PRIVACY HORIZONS: TERRA INCOGNITA

29th 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

29e Conférence internationale des commissaires à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Informatique ubiquiste

Le suivi géodépendant

Président
M. Alexander Dix, Ph. D.
Commissaire à la protection des données et à l'accès à l'information de Berlin (Allemagne)

Überveillance : Surveillance et repérage des gens – 24/7 x 365

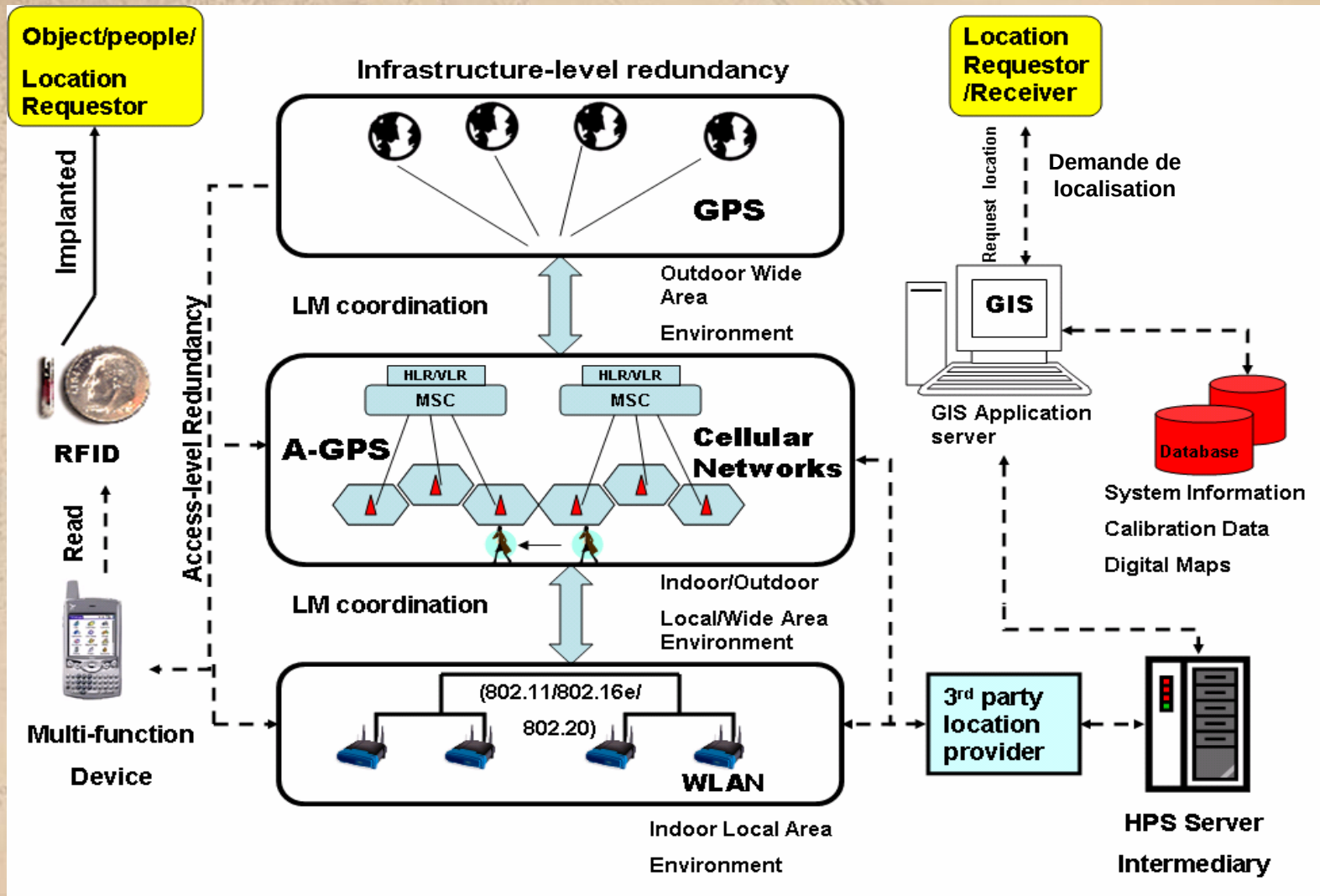
Michael G. Michael

katina@uow.edu.au, (61)242213937

Université de Wollongong, Australie

Classer les services et technologies géomatiques

- En réseau ou axés sur des dispositifs ou hybrides
- Localisation précise par opposition à localisation de proximité
- À l'intérieur/à l'extérieur, campus fermé/global
- Consommateurs, entreprises, gouvernements
- Utilisés pour repérer des objets, animaux et personnes
- Volontaires par opposition à obligatoires
- Services de géomatique : pousser ou tirer



