FCT-9-2015: Law Enforcement Capabilities topic 5: Identity Management

ARIES
"reliAble euRopean Identity EcoSystem"

D2.2– Socio ethical analysis and requirements

Due date of deliverable: 30-11-2017
Actual submission date: 30-11-2017

Start date of project: 1 September 2016 Duration: 30 months
Revision 1.0

Project co-funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D2.2 – Socio ethical analysis and requirements

Editor
Dave Fortune & Juliet Lodge, Saher Ltd

Contributors
Saher, SONAE , UMU

Reviewers
Atos, UMU

28-11-2017
Revision 1.0

The work described in this document has been conducted within the project ARIES, started in September 2016. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700085. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document History

Version	Date	Author(s)	Description/Comments
0.1	21/10/2016	Saher	Draft sections
0.2	19/11/2016	Saher	Updates to GDPR
0.3	11/12/2016	Saher	
0.4	02/01/2017	Saher	
0.5	16/01/2017	Saher	
0.6	21/01/2017	Saher	Ethics Chap 2 updating & flow charts, Glossary, EIA review
0.7	22/01/2017	Saher	ePrivacy, Single Digital Market update
0.8	23/01/2017	Sonae	Barriers to eCommerce; focus groups
0.9	23/01/2017	Saher	Barriers to eCommerce; focus group questions
0.10	24/01/2017	Saher	VIS and Umbrella Agreement update
0.11	03/02/2017	Saher	Updates and uploaded to repository / ethical advisor DSM
0.12	24/02/2017	Saher	Societal acceptance model of IT update
0.13	22/03/2017	Saher	Vulnerability updating review, plus bibliog updating, airport updating
0.14	27/03/2017	Saher	eCom updating; official doc updating
0.15	10/04/2017	Saher	eAirport EES updating
0.16	09/05/2017	Saher	Baked in ethics by design update
0.17	29/05/2017	Saher	Review post Murcia meeting
0.18	30/05/2017	Saher	Revision re ~#4.2ff
o.19	01/06/2017	Saher	Revision #2.1
0.20	19/06/2017	Saher	Revision 2.1 re LIBE on encryption/privacy
0.21	23/06/2017	saher	Re biometrics and ethics after Ethical Advisor discussion
0.22	28/06/2017	Saher	EDPS update
0.23	30/06/2017	Saher	Stakeholder claims
0.24	7/7/2017	Saher	update
0.25	9/7/2017	Saher	Revision
0.26	17/7/2017	Saher	editing
0.27	26/7/17	Saher	update
0.28	30/7/17	Saher	update
0.29	31/7/17	Saher	revision
0.30	10/8/17	Saher	update
0.31	26/8/17	Saher	editing
0.32	3/9/17	Saher	Claims and poll review
0.33	14/9/17	Saher	Revision update legislation
0.34	30/9/17	Saher	edit
0.35	7/10/2017	Saher	Update post annual mtg, ethics advisor review, and pilots
0.36	10/10/2017	Saher	editing
0.37	16/10/2017	Saher	review
0.38	3/11/2017	Sonae	eCommerce findings
0.39	6/11/2017	Sonae & Saher	Joint review & update
0.40	6/11/2017	Saher	Edit and dissemination
0.41	13/11/2017	Saher, Atos,UMU, Sonae	Discussion, revision, update & review
0.42	27/11/2017	Saher & Sonae	Final review
1.0	29/11/2017	Atos	Format review

Executive Summary

In developing a technically innovative eID, Aries seeks to move beyond the state of the art to incorporate ethical concerns into the development of an eID that citizens can trust, that is informed by adherence to ethical principles, and which is appropriate to meeting the challenges and ambitions of the digital single market.

Ethics is a key to gaining public trust in the eID for multi-purpose use. The EU is keen to see the incorporation of ethics as first principle of technical design to ensure trust. Aries seeks to develop an eID that builds in ethical considerations from the start.

