Info, Comm & Ethics in Society (2006) 3: 131-144

NOTES FOR AUTHOR:
1. YOU ONLY MARK UP THE FIRST FOOTNOTE IN THE TEXT. PLEASE INDICATE WHERE THE FOOTNOTE NUMBERS 2-5 SHOULD GO
2. HAVE YOU MENTIONED ALL THE REFERENCES IN THE TEXT? PLEASE ENSURE THAT ALL REFERENCES ARE MENTIOEND IN THE TEXT AND THAT THE DATE FOLLOWS (IE., SMITH, 2003).

Ethical EU eJustice: elusive of illusionary?

Juliet Lodge
Jean Monet European Centre of Excellence, Inst. of Communication Studies, University of Leeds, Leeds
Email: j.e.lodge@leeds.ac.uk

eJudicial cooperation is a goal of EU policy. It appears to offer procedural and technical ICT solutions to enhancing EU security. This paper outlines particular dilemmas posed by operationalising ejudicial cooperation within the EU and its member states, and assesses how political weakness is reconfigured as a problem of technical ethics. The application of biometrics and ICT based ejustice potentially bring the EU closer to the citizen without closing the confidence and trust deficit. The paper first outlines three political dilemmas of ejudicial cooperation: political competence, public accountability, and globalisation imperatives. It examines the rationale for introducing biometric IDs, highlighting a general problem of ejudicial cooperation and egovernance which aggravate the trust deficit. Then, it assesses the technical and managerial procedures to ethical practices for quality justice and security to combat the trust deficits which elude open public accountability and compromise trust.

Keywords: biometrics, judicial cooperation, trust, accountability

INTRODUCTION

EU institutions and member governments are committed to realising judicial cooperation as part of a strategy to guarantee and sustain security in the EU: the freedom, security and justice agenda. The three elements clash both in terms of their prioritisation, their mutual compatibility and their feasibility. The phrase judicial cooperation evokes ideals of value-free, neutral cooperation designed to produce justice. It is supposed to be a public good. Yet judicial cooperation in practice is anything but neutral: it is a political minefield. While the EU goals of pillar III – promoting sustainable freedom, security and justice – enjoy broad public support, why do the implementing measures and objectives to improve security appear to produce opposite effects to those intended? Why does ejudicial cooperation in particular aggravate suspicion that the end-product will be anything but 'just' and fair? Is eJustice a chimera in the making and ejudicial cooperation elusive?

Judicial cooperation (a term used as shorthand to embrace cooperation among all the agencies involved in combating crime, including legal, customs, immigration and police agencies) exemplifies the clashes and dilemmas central to egovernance in general, epitomises the difficulties in claims-making regarding making judicial cooperation in practice acceptable to an increasingly distrustful citizenry, and highlights the urgent need to combat the public diplomacy failure on liberty and security at a time when ICT applications bring the EU ever-closer to the citizen while simultaneously aggravating the trust deficit. Is this especially problematic in respect of judicial cooperation because government

claims that introducing biometric documents will enhance security fuel the trust deficit and scepticism over the reliability of the technology, and the robustness of government controls? This paper outlines problems over facilitating e-judicial cooperation in the EU. It examines tensions arising from political failures between the supranational, national and local levels in implementing the technical tools of ejudicial cooperation. If judicial cooperation widens the existing trust deficit, could EU eJustice be a contradiction in terms, elusive and illusionary?

The paper first outlines the background to the problem by examining three political dilemmas of ejudicial cooperation: political competence, public accountability, and the globalisation imperative. It then examines the rationale for introducing biometrics and shows how this one tool highlights a general problem of ejudicial cooperation and egovernance which aggravate the trust deficit. Finally, it assesses the technical and managerial approach to combating the trust deficits through the adoption of ethical practices to fashion quality justice.

Political dilemmas: competence, accountability and globalisation

Cross-frontier judicial cooperation to combat organised crime is the most sensitive area to which governments and the EU Commission routinely allude in order to justify the introduction of biometric, digitised identity documents (IDs) that they claim are essential aids to enhancing EU security. Public and private agency advocates of the technology argue that the collection and storage of biometric identifiers (i) augments collective and individual security, (ii) enhances the quality of justice, (iii) boosts the efficiency and quality of law enforcement agencies; and (d) intensifies confidence and trust in government. The problem is that technology and political trust are out of kilter owing to both the imperative of globalisation and the techniques of giving effect to judicial cooperation in practice. To realise ejudicial cooperation, cultures, law enforcement processes and procedures associated with uncovering, preventing, prosecuting, tracking and penalising crime have to be unpicked to make them comprehensible and susceptible to being captured in ICTs processes, whether open or not.

The idea of EU member states cooperating in a sphere where national sovereignty has been jealously guarded poses major questions of jurisdictional competence. Cooperation (as opposed to the infinitely more threatening concept of integration) in judicial affairs compromises national sovereignty. Action here is subject to intergovernmental requirements that escape supranational parliamentary control and maximize national governments' discretion. The powers of the Commission and the European Parliament are limited. The European Parliament is excluded from co-decision with the Council. Supranational and national parliamentary accountability is weak, illusionary or elusive. The stalling of the draft Constitutional Treaty, which would have rectified this, means that the question of the ultimate locus of political authority and accountability in judicial cooperation has been ducked. Consequently, there is public suspicion that: ejudicial cooperation instruments and agencies escape appropriate democratic controls; that a proportionate raft of measures (Rowland, 2004) is rapidly being replaced by politically expedient goals; that the principle of 'availability' will enable agencies to evade political oversight; and that as a result procedures and practices will arise that compromise civil liberties and sustainable democracy, freedom, security and justice.

Competence and Accountability

Article 65 of the Treaty of Amsterdam transferred judicial cooperation in civil matters from pillar III to pillar one subject to the requirement of it being necessary for the proper functioning of the internal market. To create a single judicial area, it promoted measures to improve and simplify the cross-border service of judicial and extra-judicial acts; the taking of evidence; the recognition and enforcement of decisions in civil and commercial cases (the Brussels 1 Regulation) and practice guides for the application of regulations, such as the Brussels II Regulation. Central to this is not a process of communitisation or harmonization of national rules but information exchange, mutual recognition and accommodation to create a European judicial culture, for example via the European Judicial Network and Eurojust that enable practitioner information seeking and exchange about national laws. By contrast, intelligence exchange, exemplified by judicial cooperation among law enforcement agencies including Europol on criminal matters (of which terrorism is but one) is of a different nature. It concerns data that has been collected, possibly partially analysed and is designed to be used primarily for operational purposes in combating crime at the most local of levels.