HLR: Home Location Register VLR: Visitor Location Register
MSC: Mobile Switching Center LM: Location Management
▲: Base Station : Access Point : GPS Satellite

Chew & Michael, 2005

Approches pratiques pour mesurer les répercussions en matière de protection de la vie privée

- Avant de diffuser largement une innovation
  - Discussion et débat
    - Participation des citoyens et des secteurs privé et public
  - Planification fondée sur un scénario
    - Méthode historique; tirer des leçons du passé
    - Meilleur scénario/pire scénario et déconstruction/interprétation
  - Évaluation de la technologie et prévision
    - Consulter un groupe d'experts universel ayant des antécédents diversifiés
- Après avoir largement diffuser l'innovation
  - Analyse fondée sur la jurisprudence
  - Examen des normes techniques, lignes directrices et protocole
  - Une pratique fondée sur des preuves permet de mettre au point la réglementation

Le repérage omniprésent : réalité ou fiction?

- Le repérage omniprésent est ici, MAINTENANT
  - Exemple : Les fournisseurs de services logistiques repèrent des cargaisons
    - DHL-Asie soutient qu'il « localise quotidiennement » 5 millions de colis
- Le repérage de personnes est-il omniprésent?
  - Êtes-vous un criminel ou soupçonné d'activités terroristes?
    - Les organismes chargés d'appliquer la loi peuvent repérer quiconque (mandat)
  - Êtes-vous détenu dans une prison ou avez-vous un dossier médical?
    - Les groupes minoritaires sont toujours ceux qui adoptent les premiers (essayabilité)
- Équilibre nécessaire entre les points de vue extrêmes
  - L'industrie *fait* la promotion de l'omniprésence auprès de ses clients
  - Les défenseurs de liberté civile *ne sont pas* toujours pleinement informés

Le débat qui fait couler beaucoup d'encre au sujet des étiquettes d'IRF dans le commerce de détail

- Tirer des leçons de l'expérience du code à barres des années 1970 et +
- Avons-nous besoin d'un « dispositif d'arrêt » sur les étiquettes d'IRF?
  - Quel type d'information l'étiquette révèle-t-elle au-delà de l'utilisation qu'on fait de sa carte de crédit (habitudes de dépense)?
  - Perspectives d'avenir : lecteurs importuns ou non
- Devrions-nous être plus inquiets des techniques d'« anticlonage » des étiquettes d'IRF?
- Quelle est la proposition de valeur des étiquettes d'IRF pour
  - les commerces : gestion de la chaîne d'approvisionnement, contrôle des stocks, etc.
  - les consommateurs : plus « pratiques » (reste à prouver)
- Et que dire des étiquettes d'IRF dans les passeports/péages biométriques?