The Aries eID rests on the premise that ethical concerns are ubiquitous but not uniform, have different roots and connotations in different societies and across time, and are not readily overcome by systems that rely on large data bases to check and manage identity claims.

Aries seeks to find a means of allowing a genuine person to use an eID for all manner of transactions in ways that preserve his/her dignity, autonomy, privacy and security. The Aries eID solution is designed to be non-discriminatory and societally as neutral as possible (meaning, for example, that gaining such an eID does not depend on ability to pay for one, thereby meeting criteria on optimising inclusiveness).

Aries develops a technical solution in the vID that is as neutral as possible and minimise the myriad discrepancies across states that arise from different societies; traditions and legacy systems and practices.

Informed by an appreciation of tensions in society that may have inhibited eID take-up, and may still hinder its acceptance, Aries recognises that the Digital Single Market goal of once-only enrolment for egovernment has advantages and disadvantages. It outlines issues around automated cross-border information exchange and re-use and related questions. It reflects concerns over an enhanced digital divide; and the ethical concerns related to exaggerated claims for biometrics as well as citizen anxiety over biometric enrolment and sustainable biometric eID dependability.

The Aries eID is developed in line with respecting fully existing EU law, standards and prospective requirements under the GDPR.

ETHICAL PRINCIPLES
Pre-cautionary principle
Trust
Dignity
Autonomy
Self-determination
Consent
Equality
Inclusion
Non-discrimination
Purpose specification
Purpose minimization
Accountability
Transparency
Privacy
Security
Accessibility
Necessity

Aries goes beyond the SoA technically with a view to showing that privacy and security can be advanced simultaneously rather than as a trade-off in a zero-sum game. By providing a technical means to do this, issues around the acquisition of informed and explicit consent, compared to implicit consent (and the inferred consent deduced from ticking T&Cs) is addressed and overcome.

As a result, many ethical problems are addressed by the technology. They are not therefore dependent on compliance with rafts of national legislation which may not be consistent, uniform or easily enforceable by the user of an eID.

Aries technical solutions seek to mitigate barriers to eID adoption which may have cultural or societal origins, and which are often conflated with enrolment process concerns (biometric template generation and storage) and privacy objections. Challenges arise as to the relative weight to be given to the right to privacy (that some see as non-existent and redundant) and to the principle of autonomy, upon which the right to consent and the 'right to be forgotten' rest. Some barriers are generic.

Perhaps the biggest ethical concerns arise not from the eID itself but from subsequent unknowable re-use of information from which it is derived. Can such information be mined, re-configured in full or part, sold or used to make inferences about behavior and transactions. Can it be re-used and linked without the live and explicit consent of the live person to whom it relates and whom it identifies? Aries is aware that information collected for one purpose may not only be re-purposed but used to re-categorize citizens for all manner of purposes, whether tracking for commerce, surveillance, social trends, behaviour or re-selling partial slabs of information. The Aries eID departs from such categorization to create an eID that is a neutral as possible.

Aries eID, in seeking to be as neutral as feasible, seeks to use technology to safeguard individual privacy and security against intrusion using algorithms informed by ethical reflection. The Aries eID is a token of the real human. Part of it may be accessed for limited, specific purposes (e.g. to confirm age without revealing date of birth: this person is over 18).

Aries recognises the potential of biometrics to provide additional information about an individual claiming to be the person with whom eID is to be matched. It has taken into account different laws relating to the enrolment and storage and use of different biometrics by different states (eg common biometrics like face, palm, voice, iris, gait and fingerprints). It is aware that the EU's definition of biometric differs from that of the USA. It is aware that video analytics, making use of biometrics, is growing. It is aware that mutual recognition of roles, entitling specified persons to access specified pieces of information, is a complicated process and is not fool-proof.

The continuing growth in the development of technologies to mask aspects of biometric identities, in the name of purpose limitation, data minimization and preventing mission and function creep, poses additional challenges. Society may be inclined to adopt steps that inhibit biometric recognition (such as masks).

