

European Parliament Committee on Civil Liberties, Justice and Home Affairs

PUBLIC HEARING
on
The Future of Europol

Brussels, 10 April 2007

Draft: may be cited with due acknowledged to source and permission of author.

Information, Intelligence and Inter-operability : the
principle of availability and the problem of
biometricised security

Prof Juliet Lodge

Jean Monnet European Centre of Excellence¹
Institute of Communication Studies
University of Leeds (UK)

Thank you for the invitation to this august meeting. It is a privilege and honour to be here to give some views on the implications of new technologies (ICTs) on Europol's role. The work of this Committee is vital for sustaining and realising an area of freedom, security and justice and for informing and shaping a debate about the contours of democratic accountability in a digi-age. Thank you M Cavada for allowing me to contribute some thoughts to your deliberations.

From a swift overview, you will see that there is some logic in suggesting that consideration be given to over-arching legislation in respect of egovernance and information and data sharing as territorial boundaries are increasingly irrelevant in digi-space and a future of enhanced nano and ambient technological capabilities.

I have prepared a powerpoint to display some of the articles in the *proposal for a Council Decision establishing the European Police Office*.

¹ My comments are in my personal capacity. They draw on some of my work conducted in the framework of f6p Challenge CITI-CT-2004-506255; and r4eGov IST-2004-026650.

Prof Juliet Lodge, Jean Monnet European Centre of Excellence, University of Leeds
LS2 9JT (UK) email: j.e.lodge@leeds.ac.uk; www.leeds.ac.uk/jmce; www.liberty-security.org

Introductory remarks

My focus is on issues relating to the automated exchange of information, rather than on institutional accountability, for example, through the Joint Supervisory Body, EDPS and European Parliament. However, open, visible parliamentary accountability and control should be exercised at all levels in relation to the implementation of the principle of availability under the Hague Programme : the European Parliament's role is too weak. 'Consultation', as provided for in the proposal, is insufficient. National parliaments' roles needs to be revisited and strengthened individually vis-à-vis their domestic law enforcement agencies *and all those other agencies who are and will be increasingly engaged in bilateral and, multilateral information exchange and intelligence exchange*. In addition, closer cooperation and information sharing between them and the European Parliament is desirable.

General Remarks

The proposal is a welcome recognition of the operational requirements for effective supranational action to realise an area of freedom, security and justice. Europol is becoming perhaps the visible tip of the iceberg. Many supranational and national agencies have a role to play in this. How they will share and exchange information with Europol raises many issues that are not specific to Europol but result from the realisation of the Information society itself. The proposal should be seen from the perspective of i2015.

The tendency to visualise information exchange purely as a function and operational requirement for law enforcement agencies working with Europol perpetuates the artificial and unsustainable boundaries between 'internal' and 'external' security. This and the implementation of the principle of availability is problematic for law enforcement agencies (not just Europol) and for citizens. It is especially problematic when tied to automatic information sharing and exchange.

The known risks of inefficient and imperfect information sharing and exchanges on a bilateral basis in paper-based systems will not disappear by having automated information exchange. Inter-operable systems are in their infancy. High standards that Europol and Eurojust may devise need to be higher and set the gold standard.

Effective action by the law enforcement agencies relies on current bilateral agreements, bilateral trust and bilateral cooperation. Effective 'inter-operability' does too but implies a higher degree of automated mutual access to centralised data bases (such as SISII, Eurodac, etc) and to those in the member states.

Technical issues underlying information files and automatic processing

Baked-in security and implementation of high data protection provisions are essential. The political reality is based on reliance on subsidiarity and mutual recognition but the effect is variable safeguards for citizens and all concerned. This is unsatisfactory. Citizens are not equal in EU territorial or digi-space. There is not a common definition of understanding of basic terms like 'information' and 'intelligence'. The distinctions and ambiguities could prove problematic in decisions determining their exchange and automated access to them. Intelligence normally includes viewpoints

(even hearsay, hunches, observations of behaviour) derived from an evaluation of diverse information sources : this implies a need for data mining. The constituent parts of 'intelligence' may be held in formats and databases that do respect principles of data minimisation and purpose limitation that are now being used for different purposes. Civil registration documents, for instance, may vary considerably from state to state in the information they contain and which, in theory, could be exchanged, shared or interrogated by Europol and/or other law and border enforcement agencies.