Encourager le développement d'une technologie naissante

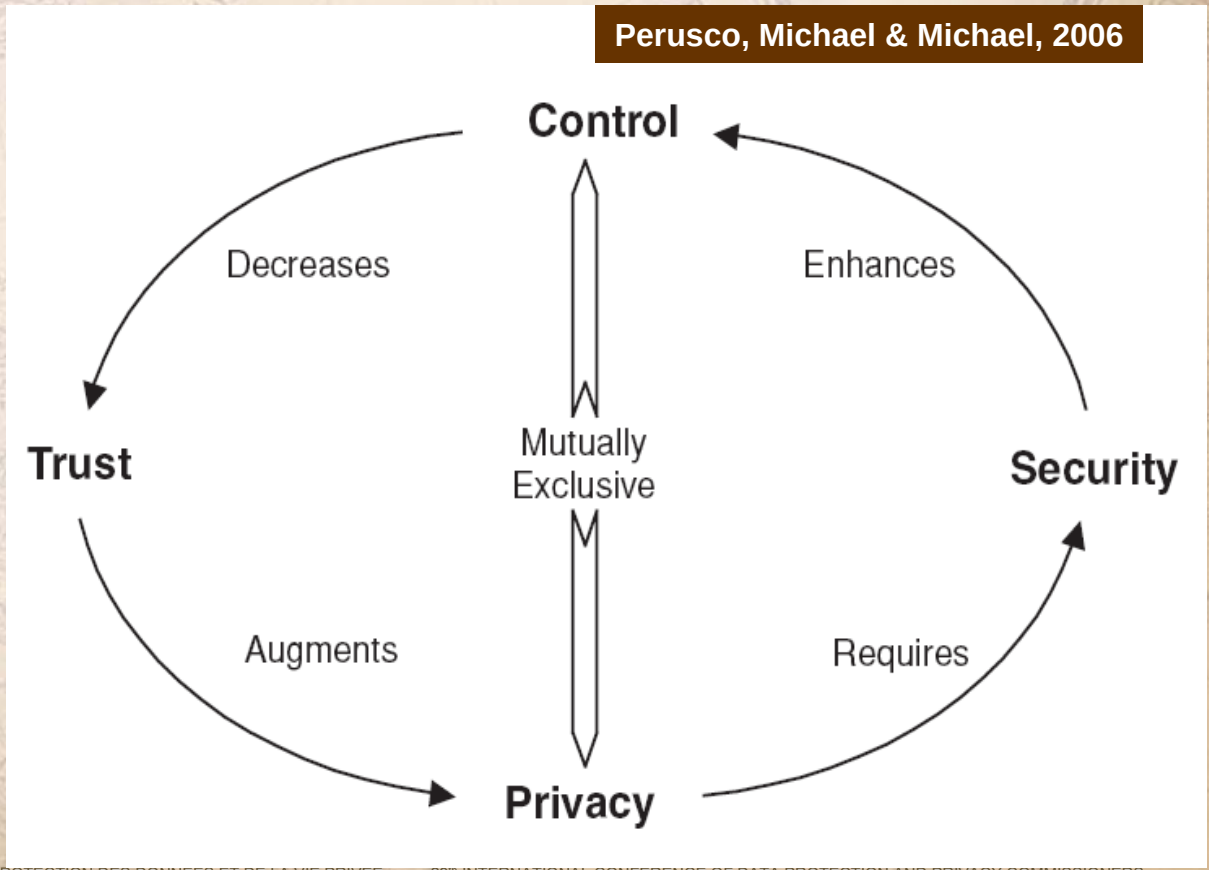
- Il est important d'éduquer le consommateur
  - Pour ce qui est de l'IRF cela *ne peut* attendre après la mise en place
- Les mesures de protection et l'appui dépendent de la facilité d'emploi
  - *Pas* de solution unique
  - Exemple : étiqueter des objets et implanter des transpondeurs sur des personnes (même si c'est volontaire), c'est très différent
- Il s'agit de se demander si l'IRF :
  - (A) Est une technologie à la recherche d'un problème que font valoir les vendeurs?
  - (B) Est une entreprise électronique intéressante pour l'avenir?
  - (C) Est une *autre* technologie provisoire qui répond à des besoins perçus?
  - (D) Est un véhicule servant à exercer une surveillance globale d'objet à sujet?

Le droit des personnes de refuser le repérage

- Est-ce que la personne qui fait l'objet « d'un repérage » est :
  - mineure, atteinte de maladie mentale ou invalide, citoyen du pays ou étranger, mari ou femme, une personne qui a loué un véhicule, un porteur d'assurance-vie, une personne ayant un dossier médical, l'employé d'une entreprise, un criminel, etc.
- Consentement personnel informé et non pas donné par un tiers (procuration)?
- Besoin de respecter les principes/croyances des personnes
- Accessibilité requise aux services par le biais de multiples mécanismes
  - Par exemple, il y a des gens qui ne possèdent pas de cellulaire, qui ne veulent pas d'Internet pour avoir accès à des services bancaires électroniques et ne croient pas aux facilités de crédit (et c'est leur droit; ils ont le droit qu'on les laisse tranquilles)
- Une personne devrait être informée de la fréquence des signalements de localisation
  - Tous les jours, toutes les heures, à la minute/seconde, selon les exigences des douanes
- Les « transactions de scrutation » doivent être transparentes pour l'abonné

Dilemmes en matière de localisation

- Exactitude
- Accessibilité
- Protection de la vie privée
- Propriété
- Contrôle
- Sécurité
- Confiance
- Coût



Mot de la fin

- Les renseignements sur les lieux peuvent en dire long sur nos relations, nos traits, nos attirances et incompatibilités, nos déplacements, etc.
- Les services de localisation peuvent présenter divers problèmes :
  - La mésinformation
  - La fausse interprétation
  - La manipulation de l'information
- Les services de localisation peuvent accroître la sécurité nationale et personnelle
  - Mais quelle part de notre vie privée sommes-nous prêt à échanger contre une sécurité accrue?
- L'Überveillance est ici maintenant : une surveillance *presque* omniprésente, exceptionnelle, 24 heures par jour, 7 jours par semaine, 365 jours par année
- Il faut prendre en considération la trajectoire des services de localisation
  - Systèmes de positionnement hiérarchique (services convergents)
  - Services de localisation à dispositif IP (dispositifs de localisation)
  - L'essor de l'Électrophore (l'« être humain » comme nœud sans fil)