Aries tackles the problem of generating and maintaining trust in the eID by focusing on purpose limitation and data minimization to generate trust by leaving the disclosure of eID fields in the hands of the individual to whom the eID token relates. It draws on feedback from Aries' interviews with citizens and focus groups to provide a benchmark for citizen perceptions to inform the development of the eID and recommendations regarding an Ethical Impact Assessment.

An initial check on compliance with ethical principles was conducted at the outset of project, and followed up through internal and external reviews at the outset and a final external review. How the IT meets ethical requirements is demonstrated in the technical work packages.

The ethical challenge addressed relates to the seeming clash of requirements between industry business models and citizens' interest in minimising privacy losses while maximising convenience gains: industry v the citizen is to be transformed into industry AND the citizen.

Ethical Guidelines

The key issue is trust. A generic vulnerability and risk exists regarding citizens' concern over eiD misappropriation. This breaks down into a loss of trust in the security and robustness against fraud in the event of misappropriation, outsourcing, loss or theft.

For stakeholders, litigation, accountability, responsibility and transparency issues arise over industry or component manufacturer liability for failure, legal redress and liabilities for re-instating eIDs for the genuine person to whom it belongs that arise in the event of loss, theft etc.

For the citizen, an eID has to be trustable, convenient, efficient, robust against intrusion and available to all.

The first principle is the pre-cautionary principle of do no harm. If this is respected, there is a higher probability that trust can be established and sustained.

Informed by the Guidelines of the Biometrics Institute, the purpose of the guidelines is to generate ' a universal guide for suppliers, end users, managers and purchasers' with a view to enabling them to demonstrate to the public that best practice has been followed in the design, management and implementation of a project or system. Accordingly, the Aries' expectation is that citizens, when providing details for an eID, can be assured that those relying on it for all manner of egovernment and private transactions are committed to the Guidelines, understand and abide by the ethical principles informing them and intrinsic to the design of the Aries eID.

An ethical eID is designed to uphold those principles regardless of the state or supplier relying on the eID. In that respect, the eID is to be as neutral as possible.

The use of an ethical eID must be seen in its contemporary policy context to understand why such a biometric eID has a practical use and potential benefit for citizens outside the usual area of physical border and travel controls.

The EU is committed to realising a Single Digital Market and the principle of digital by default. In practice, it has legislated to protect citizens' personal data and privacy, and reviewed its cyber security strategy (2013) [1]. The importance of data privacy and combating cyber-crime recurs in many EU documents and policies (EDPS, 2017a; Tasheva,2017). More recently, the EU has supplemented its concern with privacy, data and privacy protection and security with the concept of baked-in ethics by design. There is no universal agreement as to what is meant by 'ethical' ICT practices, but there is an emerging consensus over ensuring that desirable ethical principles are designed into processes as a first principle rather than as an after-thought, in order to generate and sustain citizen trust in the reliability of the technology.

The document begins by discussing what is meant by ethics and ethical principles. It recognises that diffterent societies and states have different conceptions of ethics and that these may change overtime. In the EU, ethics has been largely conflated with observance of, and compliance with, legal and technical processes of data protection and handling. That is a necessary but not sufficient condition for ethical impact assessments.

Public trust in the technology and use of personal information linked to an eID has to be generated and sustained. The biometric eID has to be reliable in practice. Scepticism to eIDs potentially overrides acceptance based on the convenience of being able to use the eID for all manner of online transactions. In reflecting on socio-ethical issues, and the piecemeal way in which ethical reflection has seeped into realising digital opportunities and the digital single market, this document underlines the importance of ethical principles and requirements that are key to building trust in eIDs. It recognises that so far ethics has not had a high priority for many sectors; that there is a potential need for regulation, and that as a first step using a scalable ethical compliance checklist may be a realistic approach to moving forward. Conducting an EIA