EU member governments are committed to the Hague programme's key aims to sustain the area of freedom, security and justice based on existing

treaty provisions, the Europol convention, the internal security acquis and soft law measures. To implement facilitating measures pending ratification of the Constitutional Treaty, the Hague multi-annual programme envisages preparatory steps guided by the general principles of 'subsidiarity, proportionality, solidarity and respect for the different legal systems and traditions of the member states.' (Point II.1) These translate at the functional, operational level of practical judicial cooperation as the principles of availability, proportionality, fitness-for-purpose, and mutual trust. The inherently complicating factors of political accountability are dodged. The risk is that as the functionality of ejudicial cooperation progressively escapes the territorial borders of states, so governments and the EU will find themselves unable to regulate them. This creeping emasculation of the authority and ability of government bodies to safeguard citizens' interests denudes them of authority, respect, credibility and legitimacy.

The EU's dilemma is to reconcile legitimate operational needs for enhancing EU member states' abilities together to combat organised crime with equally legitimate institutional and civil society requirements to maximise openness, transparency and democratic accountability. The mainstreaming of 'security' across EU policy domains, not always subject to co-decision, means that democratic accountability and legitimacy norms and values are challenged by the attainment of functionally specific goals. Simultaneously, contradictory messages are communicated to the public even though the Hague programme commits the EU to 'open, transparent and regular dialogue with representative associations and civil society…citizens' participation in public life'. EU Commissioner Frattini's agenda is to bring justice closer to the citizen by capitalising on the EU's commitment to the creation of a knowledge society.

The globalisation imperative

The Lisbon strategy commits a 'greying' EU to becoming a globally competitive economy and to taking precautions against security threats. Setting or keeping pace with the globalisation imperative and standards is likely to give major ICT suppliers more than a competitive edge. The greater their market share and the more the demand for interoperable or at a minimum compatible systems in different agencies and member states, the more likely it is that they will secure a market dominance with serious implications for the conduct of public life and politics. Leaders are not necessarily 'European' players.

Globalisation poses an acute politico-ethical challenge for judicial cooperation because to be commercially viable technical advances must be based on the premise of inter-operability, and 'killer', full network citizen cards. Creating and applying inter-operable systems in private and public domains raises major problems of trust relating to: confidence in the robustness of the technology to withstand hacking, fraud and identity theft; and trust in the ability of government to control those in charge of the technology and to deliver the personal security that government agencies claim follow from embracing the technology. As Jean-Marie Cavada, chairman of the EP committee on Civil Liberties, Justice and Home Affairs argues: 'There is inevitably a conflict between freedom of the individual and measures taken by the government in order to protect civil society. It is essential to find a balance between the two.' But his claim that citizens control the State is at variance with globalisation and the Europeanisation of ejudicial cooperation.

Judicial cooperation is supposed to enhance the procedures for applying the law in order to sustain security. ICT measures compromise individual liberty and privacy in ways that are deeply uncomfortable to citizens in some member states. e-judicial cooperation underlines the tension between and mutual dependence of individual and public privacy. Digitised and possibly commodified individual identities occasion privacy problems in digitised cyberspace that differ from those in territorial, physical space and challenge the claim that more ICTs identifiers will enhance security. Political ambiguity, obscure accountability and opacity rather than transparency need to be addressed. The application of ICTs is not neutral: structures of power are embedded in their deployment in the judicial sphere. Ultimately, they are contingent on the socio-political context that informs political choice.

The application of ICTs together with biometric identity authentication and verification systems under both pillar III and increasingly securitised domestic areas of socio-economic and welfare activity closest to the citizen challenges raises questions about the robustness of existing democratic institutions; the technical systems themselves; the relationship of presumed trust between the citizen and the state; and the appropriateness of territorially based institutions of political accountability to control and protect democratically and openly citizens within their borders whose personal integrity, once digitised and stored, becomes subject to the market forces of agencies outside the control and

the borders of those agents. The basic contract between the state and citizen, which formed the basis for contemporary understandings of sovereignty, are therefore eroded and require rethinking. The problem for policymakers is that the public is not convinced that judicial cooperation benefits the public good sufficiently to justify pervasive deployment of ICTs – e-justice – by faceless, possibly private and commercial, interests and cyborgs (Introna's autonomous constructed realities) able to evade public political accountability. Central to this is the issue of trust. Surprisingly, whereas trust has been recognised as the most important element of successful e-commerce (Kracher et.al, 2005), it is only beginning to be addressed in the context of e-judicial cooperation. Consequently, many different aspects of delivering ejustice become muddied by a focus on civil liberties and human rights discourse.

Biopolitical dilemma

Paradoxically, ICTs in the service of ejudicial cooperation or esecurity bring the EU closer to the citizen than ever before. Tangible examples of EU identity – passports, identity cards, health cards all embellished with EU logos, for example, sit in citizens' pockets with domestic smart ecards etc. Those elements where the citizen is in charge of obtaining e-services and divulging limited information do not raise as much concern as those which the citizen associates with covert surveillance. Remote, unseen, automatic inter-operable exchanges of information fall into this category.

The sufficiency of political and ethical standards in the practice of ejudicial cooperation in an EU *sans frontieres* is challenged by the adoption of biometric identifiers and the principle of 'availability'. Both raise serious concerns about inter-operability. This is the cryptic internal agenda of enabing judicial cooperation: information exchange is operationally valuable if it is feasible and mandatorily incumbent on relevant agencies to participate, to disclose and give unconditional access to information they hold to their counterparts. Governments have therefore agreed to implement a new principle of 'availability'. Crudely, this means that if the information exists in the data bases of a law agency in one jurisdiction it should be made available for specified and legitimate law enforcement purposes to another in another member state (2). Article 1.2 (TEU) states: 'Member States shall ensure that the disclosure of personal data to the competent authorities of another Member State is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for under this Framework Decision.'

