INTUG

ITU/MIC, Seoul 4-5 March 2004

www.INTUG.net

privacy and identity
in a (more) mobile world

Ewan Sutherland
Executive Director
International Telecommunications Users Group
ewan@intug.net

INTUG contents

- INTUG
- what users want
- principles
- threats and risks
- location
- roaming
- cameras
- conclusions and issues

INTUG what is INTUG?

- members
  - national associations
  - corporations
  - individuals
- activities
  - ITU and WTO
  - OECD
  - APEC TEL, CITEL and EU

INTUG our aims

- real and effective competition
- genuine choice for users
- lower prices
- higher quality
- more innovative services
- constructive co-operation with
  - international bodies
  - governments
  - regulators

INTUG priorities

1. open access to global mobile networks
2. regulatory best practice
3. liberalization
4. leased lines
5. IP telephony
6. digital divide
7. universal access
8. numbering

INTUG principles

- economic growth:
  - openings for innovation
  - removal of barriers to adoption
- privacy and data protection
- technological neutrality:
  - issues are ubiquitous
- open access

INTUG wants and needs

Consumers:

- secure
- private
- free choice:
  - networks
  - operators
- low price
- new services

Service providers

- open networks
- fair and non-discriminatory access
- secure transfer of:
  - data
  - transactions

Free choice of telecommunications platform.
GSM, cdma2000, BCN, Wi-Fi, PSTN, etc.

accenture definition

- always on
- always aware
- always active
- continuously analysing situations to provide access to content and services that are relevant and useful

OECD Recommendation on protection of privacy

- obtained by lawful and fair means and with the knowledge or consent of the data subject
- relevant to the purposes for which they are to be used, and accurate, complete and up-to-date
- limited to the fulfillment of those purposes
- should not be disclosed for purposes other than those specified except:
  - (a) with the consent of the data subject; or
  - (b) by the authority of law.
- protected by reasonable security safeguards against loss or unauthorised access, or disclosure

OECD Document C(80)58(Final), October 1, 1980

European Union directives

- 15 member states, plus accession countries and copied elsewhere
- similar to OECD Guidelines
- 95/46 Data protection
- 02/58 Electronic communications
- tranposed into national law with variations

police and security services

- wire-tapping with a court order:
  - e.g., USA Communications Assistance for Law Enforcement Act (CALEA)
- retention of traffic data:
  - Cybercrime Convention of the Council of Europe
  - European Union 02/58 Article 13
  - definition and scope of data
  - duration of retention

additional data

- location:
  - time and place of an individual
  - can give patterns of movement
  - can be combined with
    - call data
    - locations of family and friends
- content:
  - what and when and where?
- payments and micro-payments

some parallels in bank and credit card data

INTUG fixed and mobile threats

- spam, spim, pop-up ads, etc
- viruses, trojan horses, worms, etc
- hacking and phishing
- identity theft
- mobile:
  - physical loss/theft of devices
  - snarfing (address book, photos, files)

systemic weaknesses,
not least people.

INTUG profiles

- used on fixed and mobile (e.g., login ID and cookies)
- mobile is more clearly a given individual through X.164 number
- can be linked to home address and socio-economic data
- also transaction data
- also location data
- also content data

INTUG location

- on a national network:
  - triangulation or GPS from device
  - used by operator or third party
- from a local network:
  - 2G/3G micro-cell
  - Wi-Fi, Infra-red, bluetooth, etc
  - RFID
- inferences from location and time

already concern over the use of GPS location data by car rental firms

INTUG the “threat” of RFID

- Radio Frequency IDentification tag
- very small and very cheap
- commonly on goods at pallet level
- increasingly on individual products
- already raised significant privacy fears
- how do you get the right balance?

INTUG international roaming

- in a different legal jurisdiction
  - are the rights/duties different?
- with a different operator(s)
  - are their policies different?
- potentially greater value of location based services when abroad
- severe legal problems for operators in complying with data protection legislation across borders

INTUG ENUM

- mapping E.164 number to multiple URIs
- heavily promoted
- but no security
- tried to map one person to one number:
  - a residence can have several residents, not all human (appliances, etc)
  - an individual can have several numbers
- functions can be delivered by SIP and instant messaging

INTUG multifunctional device

- phone
- personal digital assistant
- electronic purse
- camera
- identity document
- banking card
- music and games players

attempts at “wearable” telephones

INTUG cameraphones

- potentially concealed
- policies to exclude cameraphones for certain locations:
  - locker rooms
  - factories
  - R&D facilities
  - some offices
- some devices will make a camera noise

commercial communications

- immense volume of obviously illegitimate
- TACD survey shows a big discrepancy between senders' and recipients' views of what is legitimate
- new forms of communications:
  - SMS, MMS, etc
  - location based adverts
  - locally broadcast "neon" ads in cyberspace
- adverts may pay for/towards a service

INTUG risks

- how to strike the right balance for a given market?
- which market players have brand strength for security?
  - handset manufacturers
  - operators
  - third parties
- will bad communications drive out the good?

INTUG conclusions

- ubiquity of threats and risks
- but smaller and weaker devices
- added value in attacking a personal device
- a personal device reveals more
- human weakness with a “personal” device

INTUG issues

- how to maintain a balance that is:
  - reasonable
  - proportionate
- can we keep up with the hackers?
  - they innovate very rapidly
- can operators restrain the threat?
  - without harming competition
- can the law keep up?
  - legislators, police, judiciary, etc
- can it be controlled across several networks?

INTUG thank you

Ewan Sutherland
International Telecommunications Users Group
Reyerslaan 80
B-1030 Brussels
Belgium

+32.2.706.8255

ewan@intug.net
http://www.intug.net/ewan.html