[1] The own-initiative report prepared by the LIBE Committee focused on questions which fall within the remit of the committee, namely the serious threats posed by cybersecurity risks and cybercrime to the fundamental rights of individuals, the rule of law in cyberspace, and their implications for the internal security of the Union as a whole. It examined existing legislative and non-legislative which may help to address cyber-threats, as notably referred to in the European Agenda on Security; current challenges related to the fight against cybercrime and proposed measures to be taken by Member States, the EU and the different stakeholders to address them. Specific issues related to cybersecurity and cybercrime falling within the scope of LIBE exclusive competences are covered by this report, as for example the security of processing of personal data and the risks of personal data breach (as regulated in the General Data Protection Regulation 2016/679) or the international and intra-EU cooperation in criminal matters addressing current and upcoming cyber-threats. http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20170419CDT01461

coupled to a neutral eID, as envisaged by Aries, would be a contribution to constructive an ethical digital ecosystem for citizens.

Contents

List of Figures

List of Tables

1 Introduction

1.1 *Purpose of the document*

The purpose of this document is to show how socio-ethical issues are reflected in the Aries innovative eID. The document outlines ethical and societal considerations of the actual and prospective use of eIDs to help better understand and inform the e-ecosystem landscape. The document is informed by understanding that points in eID chain management occasion ethical considerations that may inhibit eID take-up.

This document addresses issues that must be better understood in order to identify the potential barriers to eID take up in society, and to help inform the development of an eID that is as neutral as possible.

This document seeks to provide some ethical guidelines to inform a workable, trustable and dependable eID. The objective is to inform other project work with a view to advancing a model that (i) could have traction in realising the eDSM; (ii) contributes to cutting the financial and personal costs to citizens of identity theft and impersonation; and (iii) develops understanding of how ethics is a prerequisite to developing a sustainable, trustable and reliable virtual identity ecosystem not an optional add-on in the design of eID and e-transactions.

It examines actual and potential stumbling blocks to the universalisation of eIDs. It features two use cases: eCommerce and eAirport to illustrate barriers and opportunities. The focus group and questionnaire feedback informed Aries attempt to innovate and build in ethics as a first design principle.

1.2 *Relation to other project work*

This document relates to the two case studies (eCommerce and eAirport) in providing an overview of the landscape and meaning attached to ethical eID use for public and private purposes.

It examines where in the use of eIDs there may be stumbling blocks to their universalisation. Scepticism on the part of the public presents designers of universally applicable eIDs with problems that must be overcome if the eID is to be trusted and gain widespread sustainable acceptance.

Through an exploration of eID use in respect of two use cases - eCommerce and eAirports - this document identifies points at which ethical issues may arise in the use and onward use of eIDs. This is designed to augment awareness among designers so that they can try and address those issues with a view to finding technical means to overcoming them. The innovative Aries eID is designed with awareness of the socio-ethical issues. This effort is informed by awareness of public perceptions as to the trustability and reliability of eIDs; and through pilot use cases of an Aries approach to mitigate perceived obstacles to uptake, and to build in ethics as a first design principle.

This should help to provide insight into:

i. the probability that the public will readily take-up, retain and use a biometric eID for the wide range of public and private transactions it could enable across services, legacy systems and borders;
ii. public perceptions that the virtual eID somehow guarantees the integrity of the information and person to whom it relates.

In order to develop actionable guidance on ethical eIDs for industry, the Aries project examines the potential acceptance of eIDs by society by asking questions about what it is about the proposed Aries' neutral eID

solution that may make it useful and acceptable to individuals. This adapts the findings of Venkatesh (2008: 275) on explaining the variance in intention to use, and actual use of, technology.

Reflection on ethics has a role in the design of the eID. This document therefore is an input to inform the more technical elements of the project. It also complements the deliverable on privacy where the legal privacy requirements are explained in depth. In the case of eCommerce, the project also draws on tried practice in Sonae.
The project recognises that ethical reflection is generally not a priority for business and public sectors but that it is becoming an essential requirement associated with trust and in constructing the Single Digital Market. A solution that is scalable and universalisable, along with an assessment procedure to enable ethical practice, potentially provides gains to citizens, businesses and the public sector.