Surveillance Web 2.0 : Traçabilité dans l'Internet des choses

David Lyon
Professeur de sociologie à l'Université Queen's
Kingston (Ontario)

Questions de protection de la vie privée et de sécurité et services géodépendants

Eloïse Gratton
associée, McMillan Binch Mendelsohn

McMillan Binch Mendelsohn

Introduction

- Les technologies sans fil et la protection de la vie privée

- **Collecte de données personnelles et de localisation**

  - Profilage statistique
  - Profilage dynamique
  - Profilage axé sur la localisation

- **Pourriels sans fil**

- Cadre juridique

- Canada : la *LPRPDÉ* et les lois provinciales
- États-Unis : Safe Harbor Agreement
- Europe : Directives de la CE

Qui devrait autoriser la communication/obtenir l'autorisation de communiquer?

Communication : le responsable de la collecte des données devrait communiquer à la personne sur laquelle portent les données le type de données qu'on recueille sur elle et la raison de la collecte.

Destinataire de la communication : La personne sur laquelle portent les données

Questions :

- Statut des données de localisation anonymes
- Propriété des données de localisation

Fournisseur de la communication : le responsable de la collecte des données

Question :

- Diverses parties en cause : fournisseur de services géodépendants, fournisseur de contenu, exploitant de réseau, etc.

Comment la communication doit-elle être assurée?

Méthode :

- Cadre juridique :
  - Oralement ou par écrit
  - Selon la nature de l'entreprise
  - Sur le dispositif sans fil, lorsque cela est possible techniquement

- Méthode suggérée : dans un contrat de services

À quel moment :

- Cadre juridique :
  - Avant l'utilisation ou la collecte de ces données

- Moment suggéré : avant la collecte

Le contenu de la communication

- Collecte des données :
  - Type et qualité des données recueillies
  - Méthode de collecte des données et raison
  - Identité de la personne responsable de la collecte, établissement et procédure à suivre pour déposer une plainte
- Sécurité des données, entreposage et transfert
- Accès aux données
- Choix et consentement :
  - Période de validité du consentement
  - Consentement retiré et conséquences liées au refus
  - Mise à jour dans la politique sur la protection de la vie privée

Obtenir le consentement

Consentement : Le responsable de la collecte des données doit obtenir le consentement de la personne sur qui elles portent avant d'en recueillir ou d'en utiliser les renseignements personnels.

De qui obtenir le consentement?

- Les utilisateurs de cellulaires faisant l'objet d'un repérage (anonyme ou non) :
  - Chaque dispositif transmet un identificateur unique
  - Le dispositif appartient en général à une personne
- Les utilisateurs de cellulaires reçoivent un contenu fondé sur l'emplacement

Qui devrait obtenir le consentement?

L'exploitant du réseau :

- Il a déjà une relation avec les utilisateurs de cellulaires
- Motivation pour protéger les données de localisation

Contenu du consentement

- Questions relatives à la collecte des données, utilisation des données de localisation, etc.

- Questions relatives aux messages :

  - Nombre et fréquence des messages

  - Fournisseur et type de messages

  - Le moment où arrivent les messages

  - La localisation des messages

- Absence de consentement :

Est-ce que des personnes qui refusent tout type de repérage doivent être légalement autorisées à recevoir des produits et services équivalents qui n'utilisent pas le repérage.

Questions de sécurité

Sécurité : Des mesures de sécurité raisonnables doivent être appliquées pour protéger les données recueillies contre la perte accidentelle, le vol, la publication, etc.

Questions :