Stakeholders claim that biometric identifiers – from single fingerprints to DNA chains – offer a reliable means to identify, verify, validate and authenticate the unique identity of individuals (for civil or criminal purposes) even accepting the possibility of false positives and data degradation (Fairweather & Rogerson, 2003). Biometrics are being introduced against a background of counter-terrorism and immigration control. Threats to territorial integrity are to be combated by cyber-border controls. Following the July 2005 London terrorist bombings an Extraordinary meeting of the JHA Council agreed to expedite measures on retaining telecommunications data, the European evidence arrest warrant, terrorist financing, the third money laundering directive, and improving information sharing on lost and stolen explosives. It further agreed to:- expedite enhanced interaction between the Visa Information System, (VIS) SIS II and EURODAC, and the proposal for law enforcement access to the VIS by November 2005; visa information sharing via VIS, including biometrics for visa applicants under VIS to regions/countries of high risk; and arrangements to share information, ensure coordination and enable collective decisionmaking in an emergency, particularly for terrorist attacks on more than one member state.

States have been introducing voluntary or mandatory biometric identity cards having different features and rules. For example, they are mandatory in Estonia but not in Sweden, and even when mandatory, penalties for non-compliance are vague on non-existent. The question to be resolved is one of securing their adoption voluntarily when governments wanted them to be universal requirements. On July 11 2005, the UK Presidency proposed requiring all ID cards in the EU to have biometrics, including fingerprints. EU competence does not cover harmonisation of ID cards. Article 18 of the Nice Treaty excludes provisions on passports, identity cards, residence permits or any other such documents. This had already caused problems in December 2004 when under the consultation procedure the Council had adopted a regulation on mandatory facial images and fingerprints in EU passports. Article 18.2, however, provides for Council action in line with Article 251 (co-decision) when action is needed and the Treaty has not provided the necessary powers. Following this an article 6 committee was set up by the Commission (excluding Ireland, Denmark and the UK) and its remit has expanded progressively from visas to passports and now to biometric identity cards. Biometrics bring the management of information exchange, technical and ethical dimensions to ejudicial cooperation into sharp relief.

Sharing information: availability and the inter-operability

Inter-operability, mutual access to nationally-held data, and e-data exchange are envisaged. New centralised European databases may be endorsed if they add-value. All member states have to focus on the security of the Union per se rather than just their own national preoccupations. Accordingly, intelligence and security service cooperation is envisaged along with the creation of conformity norms and practices. This ties in with integrating biometric identifiers into travel documents, visas, residence permits and information systems, including national identity cards (which may or may not be linked to inter-operable databases as proposed by the UK), the establishment of a European External Action service and Common consular (diplomatic) corps. These are all instruments of the Hague Programme's 'continuum of security measures' from visas to the prevention and control of crime, and terrorism using 'a coherent approach and harmonised solution' in the EU on biometric identifiers, data and interoperability between SIS II, VIS and Eurodac.

From 1 January 2008 law enforcement officers are to make information available across borders subject to the conditions that: data may be exchanged only to allow legal tasks to be performed; data integrity must be guaranteed; sources of information must be protected; data confidentiality at all stages of and after the exchange must be assured; common standards for access to the data and common technical standards must be applied; supervision of respect for data protection must be ensured; individuals must be protected from abuse of data and have the right to seek correction of incorrect data.

The Hague programme foresees the Commission taking the initiative on defining powers and funding (by the end of 2006) technical and operational assistance to member states within the framework of the Border Management Agency; supplementing Schengen (where lines of political responsibility are virtually impossible to discern) (Wagner, 1998) with a supervisory mechanism; and examining the conversion of national teams of experts into a European corps of border guards. The sensitive problems of operationalising ejudicial cooperation surface in the associated instruments.

The ethical dilemma

The ethical issues posed by judicial cooperation are generally couched in the political terms of civil rights, and the right of the individual to know and consent to personal information being given, shared or transacted. Legislation to cover this, and civil liberty vigilance, represent a macro-level response. At the micro-level of the individual, less attention has been paid to the ethical question of eliciting personal and biometric data from people unable to check data reliability or give informed consent providing biometric identifiers such as reliable finger prints and/or iris scans – such as babies, socially excluded the mentally and physically disabled. The UK Government acknowledges problems of false identification with people having roughened finger tips; dark brown eyes; or pictures taken in the 'wrong' light, and advocates using up to 13 biometrics.

At the local level of the agencies and practitioners applying ejustice tools in exchanging information via ICTs, there is a further trust deficit both as far as the public is concerned and in respect of mutual professional inter- and intra agency suspicion. Characteristic traits of knowledge-based trust, identification-based trust and deterrence-based trust - integrity, loyalty, consistency, openness, reliability, the alignment of interests and fairness – are minimal. eJustice is especially risky given the specific contextual need for swift trust in networks of law enforcement agencies, and the high risk arena of security within which these have to operate. This can be conceptualised as having and internal inter and intra agency dimension, and an external dimension related to building public trust and confidence in the absence of supranational institutional requirements to make internal security policies and their associated soft law instruments subject to open, effective parliamentary accountability.

The application of ICTs is almost always portrayed as benign: medical data record sharing is supposed to accelerate appropriate diagnosis and treatment (Kramer & Tyler, 1996). The politico-legal consequences of malicious interference with data, unauthorised transfer, entry errors, etc are known but insufficiently addressed. Medical codes cover some of the appropriate issues to be covered in codes of practice, but are too narrow and antiquated for judicial cooperation. Both generally prescribe confidentiality; common standards for access to the data; data protection; data minimisation; respect for the precautionary principle; and protection for individuals and the right to seek correction of incorrect data (Spinelli & Tavani, 2004). However, back-door biometric function and mission creep are probable and likely to challenge concepts of ethical and appropriate conduct.

Ethics as Codes of practice: management dilemmas

Biometrics as a tool of managing ejudicial cooperation highlights the structural inadequacies and the

risks of inter-operability without sufficient politico-legal and ethical safeguards. That is why there has to be vigilance as to the meaning and application of the principles of availability, subsidiarity, solidarity, proportionality and fitness-for-purpose. At the meso-level of operating procedures within organisations practising judicial cooperation, the ethical issue has been reconfigured as a problem of quality. Why?