1.3 *Structure of the document*

The document first describes what is meant by ethics, the concept of the principle of do-no-harm, and the eID and limitations of use. The project recognises that different societies and states have different conceptions of ethics and that these change overtime. Accordingly, a table is presented in 1.4 as a reference base for the project, and as a guide for developing as neutral as possible real-issue oriented ethical impact assessment.

The document defines the ethical principle within the scope of the project. It addresses the societal impact of eID use and stakeholder concerns abstractly and concretely through eID use cases: the challenges, risks and limitations on them are outlined with reference to two use case scenarios (i) eCommerce and (ii) eAirport. The central problem addressed is that of using the eID as a tool to assist in combating identity fraud.

Having provided the context against which use cases are developed, the document pinpoints the points in the ARIES project where the ethical issues must be addressed in recognition of their likely impact on society. It suggests points in the design processes where the principle of ethical by design might find leverage, and how in future limitations may be overcome, based on Aries' understanding of stakeholder concerns at the point of drafting.

The document ends with a bibliographical guide to relevant primary and secondary sources. The Annexes provide a list of some key relevant past and existing projects; and feedback giving a citizen perspective on eID use in common transactions, including the project use cases. These show points at which risks to ethical practice and the integrity of the information may occur. A final annex includes a summary regarding eborder developments.

1.4 *Ethics principles – a checklist*

The purpose of this checklist is to provide an internal reference for the ARIES team to use during the project development of the eID. The following information is included in the checklist:

1. Ethical principle, the name of which should be used consistently throughout each document in which it is referenced.
2. Definition of the ethical principle within the scope of the project.
3. Related stakeholder concerns in the context of eIDs. These should include both abstract and concrete examples, many of which are already being considered by the ARIES team.
4. How the ARIES eiD addresses the stakeholder concerns. Specifically, which aspects or design decisions of the ARIES eID address the identified stakeholder concerns; and/or how these concerns or limitations may be overcome in the future.

The checklist includes the seventeen ethical considerations given to the external Ethics Advisor in an internal document.

It is clear from the project that priority should be given to realising core ethical principles whilst observing the overarching precautionary principle of 'do no harm'. Accordingly, Aries focuses on those.

The Ethics Advisor recommended that the ARIES team develop an ethical impact assessment of using eIDs in different scenarios. The assessment is informed by the lessons from and identification of gaps and weaknesses during the two case studies (eCommerce and eAirport). It is to be supplemented by an assessment of how potential eID users might be made better aware of and informed about ethical compliance. The assessment also considers "best practices" for eID users with regard to overseeing their data.

Ethical Principle	Definition	Related Stakeholder Concerns	How ARIES eID Addresses Stakeholder Concerns
1. Pre-cautionary principle	The one ethical principle to which all other ethical principles are linked and subordinate. It highlights the obligation to "do no harm."		
2. Trust	Trust refers to the obligation to handle data in such a way as to build and sustain public trust in the data handler's commitment to legal, secure and ethical processing.	Concerns by the public that whoever handles their data can be trusted to do so in compliance with legal principles and respect ethical practice. This includes the principle of no loss of control of data and respect for the principle of the right to be forgotten. This places high expectations and obligations on data handlers.	Aries is designed to maximise the potential for generating sustainable public trust in a reliable virtual eID that minimises the chance of fraud. That is a core goal of the project.
3. Proportionality	No data other than that which is explicitly required for the transaction envisaged should be used.	If more data is requested than is necessary, there is the probability that insufficiently precise rules apply to the data with the risk of mission and function creep.	The virtual eID is designed to elicit only that information that is intrinsic to the transaction, and not to extract additional information.
4. Dignity	Human right to dignity must be respected. This means that if a person is unable to supply the requested data for the transaction, an alternative means of completing the transaction should be provided discreetly.	• E.g. For eIDs involving facial recognition, how best to accommodate individuals who wear face coverings, including burkas, masks or plastic surgery? • For eIDs involving iris scanning, how best to accommodate individuals with prosthetic eyes? • For fingerprints, in the event of missing fingers, what alternative is envisaged to enable that person to access a particular service? How are disabled people's needs accommodated.	Biometric data is not stored. The kind of biometric held in the master repository by a public administration will depend on the state in question. In principle, an Aries eID could be biometric agnostic : in practice, it may only be available to people able and willing to provide one or more particular biometrics (eg iris plus fingerprint/voice print/face)
5. Autonomy	The principle that a person has control and is	A service should not compromise the	Aries eID enrolment is voluntary.

