

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

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

du 25 au 28 septembre 2007
Montréal, Canada

The Battle over Location: Competing Agendas Harming Privacy and Innovation

John Morris

Center for Democracy & Technology

jmorris@cdt.org

Overview

- The Good News: Technological initiatives can *enhance* the privacy of location information
 - GeoPriv
- But other societal demands are threatening those initiatives
 - e911 emergency call requirements
 - Law enforcement surveillance demands
- This can harm privacy *and* innovation

GeoPriv

- A technical standard aimed at protecting the privacy of location information
- Development started in 2001 by the Internet Engineering Task Force (IETF)
- Created in response to proposals about location that ignored privacy implications of location information

The GeoPriv Standard

- Requires that basic privacy rules *must* be transmitted alongside location information
- Privacy rules and location information are contained in the same electronic “envelope”
- Basic privacy rules include:
 - Time limit on retention
 - Retransmission consent (or lack thereof)
 - Pointer to more robust externally-stored privacy rules

Robust Rules Possible

- Robust rules can include conditions for:
 - *Identity*: who can receive my location
 - *Validity*: when can my location be provided
 - *Sphere*: am I at work, at home, traveling?
- Allows for rules like “if I am at work the following people can learn my location”
- Does *not* assume that the network or access provider will control location information -- allows third party “privacy providers”

GeoPriv Deployment

- Intended by IETF to be used for **all** transmissions of location info using IETF protocols, e.g., SIP (VoIP/IM)
- Initial plans to implement GeoPriv:
 - 3GPP -- wireless communications
 - NENA (US) -- emergency communications
- Requires national/local laws to enforce privacy rules conveyed by GeoPriv

The Bad News

- Competing national/social agendas are setting technical requirements that undermine GeoPriv and other efforts to protect location privacy
- Various proposals would have us skip straight to the Orwellian surveillance society

e911

- Highly problematic proposed requirements:
 - Demand for *network*-provided location
 - Devices must be “automatically” locatable
 - “All IP-enabled” devices covered
- Harm to privacy
 - Takes control away from users
 - Tracking can be done without user involvement
 - More and more devices can be tracked
- Harm to innovation
 - Some possible devices cannot meet requirements

Law Enforcement Surveillance and Location Tracking

- On-going debate in U.S. about legal standard for access to location info
- Technical demands by law enforcement raise serious privacy concerns (CALEA)
 - Cell tower location not adequate >> GPS
 - In VoIP and other IP-enabled contexts, U.S. law enforcement wants to control initial design of new technologies

Concern about Both Privacy *and* Innovation

- Clear harms to privacy
 - Loss of user control and knowledge
 - Greater commercial access to location
 - “Always on tracking” capability
- Limitations on innovation and new technology can also harm or diminish privacy
 - May preclude simpler, less trackable devices
 - May preclude third parties offering privacy protection services

Conclusions

- New location technology can threaten privacy
- But technologies can also protect location privacy
- Well-intended societal goals can harm location privacy
- We need to balance other societal goals (911, law enforcement) with need to protect privacy

Questions

John Morris

Center for Democracy & Technology

Washington, D.C., U.S.A.

+1 202.637.9800

jmorris@cdt.org