First, judicial and law enforcement agencies communicating across boundaries within and across states structure processes of interaction, embed technology in processes of problem formulation and problem solving, frame agency relationships and create technological power geometries. The question of who holds legal title to databases is often obscure. Obscurity inhibits democratic practice since open democratic accountability ceases to be an obligation. ICTs are being applied to judicial cooperation at an accelerating rate with little regard to rectifying the underlying democratic confidence and trust deficits. As a result, political ambiguity is compounded and the objectives and means of judicial cooperation rendered less transparent at a time when public concern over fraud and forgery of biometric identifiers is growing.

Second, at the supranational level, because judicial cooperation is not subject to strong parliamentary accountability with its concomitant transparency and openness requirements, EU rules on transparency are framed in a technical, procedural rather than political way. Thus focus to slips to obscure intra and inter-agency information exchange, and the ways by which the public can gain access to documents processed by them. Without a transparent political culture of disclosure and communication, the democratic precept of open government is spun into technical 'workflows' for managing aspects of procedures that are about accessibility of information rather than practices of democratic accountability. The access and workflow approach domesticates and internalises what should be an external public demonstration of openness.

Third, significant discrepancies in national political cultures make the supranational principles of transparency, equality and justice ever more contingent because uncharted degrees of discretion are permitted within the various law enforcement agencies on the grounds of the need to serve 'the public interest'. Such contingency endangers public trust and aggravates democratic legitimacy deficits notably when it shifts from institutional non-disclosure to technical arguments. For example, non-disclosure can be rationalised as in the public interest in the event that security-critical information infrastructure software proves vulnerable (Takanen *et al,* 2004). The problem is that public and individual non-disclosure pose numerous problems related to the issue of who controls whom and how; and how and by whom digitised identities about real individuals can be disclosed without the latter's knowledge to invisible, autonomous agencies – the 'cyberocracy'. This concern is compounded inside law enforcement agencies and across incipient networks of e-judicial cooperation where ICT use and processes of automatic disclosure create new political dilemmas about legitimate activity and cooperation.

Deep distrust persists among and between the various agencies from police to customs and immigration, legal and law enforcement agencies within the EU. Discrepant, contradictory, insecure and corrupt practices are widespread, especially among similar agencies in applicant states. (Montanaro-Jankowski & MacMahon, 2005) These undermine agency trust in the desirability of information exchange, of any sort, and compromise incipient confidence and trust among practitioners and especially among publics not persuaded by the security-exceptions rhetoric of law enforcement and political authorities. The demise of the Constitutional treaty, which would have brought the whole area under one pillar, means that operationally determined priorities expedite police and judicial cooperation under different rules subject to minimal political accountability. A small number of member states exchange sensitive police data outside the EU framework under the May 2005 Prüm Convention (commonly called 'Schengen III') (2) (Guild & Carerra, 2005). Signed on 27 May 2005 by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria, it steps up cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. On a self-regulating basis, police autonomously exchange information, and usually without recourse to judicial authorization. This technical approach exacerbates the dangers of persistent political ambiguity, and weak legitimacy. It diverts attention from elusive political accountability to internal methods of verifying who accesses what pieces of information. It neglects the political risks of both institutional and technical failure.

Risks of failure?

Judicial cooperation is not risk-free. First, apart from the aforementioned political risks in aggravating risks to the presumed relationship of trust between the citizen and the state, ICT and stake-

holder risks arise from EU member states and others using by default procedures developed by competitors that lack the ethically and technically robust management systems that citizens find essential where sensitive public service applications are concerned.

Second, big IT projects are more likely to fail than small ones. Big government projects, especially inter-operable ones within and across states, involve thousands of new processes that have to be amended as legislation, instruments and tools change (3). Mission creep and new policy demands (Dunleavy & Margetts, 2002) create additional arenas for failure as software is updated to cope with new data entry work. Unpredictable interactions are likely both from the perspective of the technology, the accuracy, professionalism and training of data inputters, the overall security of the systems and expertise in managing the projects.

Third, complex projects cutting across several agencies, as ejudicial cooperation demands, place particular demands and constraints on leadership – both within the organizations and across it. Political management, negotiating skills, and ultimately appropriate channels of political accountability have to be clear. Indeed, keeping IT skills in-house may well be a more effective way of managing big IT applications than transferring the work to contractors under competitive tender.

Fourth, the absence of candid communication of political goals and methods is risky. It is unwise to assume that it is safe to postpone justifying to the public the potential inter-operable applications of ICTs to egovernance while bits are introduced piecemeal. This disingenuous approach can be exploited by those with a hostile agenda: judicial cooperation is especially vulnerable given the associations of ICT applications and biometrics with Big Brother, and possibly an alien Big Brother. Technically, this makes even more pressing the need to develop a European gold standard for ejudicial cooperation (and egovernance) complete with a technically robust EU standard as a technical and politico-ethical model for global application. Politically, it behoves the EU to re-visit accountability.

Fifth, inadequate parliamentary accountability underscores the need for additional means susceptible to rigorous and more immediate scrutiny, audit, monitoring and investigation. The temptation is to focus on voluntary codes of practice to disguise or circumvent the serious political failure in ensuring sufficient parliamentary accountability. The EU needs detailed (rather than draconian) legislative measures to create sufficient safeguards to protect individuals and to ensure that judicial cooperation unfurls responsibly within and across law enforcement agencies. This can take two key forms: (i) external and visible to the public in the shape of data protection officers; and (ii) internal to the agencies themselves, under the mantle of quality justice.

At the external level, the appointment of data protection officers alone is insufficient: their remits differ across policy areas and states. At the internal level, the scope for discrepancies is wide. Mutual suspicion among law enforcement bodies within and outside the member states are probably aggravated rather than alleviated by the possibilities offered by the application of ICTs to cross-border judicial cooperation. Judicial cooperation requires mutual understanding, flexible systems, locally enforceable procedures, secure methods of tracking and tracing online actions (and auditing them), and ensuring that the procedures and practices comply with local (domestic national and EU level) legislative requirements. Accountability can be practised at different levels. Hierarchical lines of accountability and checks and balances can be set up among, for instance, judges, lawyers, police and prosecutors. At the operational level, inter-agency accountability can be based on rolling programmes of peer reviews, and in the case of EU level agencies those undertaken by the heads of Europol national units to review member states' capacity to combat serious organised crime.