	able to exercise that control himself/herself without intervention.	autonomy of an individual by, for example, involving surveillance that is not essential to the transaction.	No one may be forced to enrol. There must be an alternative means of accessing public services or online services separate from the Aries eID.
6. Self-determination	The principle of personal choice. No one should be under duress.	A person should be able to choose whether or not to provide requested information, including a biometric, in the form demanded by the service provider without being discriminated against should s/he be unable to do so. This is related to the principles of dignity and autonomy.	The choice of whether or not to enrol for an Aries eID is left to the individual person to decide.
7. Consent	A person should have the right and ability to consent to how their data is managed and used; an opportunity to not consent without then being deprived of the opportunity to access a requested service; and an opportunity to consent to any onward use	A provider may not assume that they can do whatever they like in future (including data mining, ad tracking, data analysis, splicing, re-sale, etc), or rely on function and mission creep business models that implicitly get a potential customer/client to tick a 'consent' box for vague or imprecise purposes.	Aries eID holders are informed in advance of how their information will be used, held and destroyed. An individual may request the destruction/erasure of their data at any time.
8. Equality	Equal access to the service envisaged requires non-discrimination in terms of gender, age, capacity	A service may not be restricted to a given gender, educational or social group unless prescribed by law (eg access to age restricted goods and services)	An Aries eID should be universally available in future. For the purpose of the project, it is being trialled with able bodied people typical of online users.
9. Inclusion	People with disabilities or socially excluded must be included in the service to be provided.	Ensuring service and data requirements are presented in an accessible manner; ensuring that if infirmity or disability compromises a person's ability to use the service, an appropriate alternative is available immediately.	Aries eIDs should be available to all in future.
10. Non-discrimination	The service must be universally available and	Automated sifting according to	Aries eIDs will not be restricted in

	not restricted by gender,race, social class, ability to pay etc	predetermined criteria, such as race, age, disability, background, intelligence, etc.	future to those with a particular background or ability to pay high fees.
11. Purpose specification	The purpose for data handling must be presented clearly and precisely.	Vague descriptions which implicitly allow for function and mission creep are not acceptable.	Aries eID enrolment procedures make clear how data will be handled, in line with EU regulations and directives; and how onward splicing or re-use is prohibited.
12. Purpose minimization	The data collected or referred to must be the minimum necessary for the purpose of the service to be delivered.	A vague general purpose is unacceptable. No more data than is essential and necessary for the transaction envisaged may be collected. Eg if a person wishes to buy age-restricted alcohol, the vendor need know only that a person is over the prescribed age. The date of birth, home address, name etc. of the person are superfluous. Excessive data may not be collected an re-used.	Aries eID does not depend on a vast amount of data being collected and interrogated. The purpose of the Aries eID is to limit data exposure so that only that which is essential for the transaction is authenticated.
13. Accountability	Data handlers must be accountable legally in respect of their handling practices.	An individual must have the right of redress in the event of poor handling, theft or loss. The liability of the data handler is established.	Aries project team are accountability for how data is handled and used, again in conformity with EU legislation and relevant national laws.
14. Transparency	Data handling practice must be open, clear and explicit.	How data is handled must be made explicit and understandable to the public. Lengthy T&Cs are unacceptable.	The Aries eID does not assume that an enroller implicitly gives consent. Rather, explicit consent and data handling practice, in line with best practice, will be made available in future.
15. Privacy	Data handling must comply with the highest legal standards (eg EU GDPR)	• Means different things to different people. How best to ensure the privacy needs are	Aries does not regard privacy as a commodity only available to those who can afford to buy the highest

