

**Information, Intelligence &
Interoperability :**
the principle of availability and the problem of
biometricised security

Prof. Juliet Lodge

Director Jean Monnet European Centre of
Excellence, University of Leeds, UK

General remarks

- ICTs and i2015
- Subsidiarity
- ICT impact on administration
- ICT implications for accountable governance
- Three monkeys and an ostrich
- Specifics and dilemmas
- Scenarios

Europol & ICTs i2015

ICTs blur boundaries between public/private sectors inside m/s and across borders

Implications of 'availability' for Europol and cits

- outsourcing, data coupling, data mining, data tracking, digital footprints, nano-tech, data-reuse, re-sale, access (hard for cits - easy for m/s, commerce) fraud, **ownership – need defining**
- degradation, impact on cit IDs of ICT obsolescence, system integrity, standards etc)
- Discretionary disclosure (State security exception Art 8(6))
- **Europol access to centralised/IOP data bases in some m/s (with problems) and automated data exchange incompatibilities**

Impact on administration

IOP for speed and efficiency – must recognise

- Technology capabilities define agendas
(IOP – not YET there; bilat dominant +PLAs)
- B'crats more imp. in agenda setting
- Impact of info in data bases on d-m, esp in automatic info exch = Danger of (i)primacy of algorithms over analysis; (ii)tekkies over MPs – abuse of power

Blurring of admin boundaries – impact on accountability from local to supranat.

Impact on governance

- Commodification of info/intelligence
- Need standard common terms (eg biometrics)
- Implications of outsourcing, linkage & IOP
- citizen (mistrust) of govts and agencies unable to combat FRAUD
- Info trading for unclear purposes
- **Access by 3rd parties (public/private) MUST be REVIEWED in light of i2015 and securitisation**

3 monkeys & an ostrich

What public sees

- Surveillance society + growing insider fraud affecting personal and collective security
- Fraud + financial cost of weak IDs (epassport UK)+ID theft;biom role in authenticating IDs; biom theft; corruptn;
- Unbelievable claims making _ weak pol controls
- **LACK OF JOINED UP thinking re: inseparability of IOP for security and IOP for daily life**

Specifics & Dilemmas

1. **Operational need** for fed approach coupled with pol.reality of **primacy of m/s practice + vetos (art 19 on use of data)**
 - Incompatible with EU principle of equal treatment of citizens (art 31ff – variable rights and opps of data subjects; liability;redress art 48 & 51) Qn of inclusion ignored)
2. **Terminology**
3. **Financial burden of IOP** –set up, update, running, security (conflict of interest of commercial systems providers, buyers and users (law enforcement agencies) : (art9 = open ended budget) no stringent pol.oversight by NPs/EP
4. **Secrecy/confidentiality needs and impact** : need for uniformity NOT subsidiarity in EU; and issues re: 3rd parties/states/NGOs,INGOs

Problematic terminology

Variable interpretation and practice in m/s

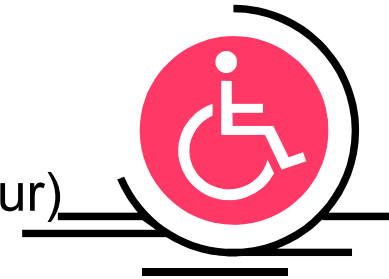
- **catch-all terms** (art 14(d)) 14(6) 'assoc expert'(and m/s 'veto' over who can be an AE in art 14#8(d))
- **Imprecision** (art 11(e) means biometrics why not say so?)
- **creeping securitisation** (Arts3-5)
- **Weak or absent time frames** (art7)(art 11(f) 13(2)**Art20!**)
- **'best practice'** (art10.5) no substitute for pol acct (10.3 – consultatn of EP/NP); reports at 'eg intervals'33#7
- Open standards (robustness ag. Hostile intrusion?)
- **IOP** (automatic data exch or PLAs)obsolescence
- 'preferred format' (art14(3) has financial implications
- Indexing and archiving (14#4(b))



Biometricised security



- Biometrics – measurement : iris,FP
- Biometrics – process/profiling:self
(associated info + data eg DNA, medical record +insur)
- Are you who you say you are?
- Use of biometrics by ‘unseen’ agencies
- Implications for policing & policy
- Agendas + Funding
- Political controls (principle of consent)
- IOP



