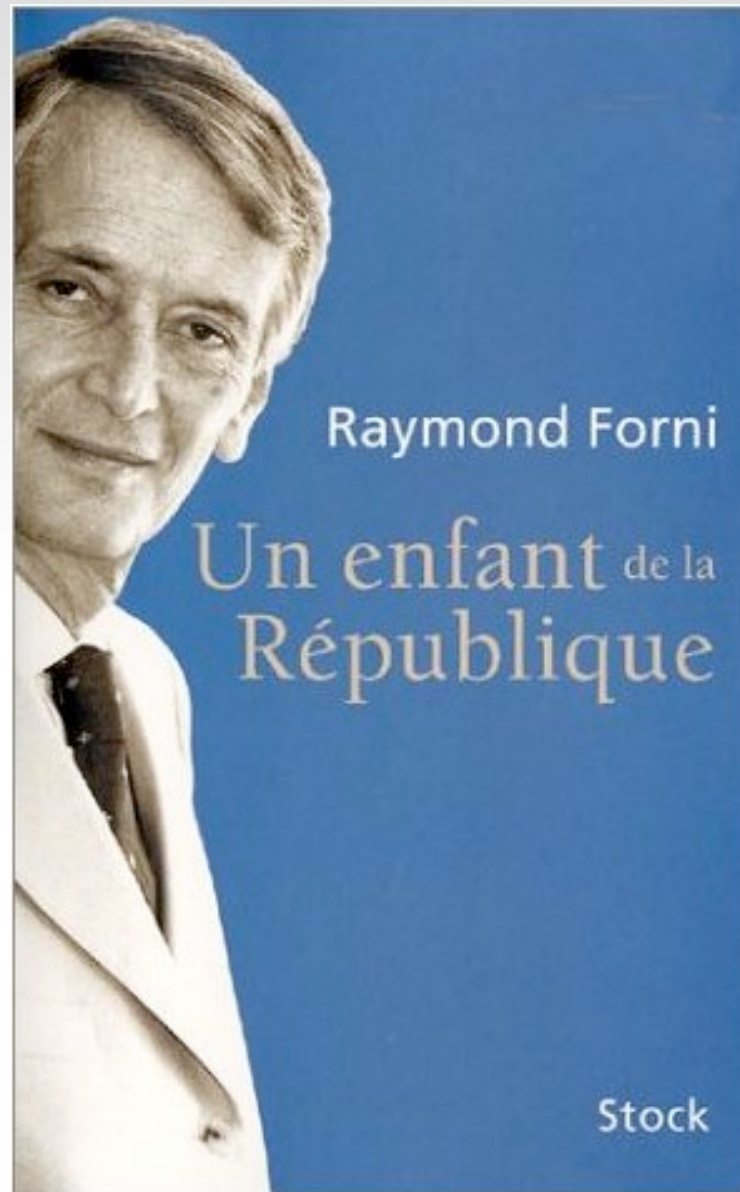


ÉTATS GÉNÉRAUX DE L'IDENTITÉ NUMÉRIQUE  
Palais du Luxembourg, lundi 27 avril 2009

# Comment contourner les systèmes de surveillance et de traçabilité ?

Jean-Marc Manach, journaliste internet,  
internetactu.net, bugbrother.net, lemonde.fr  
& co-organisateur des Big Brother Awards



“Dans une démocratie, je considère qu’il est nécessaire que subsiste un espace de possibilité de fraude. Si l’on n’avait pas pu fabriquer de fausses cartes d’identité pendant la guerre, des dizaines de milliers d’hommes et de femmes auraient été arrêtés, déportés, sans doute morts. J’ai toujours été partisan de préserver de minimum d’espace sans lequel il n’y a pas de véritable démocratie.”

Raymond Forni, considéré comme le “père inspiré de la loi Informatique et libertés”, trois fois vice-président de la CNIL entre 1981 et l’an 2000, poste qu’il quitta pour devenir président de l’Assemblée Nationale.

# "Soyez paranoïaques et apprenez à dire non !"

L'espionnage ?

- . à 60% économique, scientifique et industriel
- . à 40% politique, diplomatique ou de défense

"Il faut cesser d'être naïf et de croire au hasard :  
95% des vols d'ordinateurs sont ciblés".

Des pirates ? Non, des "corsaires" : services de renseignements, sociétés de renseignements privées, concurrence, groupes mafieux et criminalité organisée

- . clefs USB qui aspirent les documents dans les PC,
- . douaniers qui "confisquent" les ordinateurs portables...

"Cryptez les informations importantes, surtout sur les terminaux mobiles.



Et surtout n'oubliez pas de faire appel à la DST si nécessaire.  
La DST fait de l'audit, de la sensibilisation et organise des conférences.  
« N'hésitez pas à venir nous voir. Nous sommes joignables au  
01.77.92.50.00 ». (Le n° est aujourd'hui celui de la DCRI).

Réf.: "DST : Les attaques arrivent rarement par hasard..." (globalsecuritymag.fr)

# Sécurité & protection de la vie privée font peur... aux autorités

Philip Zimmermann, le créateur de PGP, le pionnier des outils grands publics de cryptographie, fut longtemps harcelé par les autorités américaines.

security.tao.ca, le seul site qui explique comment "se protéger dans un monde constamment surveillé" (cf [bugbrother.com/security.tao.ca](http://bugbrother.com/security.tao.ca)), considéré comme une menace "hacktiviste" par l'organisme américain de protection des infrastructures internet.