Accountability as ethical codes of practice

Institutional structures of power relationships among and within political and judicial agencies, diverse political cultures and bureaucratic practices of administering justice, and law enforcement agencies' cultures of combating crime are opaque and inconsistent. Judicial cooperation and democracy implicitly assumes the existence of a homogeneous judicial web which is at variance with reality. A judicial public sphere exists neither in cyberspace nor within the EU. The security imperative places operational needs that enhance and depend on judicial cooperation among law enforcement agencies above political desiderata of democratic accountability. The idea that these agencies should be responsible to political masters is not entirely lost however. Instead, it is reframed in terms of the adoption of ICTs, and of management procedures: delivering quality justice and quality security using ICTs.

Accountability as technical failure

Technical problems mask a plethora of residual concerns about the sanctity of the sovereign rights of national jurisdictions – and more importantly, their different interpretation and application by different agencies within the member states; flawed data handling and storage practices; and differences between even those states who have signed and ratified relevant Council of Europe Conventions. At a technical level this leads to (a) a focus on digital rights management regimes and multi-signature requirements to support the management of intellectual property rights for digital resources; and (b) robust management systems to inhibit illicit transactions. This is not just about rights and obligations, trading, protection, tracking and tracing transactions. It is about secure authentication and authorisation systems that can be used in a context of mutual trust by those sharing a common goal: secure judicial cooperation for security. It is about creating applicable, simple technologies that protect ownership and control over privacy while fostering secure ejudicial transactions (Mason & Raab, 2002). Just as in politics, key questions are who, when, why, how and where?

The risk of fraud and inbuilt cryptography obsolescence undermine trust in the ICTs and judicial and political authorities. A focus on managing and controlling illicit transactions across borders – from goods, to money and people - provides a vehicle for trying to persuade citizens of the necessity of the technology and the sensitive objectives of judicial cooperation. However, technological advances – from digi-paper to RFID human therapeutic implants, tooth phone implants, using human skin as a tracking agent and robotics are now above the horizon, while older ITs like Radio Frequency Identification (RFID) raise the spectre of even more invasive intrusion into personal privacy and the likelihood of supervision and controls becoming ever more elusive. The EU's Article 29 Working Party fears that some applications give rise to serious privacy concerns (4). These include 'benign civil' actions such as commercial electronic tagging, vote or pay-by-fingerprint, secure contactless payments, and hidden RFID chips. All highlight the potential commercial market for global players with a stake in extending common commercial profiling, ehealth sub-dermal verichips, CCTV surveillance and 'ants' (crowd behaviour patterning) to surreptitious data collection tracking individuals in cyber-space (via internet) and territorial public places under the guise of assisting law enforcement. Technical 'solutions' created for one sector can be applied to others in ways that offend civil dignity, privacy, liberty and equality, and that compromise open, democratic government. Without EU wide or international laws on internet security and privacy many of the ideals and values taken for granted in the EU are potentially compromised, and not simply by unregulated blogopoly. Disagreement persists over the correct legal basis – and therefore accountability to political authorities – for EU action. The Commission argued that retaining internet traffic data should be subject to pillar I rules, whereas exchanging data and information be subject to pillar III. The European Data Supervisor was especially critical of the proposals. The intractability of finding a political solution has resulted in the ethical issue being been reconfigured as a problem of quality.

What are the quality criteria to be applied to ensure ethical ejudicial cooperation? How can we recognise quality justice? The counterpart to secrecy is not just privacy. The remedy does not simply lie in the application of existing mechanisms and institutions of democratic accountability. The use of ICTs and biometrics in the security domain raises further issues as to the *disclosure* of personal information among professionals for unspecified purposes, at unknown times, to unknown places and unbeknown to the individual concerned. There is a need to clarify precisely the meaning of words which are loosely and sometimes indiscriminately used by public and private sector agencies both of whom may be involved in the processing and exchange of personal information and data.

The individual's 'confidentiality' and *'privacy rights'need* to be balanced against other legitimate rights of the state and other citizens. Information exchange in sensitive sectors, like health, suggests that the notions of confidentiality and privacy rights lead to different obligations. *Disclosure* of personal information is not universally understood to mean the same thing, for instance, although it is easily seen as an implicit requirement of applying the principle of availability. Disclosure has to be based on an assessment as to the need for it, proportionality, risks to the individual as well as to third parties of non-disclosure and of disclosure, the practicalities of the processes involved (including their viability, sustainability, integrity and robustness from non-authorised interrogation), and the requirements of civil and especially criminal justice.

Managing judicial cooperation – The Procedural dilemma: a clash of cultures?

Implementing ejudicial cooperation involves complex political, legal, technical and operational administrative procedures at all levels. It concerns

cultural procedures within organisations. Rolling out ejudicial cooperation is a backroom operation. Big commercial interests compete for a lucrative share of an ever-growing market for e-card and ambient intelligence operations. Intelligence may not be the same thing as judicial information exchange but the sharing of intelligence can be central to effective detection and subsequent prosecution by judicial authorities. The boundaries between the two are somewhat permeable and opaque. Yet, both involve organisational, technological and procedural steps that affect what is finally delivered.

It is assumed that ICTs will boost effectiveness and make administrative efficiency gains. However, swifter information exchange does not necessarily mean that the quality of the data and data reliability are assured. Nor does it mean an equivalence in high standards for either the technical aspects of data processing, handling, retention, inter-operability or transmission and especially for the qualitative aspects of data analysis upon which further steps in combating crime rest. Success or failure in rolling out judicial cooperation is affected by inter alia:- organisational culture, technology and know-how; strategic political priorities; function creep; law enforcement uptake; and citizen compliance.

Organisational culture: cutting efficiency gains of deploying ICTs

The culture of an organisation deploying ICTs affects its efficiency. This reflects many variables from training, pay, professionalism, hierarchy, bureaucratic politics to group-think outside the scope of this paper. The technology and know-how exist, are being improved, developed, marketed and piloted. Software has also to be developed for tracking and monitoring judicial and legal procedures, organising and processing papers in secure communication channels, such as the e-Alternative Dispute Resolution procedure.

