été acceptée par la justice américaine en juin 2006.

Si les équipements que doivent installer les fournisseurs d'accès Internet ne permettent pas une surveillance continue de tous les individus, ils facilitent grandement la mise en place d'écoutes.

Les nouveaux équipements devraient permettre d'assurer une surveillance quasiment immédiate après réception d'une injonction par un tribunal.

L'analyse des données pourra être effectuée par la police ou par des tiers, ce qui a suscité la colère des groupes de défense de la vie privée.

"[VeriSign](#) offre aux FAI empruntant son réseau télécoms un service d'interception des appels légaux . Ce qui les oblige à acheminer toutes leurs données vers VeriSign," déplore l'[Electronic Frontier Foundation](#) (EFF). "Des collaborateurs de VeriSign procèdent alors à l'analyse des données et à l'extraction des informations concernées par l'injonction avant de les retourner aux services de police".

Un système qui sous-tend des risques de dérive, selon EFF. "Cette méthode de communication rend les données personnelles potentiellement vulnérable. Car les informations transitent entre le réseau du fournisseur d'accès et celui de VeriSign. Ce dispositif place également les données personnelles de personnes innocentes entre les mains d'un tiers sans leur consentement."

Traduction adaptée d'un article de [VnUNET.com](#) en date du 14 mai 2007

*Post-scriptum :*

<http://www.vnUNET.fr/fr/vnUNET/news...>