La CNIL? Elle explique certes comment nous sommes "pistés sur l'internet", mais nullement comment se protéger...

securite-informatique.gouv.fr, censé aidé les Français à se familiariser avec les rudiments de la sécurité informatique... n'a été lancé qu'en 2008...



...et son logiciel ANSMO (apprécier le niveau de sécurité d'un micro-ordinateur) d'éducation et de recommandations est toujours "disponible prochainement".

# Mais comment, et où, apprendre à se protéger ?

Les lois visant à placer les internautes sous surveillance sont “techniquement ineptes et inefficaces à l’encontre des criminels” et risquent, a contrario, de “saper le droit à la vie privée et à la sécurité des citoyens et du marché”.

Un ex-directeur des communications électroniques stratégiques du ministère de la Défense britannique et de l’OTAN, qui explique comment les contourner, légalement.



En résumé :

- . crypto "pour les masses" (GPG, financé par l'Allemagne)
- . anonymiseurs (TOR, développé par l'EFF)
- . coffres-forts électroniques
- . effacement sécurisé des données
- . LiveCD bootables (pas de traces sur le PC)
- . logiciels libres (les seuls -ou presque- a être sécurisés)

Contourner la traçabilité - jean marc manach

# Une question (ou un problème) politique



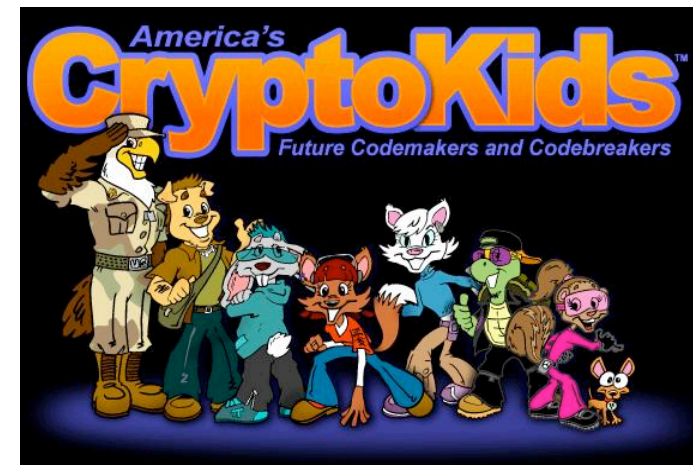
En ces temps de "guerre économique" et de "guerre de l'information", prérogatives de l'armée et des services de renseignement, les gouvernements n'aiment pas expliquer à leurs citoyens comment se protéger, mais sensibilisent les entreprises à la sécurité informatique.

En France, [internetsanscrainte.fr](http://internetsanscrainte.fr), site grand public, est à destination des... 7-12 ans, et vise plus à les protéger des "dangers" du Net qu'à leur apprendre à en maîtriser les outils, pour mieux en embrasser les possibilités.



A contrario, et aux USA, la NSA a quant à elle un site ludique destiné à initier les enfants à la cryptographie... Les hackers y ont droit de cité, militaires et "services" n'hésitent pas à en recruter, et la surveillance des internautes, notamment par la NSA, y fait scandale.

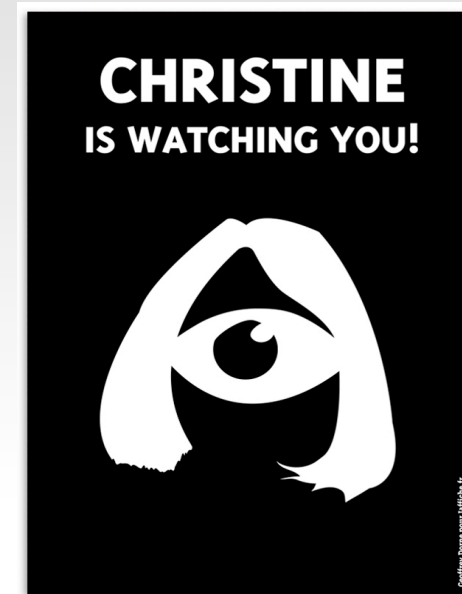
En France, le premier "club" de hackers avait été créé par... la DST.



# En attendant...

. vous pouvez téléphoner à la DCRI...  
pour qui la non-utilisation d'un téléphone  
portable fait de vous un suspect

. vous pouvez aussi faire confiance aux  
ministères de l'Intérieur et de la Culture,  
qui n'ont de cesse d'inciter les internautes  
à apprendre à se protéger sur le Net



A ce jour, seuls les défenseurs des droits de  
l'homme expliquent comment se protéger.  
REF : <http://fr.security.ngoinabox.org/>

Demain ? Google, Facebook et autres "services sociaux", intermédiaires  
privés qui, sauf à ce que l'on se défie, aussi, de leurs pouvoirs de surveillance,  
n'auront d'autre choix que de nous aider à protéger nos identités.

# Des questions ?



<http://bugbrother.blog.lemonde.fr>

<http://internetactu.net>

<http://bigbrotherawards.eu.org>

Contourner la traçabilité - jean marc manach