		met? Some data are sensitive (health for example) and should be interrogated only for the purpose for which they were provided. This compromises the collection and use of biometric data from which other issues may be inferred.	levels of privacy security. Instead, privacy in intrinsic to the aim of the Aries eID to minimise information exposed and so help combat fraud and breach.
16. Security	Data handling procedures must be robust to ensure that personal data are secure	Service providers must be compliant with the law; they must ensure their own systems are secure and robust against intrusion to prevent data loss, theft or compromise.	Aries expects highest robust data handling practices.
17. Accessibility	Online services must be accessible and presented in accessible formats to all of society.	• eIDs might contribute to the digital divide, whereby the wealthy and privileged have broader access to the service or can buy higher levels of privacy (that would be unethical); also, accessibility means that online information must be accessible (legible or vocalised), or that those unable to speak have alternative means of accessing the service without their dignity and autonomy being compromised	In future, accessing Aries eID online for disadvantaged users would be addressed by designers of the Aries eID public-facing portal. This would ensure that dignity and autonomy of all.

1.5 *Glossary adopted in this document*

Definitions are those of the EDPS or adapted from those of the EDPS

Accountability Principle intended to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with data protection principles in practice. Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.

Adequacy Decision: Decision taken by the Commission establishing wither a third country provides comparable level of protection of personal data to that of the EU, through its domestic law or international commitments. Under new data protection rules, the Commission can adopt adequacy decisions for law enforcement sectors. His includes the review of limitations and safeguards applicable to public authorities for law enforcement and national security purposes wanting to access personal data.

Article 29 Working Party: the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States. It comprises representatives of the national supervisory authorities in the Member States; a representative of the European Data Protection Supervisor (EDPS); and one from the European Commission

Article 31 Committee established by Article 31 of Directive 95/46/EC. Comprises representatives of the Member States who cooperate in taking decisions whenever Member States' approval is required under the Directive. By way of example, the Committee cooperates in the procedure for the adoption of Adequacy decisions.

Automated individual decision: Article 15 of Directive 95/46/EC and Article 19 of Regulation (EC) No 45/2001 lay down the right for individuals to object to decisions about them and solely based on automated means, unless certain conditions are fulfilled or appropriate safeguards are put in place.

Big data: Gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed using computer algorithms.

Consent: The EDPS defines consent in data protection terminology, as referring to any freely given, specific and informed indication of the wishes of a data subject, by which he/she agrees to personal data relating to him/her being processed (see Article 2 sub (h) of Data Protection Directive 95/46/EC and Article 2 sub (h) of Regulation (EC) No 45/2001. Consent is one of the conditions that can legitimize processing of personal data. If it is relied upon, the data subject must unambiguously have given his/ her consent to a specific processing operation, of which he/she shall have been properly informed. The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect. Council Working Party on Data Protection was originally set up to deal with the foundations of the EC policy on data protection, such as Directive 95/46/EC, Directive 97/66/EC and Regulation EC (No) 45/2001. It allows for a more horizontal approach in first pillar matters and Commission initiatives on PETs or RFID, and other subjects like Member States' experience with Directive 95/46/EC. The following is relevant in relation to this: EDPS Opinion on the processing of health data at the European Securities and Markets Authority (ESMA) (case 2013-0927)
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/ReferenceLibrary/16-11-16_Health_data_workplace_EN.pdf

EU Data Protection Reform package: on 25 January 2012, the European Commission adopted its reform package, comprising two legislative proposals: a general Regulation on data protection (directly applicable in all Member States) and a specific Directive (to be transposed into national laws) on data protection in the area of police and justice. In addition to his Opinion of 7 March 2012 elaborating his position on both proposals, the EDPS sent further comments on 15 March 2013. The two proposals have been discussed extensively in the European Parliament and the Council. The EDPS has continued to have regular contact with the relevant services of the three main institutions throughout this process, either following our comments or Opinions to the European Commission or in discussions and negotiations in the European Parliament and Council.