Two areas of cross-jurisdictional data transfer need to be differentiated: (i) conformity questions concerning the free flow of personal data in the EU; and (ii) quality matters relating to the retention, quality and interpretation of any such data. The first are subject to Community rules on the protection of personal data, the rights for data subjects and obligations on those processing personal data, and appropriate sanctions for offenders, and monitoring by an independent supervisory body. The EU addressed the second in 2005 when the Commission began infringement proceedings against Germany and Austria for failing to implement properly EU data protection rules under Dir 95/46/EC by breaching Article 28 requirements for guarantees as to the independence of their data protection authorities. Data about individuals held within the EU and member states by public and private (especially commercial) agencies are subject to varying degrees of data protection and privacy laws. The new set of model contract clauses approved by the Commission for the transfer of personal data from the EU to other states are also seen as insufficiently robust, although they expand upon the original directive in terms of audit provisions. Moreover, under specified circumstances exemptions may be granted. This applies to health matters, and to 'reasons of substantial public interest' (however defined) (Art 10(1)(5).

The trick now has to be to reconcile technical quality approaches to effectively controlling and scrutinising how data is handled with democratic expectations and functionally determined political practices that escape the territorial confines both of the nation state and of the EU itself. This may suggest that technical quality standards approaches could strengthen democracy rather than become a 'faceless' substitute for them. However, the limitations arising from intra and inter- agency trust deficits cannot be overlooked. They contribute to a wider inter-agency trust gap at EU level. Widely divergent definitions of criminal activity, its reporting and prosecution highlight further procedural matters likely to inhibit easy operationalisation of a 'seamless information flow' based on the principle of availability.

Managing mutual distrust

There is growing awareness that measures to facilitate data and information exchange among law and judicial agencies will not necessarily result in efficiency gains since national judicial cultures, rules, laws and practices vary greatly, mutual suspicion remains, the full application of the principle of mutual recognition has yet to be achieved, entries into national criminal records are disparate (for example, not guilty verdicts and acquittals are not uniformly recorded in national records) and access to national registers varies considerably. It may be partial or comprehensive, and different states may allow either police and judges or only one category access, whereas others may also permit professional associations, employers, private investigators to access such records. The European Parliament is therefore keen to promote quality via a procedure for mutual evaluation of good judicial practice in order to ensure that all citizens benefit from identical standards of quality. The current situation militates against this because just in the case of record-keeping, information is generally entered in differ-

ent ways and there is a need for standardisation along the lines of the forms used for Schengen databases. Standardisation, however, often precipitates and is a precondition for inter-operability, and for rules on the retention of data. It is also seen as a way of monitoring processes in states where corruption is high among law enforcement agencies.

Exchanging data is therefore as problematic as the issue of adhering to any governmental guidelines, standards, common provisions or codes of conduct for self-regulation. Clearly, to minimise discrepancies in interpreting and applying provisions, it would be desirable to create guidelines, sets of understandings and rules to promote conformity with common standards to complement the faster evolution towards integrated systems governing e-data exchange. This is happening in respect of the exchange of information between Schengen and Interpol on lost, misappropriated and stolen passports, and travel documents. Data exchange must comply with the data protection rules of the individual member states (who in turn are bound by Article 100 of the Schengen Convention) and of Interpol. The Commission sees one instrument of judicial cooperation – the European Arrest Warrant (EAW), as 'the first and most symbolic measure applying the principle of mutual recognition'. For the ordinary citizen, however, the most visible face is likely to take the shape of travel documents and identity cards.

Judicial cooperation using tools such as biometric verification and authentication systems, and ICTs to expedite the transfer of or access to information stored in data repositories (such as subject specific computers, including DNA data bases, visa, tax and health systems) can be prioritised with reference to political strategic goals, including migration and asylum, combating international crime and fraud etc. The uptake of judicial cooperation by law enforcement agencies from surveillance, migration, customs and police to those private security firms using CCTVs, tracking telephony, RFIDs – as with the new German travel document - is variable, subject to different legal requirements and practices as well as different levels of ICT systems. They are not equally robust, advanced, or secure (5). The only rule applying to any presumed transfer of information across jurisdictions is that local, domestic safeguards must be honoured. This mirrors the single market approach to technical barriers to trade. It may be seen as reasonable at a general level of principle. It is not reasonable at the level of local practices which compromise individual integrity, security and civil and human rights.

The challenge is to reconcile contradictory goals: greater security with often highly insecure applications by law enforcement agencies who do not have the same level of ICT progress or play by the same rule book or accountability mechanisms. Recent rulings at EU level regarding comitology processes to expand the competences of law enforcement agencies compound public disquiet. This was not allayed by the September 2005 Council Framework Decision committing the EU to 'strict observance of key conditions in the area of data protection' and respect for fundamental rights, 'with special attention to the right to privacy and to the protection of personal data… in particular, in view of the implementation of the principle of availability.' It stipulates that the exchange of relevant information between the member states will not be hampered by different levels of data protection among them.

Where there is a danger that processing of data may endanger the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the European Data Supervisor is obliged to check them. This requirement covers inter alia health, suspected offences, offences, criminal convictions or security measures. It is imperative to close the gap in how offences are defined and categorised: mutual recognition principles may not be entirely adequate or sufficient. At the operational level, there is an urgent attendant need for promoting conformity and good practice in the cross-border and inter-and intra agency transmission and exchange of data.

The uptake of the ICTs for judicial cooperation among practitioners at all levels is a precondition of effectively accelerating processes designed to combat crime, apprehend and prosecute suspects, track judicial procedures – from rogatory letters onwards in ever more areas of domestic civil law – such as family law as decreed by the Hague action Programme. The playing field is anything but level. There is a gaping digi-divide among legal professionals. Those at the forefront of developing and deploying ICT judicial cooperative procedures (for example the Austrian eRecht system) may have an advantage that goes beyond the demonstration effect to affect the nature of any e-law that inevitably must evolve around the deployment of ejudicial instruments, tools and procedures. Member states' legal professions remain attached to traditional practices and these could delay ejudicial cooperation. As a result, proving the efficiency gains and security of ICTs in judicial applications assumes greater importance.

The current rules are imperfect in content and application, diverse and discriminatory. The lack of common and sufficient parliamentary safeguards is

not adequately compensated for by the Council framework decision on attacks against information systems obliging member governments to approximate necessary measures to ensure that illegal access to an information system and interference with its integrity or that of its data are punishable as criminal offences incurring proportionate and dissuasive penalties. This is seen as a precondition to avoid compromising the attainment of a safer information society and the area of justice, freedom and security.

