

# PRIVACY HORIZONS: TERRA INCOGNITA

29<sup>th</sup> International Conference of  
Data Protection and Privacy Commissioners

September 25 to 28, 2007  
Montreal, Canada



## LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29<sup>e</sup> Conférence internationale des commissaires  
à la protection des données et de la vie privée

du 25 au 28 septembre 2007  
Montréal, Canada

# Le combat pour la localisation : des préoccupations conflictuelles ne favorisent pas la protection de la vie privée ni l'innovation

John Morris

Center for Democracy & Technology

[jmorris@cdt.org](mailto:jmorris@cdt.org)

# Vue d'ensemble

- Les bonnes nouvelles : les progrès technologiques peuvent *améliorer* la protection de l'information sur la localisation
  - GeoPriv
- D'autres exigences sociétales viennent toutefois menacer ces initiatives
  - Les exigences des services d'appel d'urgence 911
  - Les exigences en matière de surveillance de l'application de la loi
- Tout cela peut nuire à la protection de la vie privée *et* freiner l'innovation

# GeoPriv

- Norme technique visant à protéger le caractère privé des informations sur la localisation
- Le groupe d'études sur l'ingénierie Internet (IETF) en a commencé l'élaboration en 2001
- Créé en réponse aux propositions au sujet de la localisation qui ne tenaient pas compte des incidences sur la protection de la vie privée des renseignements permettant la localisation

# La norme GeoPriv

- Exige que des règles fondamentales de protection de la vie privée *soient* transmises en même temps que les informations sur la localisation
- Les règles de protection et les informations sur la localisation font partie de la même enveloppe « électronique »
- Les règles de protection fondamentales comprennent :
  - Le délai de conservation fixé
  - Le consentement de retransmission (ou son absence)
  - Des conseils en vue de créer des règles de protection de la vie privée stockés à l'externe plus strictes.

# Des règles plus strictes sont possibles

- Les règles strictes peuvent comprendre certaines conditions :
  - *Identité* : qui peut connaître ma localisation
  - *Validité* : quand ma localisation peut-elle être donnée
  - *Sphère* : au travail, à la maison, en voyage?
- Permet une règle comme celle-ci : « Si je suis au travail, les personnes suivantes peuvent être informées du lieu où je me trouve. »
- *Ne présume pas* que le réseau ou le fournisseur d'accès Internet exercera un contrôle sur l'information concernant la localisation – permet des « fournisseurs de protection de la vie privée tiers »

# La mise en place de GeoPriv

- L'IETF prévoit que la norme peut s'appliquer à **toutes** les transmissions de renseignements permettant la localisation qui utilisent des protocoles IETF, p. ex., SIP (VoIP/IM)
- Plans initiaux pour mettre en application GeoPriv :
  - 3GPP – communications sans fil
  - NENA (É.-U.) – communications d'urgence
- Exige des lois locales/nationales pour faire appliquer les règles de protection de la vie privée qu'implique GeoPriv

# Les mauvaises nouvelles

- Des plans d'action sociaux/nationaux en concurrence établissent des exigences techniques qui viennent saper GeoPriv et les autres efforts visant à protéger les renseignements sur la localisation
- Diverses propositions nous feraient passer directement dans la société de surveillance dont parlait Orwell

# Service d'appel d'urgence 911

- Exigences proposées très problématiques :
  - Exigence d'emplacement fourni par un *réseau*
  - Les dispositifs doivent être localisables « automatiquement »
  - « Tous les dispositifs IP » sont couverts
- Tort causé à la protection de la vie privée
  - Les utilisateurs n'exercent plus le contrôle
  - Le repérage peut être fait sans la participation de l'utilisateur
  - De plus en plus de dispositifs peuvent être repérés
- Tort en matière d'innovation
  - Certains dispositifs ne peuvent répondre aux exigences

# Surveillance de l'application de la loi et repérage de la localisation

- Débat permanent aux États-Unis à propos de la norme juridique d'accès aux informations sur la localisation
- Les exigences techniques liées à l'exécution de la loi soulèvent de graves préoccupations en matière de protection de la vie privée (CALEA)
  - L'emplacement de la station de base n'est pas adéquat >> GPS
  - Pour ce qui est des voix par IP et d'autres dispositifs IP, la loi américaine exige de contrôler la conception initiale des nouvelles technologies

# Préoccupations au sujet de la protection de la vie privée *et* de l'innovation

- Tort évident causé à la protection de la vie privée
  - Perte du contrôle effectué par l'utilisateur et perte de la connaissance
  - Meilleur accès commercial à l'emplacement
  - Capacité « de repérage en permanence »
- Les limites en matière d'innovation et de nouvelles technologies peuvent aussi nuire à la protection de la vie privée ou la réduire
  - Pourraient empêcher la création de dispositifs plus simples, moins repérables
  - Pourraient empêcher des tiers d'offrir des services de protection de la vie privée

# Conclusions

- De nouvelles technologies de localisation peuvent menacer la protection de la vie privée
- Mais ces technologies peuvent aussi protéger la vie privée
- Des objectifs de société fondés sur de bonnes intentions peuvent nuire à la protection de la vie privée pour ce qui est de la localisation
- Nous devons équilibrer les objectifs sociétaux (service d'urgence 911, exécution de la loi) avec le besoin de protéger la vie privée

# Questions

John Morris

Center for Democracy & Technology

Washington, D.C., É.-U.

+1 202.637.9800

[jmorris@cdt.org](mailto:jmorris@cdt.org)