Whereas the proposal for a Council Decision (COM(2006)0817) is about Europol, many of my remarks are relevant to ICT enabled data, information and intelligence sharing in general. Europol is possibly subject to stricter oversight than many other law and border enforcement agencies.

Different understandings of common terms (eg criminality, organised crime, serious (Art4.2) criminal offences (Art 4.3) crime, criminal justice) in the member states have serious consequences as to how information and intelligence (which are not the same things) are managed, processed, communicated and subject to exchange and sharing with other public *and* private or semi-private agencies within the state and across borders, and in and with third states. This includes, for examples, consulates regarding visas and, under the envisaged common consular space, evisas and enrolment of biometric data such as fingerprints.

Vested interests in creating the ICT systems that facilitate automatic information storage, retrieval, exchange, sharing and so on make claims needing careful, independent scrutiny. If individual security is not necessarily enhanced by them, is collective security also at risk?

Subsidiarity (exemplified in for instance PLAs) underpins the realisation of the area of freedom, security and justice. That is a strength but operationally potentially risky if the opportunity is not taken now to inject greater precision into Decisions that will become reference points and shape the future both for management of information sharing and exchange among such agencies as Europol and Frontex, Sirene, VIS and SIS II.

Why is there seemingly no recognition of the potential of nano-technology, RFID and ambient intelligence work of the Commission's strategy on the Information Society?

Who operates the ICT systems outside the controlled environments of Europol and, for example, Eurojust? How are systems selected and funded (this will be a growing drain on the EU budget and matter for the European Parliament as part of the Budgetary Authority (art 9 financial burden of IOP - open-ended budget, and financial consequences of the 'preferred format' (Art 14(3), and indexing and archiving (Art 14.4(b)?)) How are data inputters screened at local through to supranational levels and in all those third state agencies with whom data exchange is envisaged? How strong is ID management and authentication?

What rules cover system obsolescence, out-sourcing, data coupling, data mining and tracking, digi-footprints, data storage and deletion (eg of DNA), data re-use, access

(hard for citizens, relatively easy for member state agencies, commerce) insider and outsider fraud, corruption, data ownership, degradation, the updating of communication protocols? How are different categories of data subject defined?

Invisible implications of automated information exchange

There is little doubt that genuine inter-operability will boost the speedy response needed to enhance effectiveness. That is operationally necessary. At all levels, however, over-reliance on technology means that technological capabilities (that vary greatly among EU27) define agendas in ways which allow bureaucrats greater input than elected politicians and heightens the known tendencies of groupthink. The blurring of administrative boundaries impacts on accountability at all levels. This needs addressing : controls on Europol may be tighter than on other levels and encourage reliance on 'softer' bilateral channels.

Politico-legal controls lag behind IOP capabilities across the board. The EDPS' vigilance and recommendations are instructive and vital.

Liability for ICT failure needs clarifying.

Invisible impact on governance :three monkeys and an ostrich

Automated information sharing and exchange leads to the creation of 'new information' files and intelligence. ICTs commodify data. Outsourcing to third states and parties, growing fraud (all too close and visible to the citizen), information trading for unclear purposes without the direct consent of the data subject are generally problematic but especially sensitive in the FSJ field. Linkage of data bases within states (eg welfare with health, education, tax, vehicle licensing, motor insurance, eIDs and epassports) has to be considered. Law enforcement information and intelligence derives from many sources (not necessarily universally shared or trusted, that may skew or claim ownership over them). Who, for example, 'owns' the data in new Work Files, including the new data products of 'intelligence'.

Access by public and private third parties must be reviewed in the light of i2015 and securitisation of hitherto 'domestic' areas.

The public hears unbelievable claimsmaking, sees weak political controls, rising ICT enabled fraud, escalating costs for weak eIDs (such as epassport failures and incursions), and doubts that its reservations are taken into consideration by governments. Individual redress against misuse of data is cumbersome, protracted, costly and difficult.(art 31bis; 48, 51) Clusters of citizens (such as handicapped) are not included but are subject to processes (biometric enrolment) and information exchange over which they cannot make informed decisions, or realistically make amendments to errors.

The lack of joined up thinking as to the inseparability of IOP for security and IOP for daily life needs to be addressed if distrust is to be overcome. There is a need to convince practitioners and the public alike about the security of ICTs; to convince

them that ICT applications are not a threat to their identities, personal or collective security; that costly big system failure and critical infrastructure incursions will not compromise their ability to prove who they are; and that their interests can genuinely be protected by political authorities. IOP is in its infancy and it is unhelpful for exaggerated claims to be made.