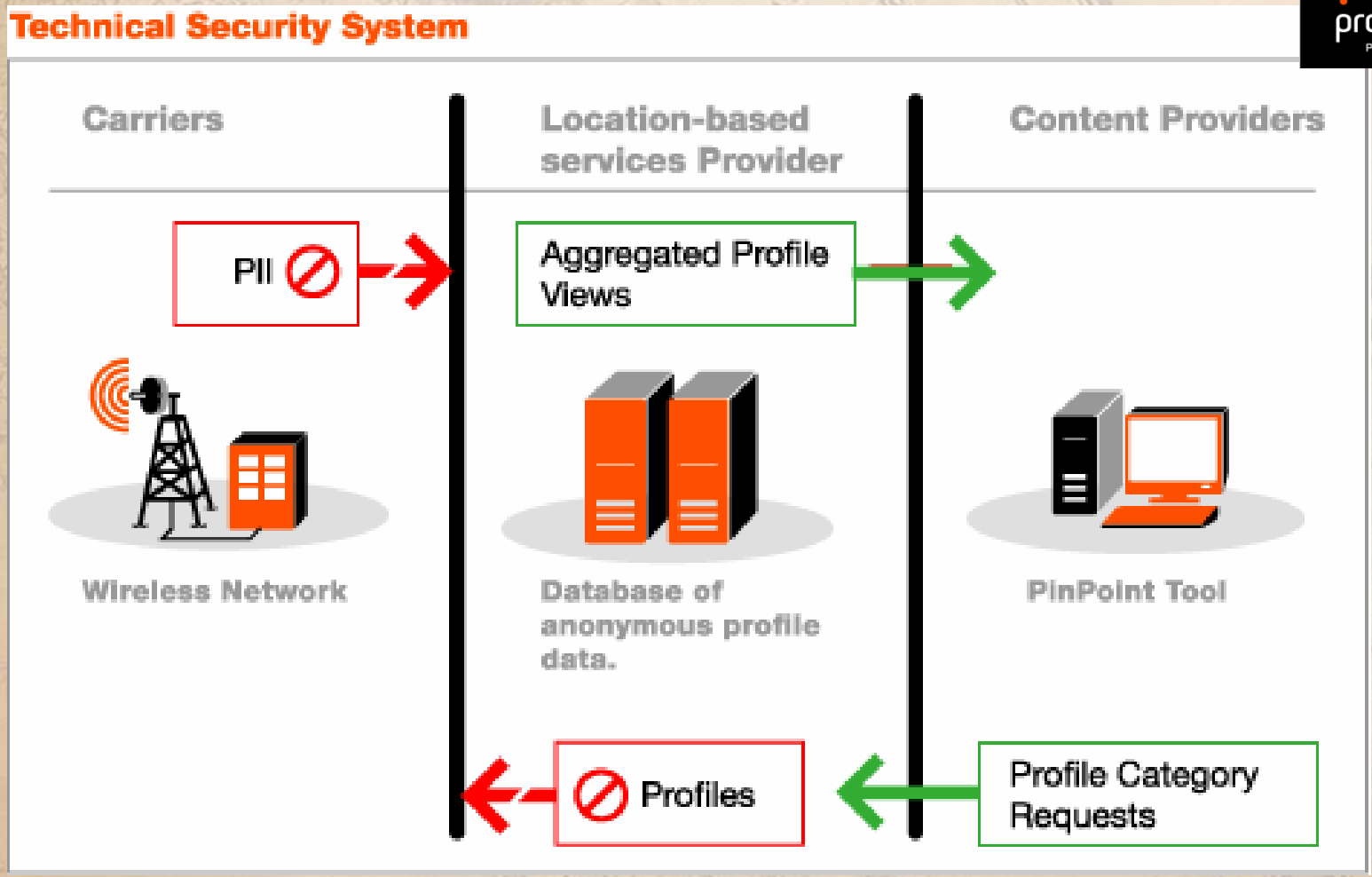
- Quelle est la technologie de repérage de localisation la plus sûre?

- Qu'est-ce qu'un système de sécurité technique « raisonnable »?

- Quel est le modèle de gestion approprié?

- Questions liées à l'entreposage.

Système de sécurité : Étude de cas



Autres principes de protection de la vie privée

- Qualité des données :

  - Les données utilisées et recueillies doivent être exactes et pertinentes compte tenu du motif de la collecte

- Transfert des données :

  - À quelles conditions les données de localisation doivent-elles être mises à la disposition de tierces parties, y compris les organismes chargés d'exécuter la loi?

- Accès aux données :

  - Le responsable de la collecte des données doit accorder à la personne sur laquelle portent ces données un accès raisonnable aux renseignements recueillis dans une forme qui lui est intelligible

Conclusion

- Les lignes directrices facultatives ou lois existantes pourraient ne pas être suffisantes pour régir l'utilisation des données de localisation

- Les lois sur la protection de la vie privée sont rédigées en termes généraux; par conséquent, l'industrie doit traduire le cadre juridique de la protection de la vie privée en pratiques de gestion qui tiennent compte :

  - De l'intérêt de l'industrie et des utilisateurs de cellulaires

  - Des questions de protection de la vie privée liées à l'utilisation des cellulaires

  - Des questions de juridiction : utiliser le cadre de protection de la vie privée le plus stricte.

McMillan Binch Mendelsohn

Questions?

Courriel : eloise.gratton@mcmbm.com
Tél. : 514-987-5093

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

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