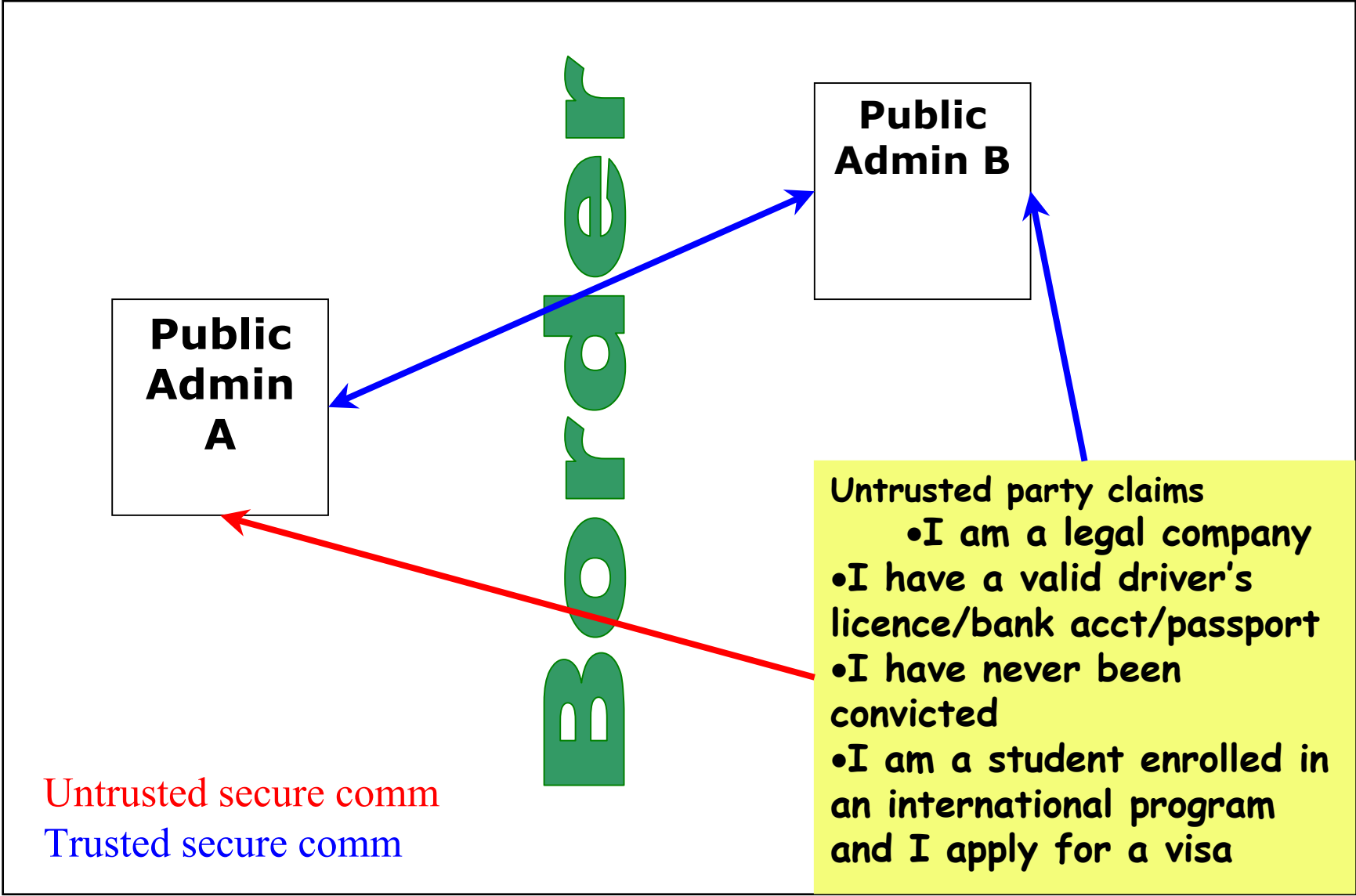
Public Admin
A

**Legal system and
National/European
regulations.
Subsidiarity principle**

Processing
systems and
procedures

Privacy policies
Data protection
ID theft & fraud

Security policies
and
architecture



Audit v. political vigilance & control

Art 16 Analysis Work Files audit logs give impression of robust oversight by Management Board

Implementation and access – contingent on m/s practice

Art 18 – info retrieval : need for

EDPS/EP role; Art 23 (outsourcing); data protectn(25)
Art 27 (compliance time consuming and no parl oversight)

Art28(2) ambiguous and likelihood of delay for pol.reasons poss.

Need for capacity building : tech, pol, operational, fin, data and ethics; definition of **Discretionary disclosure**

Art8(6) State security exception

Vigilance – duty of care by govt is not defined

Conclusions : politico-legal controls lag behind IOP



IOP – automated access and exch cannot be seen in vacuum NOR is it yet fit-for-purpose - IOP is a tool not an end in itself

IOP using poor quality biom.data taken by 3rd party (eg consular/visa post on planet Zog) compromises security all the way down the line

- Paradox – biometrics enhance ID verification but their indiscriminate deployment and outsourced handling and selling could compromise individual liberty and collective security

Accountability is not simply audit trail

Access by 3rd parties (public/private) MUST be REVIEWED in light of i2015 and securitisation

eGov and border management dissolves admin boundaries ; not neutral in impact on cits, gavs, policy

Can biometrics deliver security?

- Need stronger DP, EU law on ID theft as boundary between internal and external security is erased in practice;
- Need CONSISTENCY on TIGHT specifications on access rights and accountability; and on ID theft; standards, system integrity, reference architectures etc.
- Ambient intell. VoIP Info capture/exchange neglected
- An EU model for eGov info exch is needed
- Align existing and emergent Europol technical architecture eh Eurojust/Sirene/Frontex/Eurodac with an EU model for pan-EU gov
- EU principle of availability is contingent and automated data exch/IOP magnifies problem of TRUST in personnel, technology, corruptn

Recommendations



- IOP must be informed by political priorities that respect and enhance baked-in security (ie vendors' claimsmaking subject to independent test before purchase; and liability for ICT failure needs clarifying)
- EU principle of availability is contingent and contested and insider corruption and fraud in associated agencies for border management with Europol is an issue needing attention
- URGENT need for universal EU code on eGOV Need protocols for info sharing among parties (Common Intelligence framework – single database)?
- Need robust security architectures for using single contact pts between agencies, and even stronger ones in decentralised system which is more vulnerable
- Roles of NPs and EP vis-à-vis policymaking on 'IOP applications to security and border management in digi-space' need to be reinforced immediately

TRUST

‘Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it.’

Final report of the Convention on the Future of Europe
Working Group IX on Simplification 29 Nov 2002

[CONV 424/02 WGIX 13]