The ostrich-like approach of allowing others decide how IOP will work in practice technically risks allowing others to present what is available as the 'solution' instead of creating what is needed. Specificity and clarity are essential. Reliance on mutual recognition is tempting but ducks the need for uniformity, especially in defining terms like secrecy, confidentiality, rights of access.

Accountability is not just an audit trail. Best practice (art 10.5) and audits as provided for in the Decision (Art16, 18) are essential preconditions for data protection (Art 23-27) to effectiveness and accountability but are not substitutes for political accountability (10.3). 'Consultation' of the European Parliament needs reinforcing. Reports at 'intervals' (Art 33.7) could be complemented by real parliamentary oversight both of Europol *and* of national practice. *The duty of care and vigilance of government (outside the sphere of state security exceptions (Art8(6)) needs re-visiting.*

Problematic terminology

Variable interpretation and practice will impact on catch-all terms used in the Decision.

By way of illustration see 'associated expert' (art 14(d) !4.6) and member states' veto right over who can be one (Art 14.8(d)); creeping securitisation implicit in Arts3-5; weak of absent time frames allowing too much discretionary interpretation (arts 7,11(f), 13(2), 20) and ambiguity increases the potential for delays to be politically engineered (Art 28(2)).

Information and intelligence mean different things. A common intelligence framework may imply a need for a single database. How could the Decision reflect the need to align Europol's existing and emergent technical architectures with other relevant ones?

Biometricised security

Without clarity over the terminology used in the Decision, difficulties will arise. For example: the EU generally understands 'biometric' as a measure of a stable, physical trait (eg iris, fingerprint). Other states, subsume under 'biometrics' behavioural characteristics and associated 'information' (social activities, DNA, medical records, banking, gait, voice VoIP etc) that EU states associate with 'profiling'. The PNR issue and legislation on hooliganism are illuminating.

Current definitional looseness allows for ambiguity and expansion in ways that may be unintended and difficult to make subject to visible, political accountability. Public concern over the perceived risk of identity theft and the use of biometrics and

associated information by ‘unseen’ criminals and private or public agencies has repercussions on policing and policy.

IOP using poor quality data taken by third parties (eg visa posts on planet Zog) potentially compromises security all down the line. While biometrics may enhance identity verification their indiscriminate deployment and outsourced handing and sale may compromise individual liberty and collective security. There is a public duty to ensure that the systems envisaged for say Europol-Eurojust are genuinely models of public systems that are as robust-against-fraud from data collection to inputting, access, storage and retrieval as possible.

Conclusions

Automated access, information exchange and intelligence sharing, and IOP cannot be seen in a vacuum. The assumptions as to what the technology can deliver now are exaggerated. ICTs are probably as yet not quite fit-for-purpose (even allowing for respect for ethical principles, data minimisation, purpose limitation, and so on).

The principle of availability is contingent.

Automated data sharing, access and exchange magnify the problem of trust in private and public sector personnel, technology, administrators, officers, and politicians both inside the EU and where third parties in third states or NGOs and international organisations are concerned. Communication to and from third parties and non-EU interests needs to be rigorously examined. The mere existence of rules or laws in third states or agencies is but one prerequisite to consider allow information sharing : it is not a sufficient condition in itself. It would be foolhardy to allow a ‘tick box’ approach to verifying the ‘adequacy’ (however that term is defined) or otherwise of , for instance, robust data protection.

IOP is not an end in itself. It is a tool of egovernance. It is not neutral in its impact. It must be informed by political priorities.

There is a need for consistency and tight specifications on access rights, standards, system integrity, reference architectures, etc.

There is an urgent need for an EU law on ID theft. This could be considered complementary to or a part of the Decision.

The Decision needs to show awareness on the implications of ambient intelligence.

The tasks given to Europol associated with assisting in combating crime and border management highlight dissolving administrative boundaries. This demands attention to how good governance and procedures introduced by this Decision may provide a model for and shape practice within the member states.

The Decision highlights the need for a cross-pillar, universalised EU model on information exchange is needed.

Trust is at the heart of effective information exchange and communication whether enabled by ICTs or mediated by humans. The EU Constitution's provisions on FSJ and Europol are illuminating.

The Convention said: 'Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it'.

Thank you for listening.