The Democracy and transparency dilemma – the insufficiency of Quality as a Code of Practice

There is a need to differentiate between codes of practice and democratic accountability. The codes of quality practice are instruments to: soften-up national administrative agencies to procedural changes having culmulatively and progressively deep political consequences; and advance consistency and coherence in operationalising common commitments, as in the case of the Common Manual for border agencies. This is to lead to common quality practices and standards at internal and external borders, and a common manual. Two elements implicit in the notion of policing a common border are separated: a legislative instrument and a practical handbook for border guards. In practice, as has become apparent, the member governments use their discretion to take national decisions to revert to national modes of practice. This has serious implications for the ideal of equal treatment of people within the EU, and for the nature of quality standards in practice.

Quality codes of practice or manuals add to transparency in making clear what the requirements and practices are. They do not equate to democratic checks on how policy is implemented, in whose name and on whose authority and in pursuit of which particular EU objective. They do prescribe a form of internal, peer accountability, and facilitate the development of indices by which progress can be measured. This is needed to produce quality justice, consistency and certainty for citizens and for governments seeking a predictable and uniformly secure border regime. But such codes of practice are not a substitute for, robust and credible, publicly legitimated and political accountability. To make the political commitment to mutual legal assistance work codes of practice, terms of art and organisational cultures have to be unpicked. Conformity remains a leit-motif. The Article 29 Data Protection Working Party regularly stresses this and the need to adhere to the principles of proportionality and lawfulness (4). The European Parliament has been vigilant, but parliamentary powers remain inadequate and elusive. Technology outpaces transparency and accountability as well as procedural codes of managing judicial cooperation that mask genuine ethical standards.

CONCLUSION: A DOUBLE DEFICIT

A common EU identity document has symbolic value in creating a tangible symbol of equal EU identity. But the embedded biometric tool and chips potentially exacerbate the apparent trust deficit. The introduction of the judicial cooperation tool of biometric identity cards for which individuals will have to pay and for which no common EU standard as yet exists[1] illustrates this. Biometric identifiers are very crude and inadequate instruments. The readier identification of an individual by itself is no substitute to the institutional codification and entrenchment of norms, values and quality practices that uphold enlightened, open, democratic government which is at the heart of liberty and security. The presumption that a seamless information area can expedite judicial cooperation questions the territorial realities of statehood and the constitutional defects of the EU as well as the relationship of trust between the governed and the governors (at whatever level). Constitutional norms clash with operational needs.

Whereas in the past, operational needs determined what constitutional measures would subsequently be needed to legitimise them, the prospect of ICTs being deployed as instruments of the already legitimated goals of pillar III highlight how fast operational requirements outstrip constitutional legitimation. It has long been understood that in war times, normal democratic values and practices may have to be suspended for the public good. Exemptions to open government have been accepted as operational necessities. Extrapolating these codes of exemptions to the daily conduct of policy-making and implementation not traditionally associated with wartime operations, creates tension and suspicion. This may be the inadvertent side-cost to ad hoc operationalisation of steps that evolve necessarily in response to legitimate security concerns. Their exclusion from accountability requirements and practices however compromises the system indirectly because the gap is filled by codes of practice that disguise the unquestioned assumption that governments make about their citizens: namely that

there is an adequate level of public trust in the government. This does not mean that accountability, ethical ejudicial cooperation and security must remain irreconcilable ideals. It does mean re-thinking the problem of transposing accountability into practice in a functionally determined, borderless cyber-space accessed by the traditional territorial agents of an expanding but still territorially defined securitised EU external border.

ACKNOWLEDGEMENTS

This research is conducted under Framework Six programme Challenge CITI-CT-2004-506256, and eJustice IST-2002-001567.

NOTES

1. EURODAC deletes information after 10 years, and holds only fingerprints (and no personal details). As part of EURODAC, Steria developed a central system for fingerprint identification (based in Brussels) and the Norwegian FIT-system for the electronic scanning and transmission of fingerprints. Fingerprint Image Transmission (FIT) facilitates transmission and control of fingerprints. FIT communicates with all the European AFIS systems. Over 500,000 fingerprints can be checked per second. The system can be installed in an ordinary PC and requires a minimum of training. 16 European countries have adopted the solution. Scottish Grampian police use Steria's facial recognition system.www.steria.no
2. The Council Presidency defined this as 'A judicial authority is regarded as competent law enforcement authority if the information or intelligence, according to national law, is only held by or accessible to that judicial authority';
3. One small example where there is extensive scope for error and failure concerns the issuing of driving licences. In some states this is organized nationally (as in the UK), in others at regional level. Whereas in some states major public contracts are divided into smaller packages, often with fewer risks of failure (as in the Netherlands), others are not.
4. See on the Netherlands College Bescherming Persoonsgegevens on http:www.cbpweb./nl/en and Finland, Ministry of Finance, www.hare.vn.fi See Working document on data protection issues related to RFID technology, January 19, 2005 Statewatch,org/news/2005/fed/13eu-rfids.htm. ARTICLE 29 Data Protection Working Party. This Working Party was set up under Article 29 of Directive 95/46/EC as an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136. Website: www.europa.eu.int/comm/privacy
5. Estonia was the first EU country to use home PC e-voting for local elections in 2005. Others have piloted authentication by pre-registering fingerprints that are then stored centrally, including Italy and Poland.ePoll envisages e-cvoting across Europe by 2009. The Finnish card has to be renewed every three years to keep up-to-date with technology that could be used to breach its integrity. The proposed French card differs in the scope of data to be held. See http://computerworld.com.sg/ShowPage.aspx?pagetype=2&articleid=753&pubid=3&i 13.04.05

REFERENCES

Article 29 Data Protection Working Party, Opinion 4/2004 on the *Processing of Personal Data by means of video surveillance*, 11750/02/EN, WP89, adopted 11 February 2004.

S. Booth *et. al.* (2004) *What are personal data. A Report for the UK Information Commissioner*, University of Sheffield.

Central and Eastern European Personal Data Protection Commissioners Declaration on future cooperation, *Smolenice*, May 24th 2005 www.ceecprivacy.org.

Commission proposal for a Council Framework Decision on the *Protection of personal data processed in the framework of police and judicial cooperation in criminal matters* COM(2005)475 final 2005/0202CNS, 4 October 2005.

Commission of the EU, *Communication of the Commission on Ensuring Greater Security of Explosives, Detonators, Bomb-making Equipment and Firearms*, IP/05/969Brussels, 19 July 2005 http://europa.eu.int/rapid/

Commission of the European Communities, *Report from the Commission based on Article 34 of the Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the surrender proce - dures between Member States,* {SEC(2005)267}, COM(2005)63 final, Brussels 23.02.2005.

Commission Decision (December 2004) amending Decision 2001/497/EC on the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46,COM(2004)5271.

Commission Staff working document Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC EXTENDED IMPACT ASSESSMENT {COM(2005) 438 final} Brussels, 21.9.2005 SEC(2005) 1131.

Council of the EU, Press Release 11116/01(Presse 187), press.office@consilium.eu.int, http://ue.eu.int/Newsroom 13.07.2005.

Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and

travel documents issues by member states, 13 December 2004, OJL 385/1, 29.12.2004, p 1–6.

Council Decision 2003/48/JHA of 19 December 2002 on the implementation of specific measures for police and judicial cooperation to combat terrorism in accordance with Article 4 of Common Position 2001/931/CFSP OJL 16/68, 22 Jan 2003.

P. Dunleavy and H. Margetts (2002). *Better Public Services through E-Government: Academic Article. Cultural Barriers to E-Government*. The Stationery Office, 2002, HC 704-III, Session 2001-2E.

E. Guild and S.Carrera (2005). *No Constitutional Treaty? Implications for the Area of freedom, Security and Justice*. Brussels, CEPS paper 231.

D. Elgesem (1999). The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data, *Ethics and Information Technology*, 1(4): 283–293.

European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final).

European Parliament Working Document on the quality of criminal justice and the harmonisation of criminal legislation in the Member States, Rapporteur Antonio Costa, 1.12.2004.

European Parliament, Second Report on the proposal for a European Parliament and Council directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (COM(2000)385-C5-0439/2000-2000/0189(COD)), rapporteur Marco Cappato, A5-0374/2001, 24 October 2001.

N. B. Fairweather and S. Rogerson (2003). Biometric Identification, Information, *Communication, Ethics and Society,* 2:1.

B. Hayes. (2005). SIS II. Fair accompli? Construction of EU's Big Brother database underway. Statewatch. May 2005.www.statewatch.org/news/2005/may/sisII-analysis-may05.pdf

Home Department, *Entitlement Cards and Identity Fraud A Consultation Paper*. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty July 2002 CM 5557.

Home Department, *Legislation on Identity Cards: A Consultation*, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, April 2004, CM6178.

L. D. Introna (2000). Editorial: Ethical Reflections on the virtual frontier. *Ethics and Information technol - ogy* 2:1-2.

Justice and Home Affairs Council 2626th Council meeting of 2.12.04, Press release 14894/04 Council: Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities in particular as regards serious offences including terrorist acts (4 June 2004) at www.statewatch.org/news.

B. Kracher, C. Corritore and S. Wiedenbeck (2005). A foundation for understanding online trust in electronic commerce. *Information, Communications and Ethics in Society*, 3: 131–141.

R. M. Kramer and T. R. Tyler (eds) (1996). *Trust in Organizations: Frontiers of Theory and Research*, London: Sage.

T. A. Lipinski and J. Britz (2000). Rethinking the ownership of information in the 21st century: ethical implications. *Ethics and Information Society*. 2(1):49–71.

J. Lodge (1994). Transparency and Democratic Legitimacy. *Journal of Common Market Studies*, 32:343–368.

J. Lodge (2004). EU Homeland security: Citizens or Suspects? *Journal of European Integration* 26:253–80.

D. Lyon (ed.) (2002). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, New York: Routledge.

L. MacMahon. (2005) EU Anti-corruption policy and ten principles for candidate countries. EU Commission DG JFS, Dir.D: internal security and criminal justice, Unit 2: fight against economic, financial and cyber-crime, Brussels, July.

H. Margetts (1999). *Information technology in Government*. London. Routledge.

L.Montanaro-Jankovski (2005). EU Policies to fight transnational organised crime in the Western Balkans. *EPC Policy Paper*, October.

D. Mason, C. Raab (2002). Privacy, Surveillance, Trust and Regulation. *Information, Communication and Society*. 5:3, 379–381.

J. H. Moor (1999). Using Genetic Information while protecting privacy of the soul. *Ethics and Information Technology*.1(4):257–63.

S. Peers, 'EU: Biometrics –from visas to passports to ID cards', www.statewatch.org/news/2005/jul/eu-bio-passports-id-cards.pdf 20 July 2005

I. van der Ploeg (2003). Biometrics and Privacy. A note on the politics of theorizing technologu. *Information, Communication, Society*, 6.

I van der Ploeg (1999). The illegal body: Eurodac and the politics of biometric identification. *Ethics and Information Technology*.1:.37–44.

G. Pearce and N. Platten (1998). Achieving Personal Data Protection in the European Union. *Journal of Common Market Studies*.36:529–47.

Presidency of the EU, Note from Presidency to the Article 36 Committee on Draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the member States of the European Union, in particular as regards serious offences including terrorist acts. Doc13867/04 4 Nov 2004.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1, 12.1.2001.

D. Rowland (2004). Data Retention and the War against terrorism – a considered and proportionate response? *Journal of Information, Law and Technology*, 3.

A. S Sertifitseerimiskeskus. The Estonian ID card and

Digital signature concept: principles and solutions. *White Paper* 5 June 2003, www.sk.ee

R. A. Spinelli and H. T. Tavani (eds) (2004). *Readings in Cyberethics*. Sudbury, MA. Jones and Barlett.

A. Takanen, P. Vuorijarvi, M. Laakso and J. Roning (2004). Agents of Responsibility in software vulnerability processes. *Ethics and Information Technology* 6: 93–110.

H. T. Tavani (2005), Ethical Reflections on the Digital Divide. *Information, Communication, Ethics and Society*.1.

T. Vaden (2004). Digitial Nominalism. Notes on the ethics of information society in view of the ontology of the digital. *Ethics and Information Technology* 6:223–231

UK: Identity Card Bill published 25 May 2005 http://www.statewatch.org/news/2005/may/uk-ID-CARD-Bill.pdf

E. Wagner (1998). 'The Integration of Schengen into the Framework of the European Union,' *Legal Issues of European Integration*, 25(2) 1-60

J. Wagner DeCew (1999). Alternatives for protecting privacy while respecting patient care and public health needs. *Ethics and Information Technology* 1(4):249–55.