GDPR Regulation 2016/0679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, will replace Directive (EC) 95/46 as from May 2018.

Information Security: Information security refers to the ways and means to protect printed, electronic, or any other form of confidential, private and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption. When dealing with personal data, it is also necessary to consider the potential impact on citizens and strong measures to reduce the associated risks. The EDPS has produced guidelines on this topic: Guidance on Security Measures for Personal Data Processing -Article 22 of Regulation 45/2001
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/ReferenceLibrary/16-07-07-Information_security_EN.pdf

Information Security Risk Management (ISRM) is the specific process that helps those responsible for Information Security to manage the uncertainties which might affect the security of their organisation's information over time and indicates how to best react to these uncertainties within the constraints of their work environment. ISRM includes an analysis of the risks faced by an organization and defining appropriate security measures to tackle those risks.

NIS Directive: The national information security Directive (due to be in effect in the EU28 by May 2018) commits members to notification and compliance procedures, as well as to the establishment of Computer Security Incident Response Teams (CSIRT)

Personal information or data: Any information relating to an identified or identifiable natural (living) person (eg names, dates of birth, photographs, video footage, email addresses and telephone numbers). Other details such as IP addresses and communications content - related to or provided by end-users of communications services - are also considered as personal data.

PETs Privacy Enhancing Technologies: Important advances by ENISA framework relies on a set of assessment criteria, which can be broken down into specific parameters and assessment points, acting as indicators of certain properties and features of the tools. A distinction is made between generic criteria (applicable to all tools) and specific criteria (addressing technical characteristics of different categories of tools). For the purpose of this work, the following categories of PETs have been considered: secure messaging, virtual private networks (VPNs), anonymizing networks, and anti-tracking tools (for online browsing).

The 'PETs control matrix' is the implementation of the proposed methodology into a practical tool that can be used for performing the assessment of a PET and presenting the relevant results. As such, it comprises different sets of detailed assessment questions (and relevant closed sets of answers) corresponding to the predefined assessment criteria. In this way, the 'PETs control matrix' can facilitate a standardized and clear

presentation of different privacy tools, supporting in this way the possibility of comparative assessments. https://www.enisa.europa.eu/media/news-items/news-wires/RSS

Privacy: the right of an individual to be left alone and in control of information about his or herself. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7). The Charter also contains an explicit right to the protection of personal data (Article 8).

Processing of personal data: According to Article 2(b) of Regulation (EC) No 45/2001, processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." See the glossary on the EDPS website.

1.6 *Acronyms used in this document*

AI	Artificial Intelligence
ATD	Automated Threat Detection
BGP	Border Gateway Protocol
B2C	Business to Consumer
CFR	Charter of Fundamental Rights in the EU
CNIL	Commission Nationale de l'Informatique et des Libertes
CSIRT	Computer Security Incident Response Team
DNS	Domain Name System
DPI	Deep Packet Inspection
EC3	European Cybercrime Centre (Europol)
ECJ	European Court of Justice
ECTC	European Counter Terrorism Centre (Europol)
EDI	Electronic Data Interchange
EDPR	European Data Protection Regulation
EDPS	European Data Protection Supervisor
EFT	Electronic Funds Transfer
EGE	European Group on Ethics
EMSC	European Migrant Smuggling Centre (Europol)
ENISA	European Union Agency for Network and Information Security
EPRIS	A European Police Record Index System
ERP	Enterprise Resource Planning
EU	European Union
Eurojust	European Union Judicial Cooperation Unit
Europol	EU law enforcement agency (agency status as of 1 Jan 2010)
EULA	End User Licence Agreement
EU LEA	EU Law Enforcement Agency
FIDO	Fast Identity Online Alliance (est 2013)
FIU.net	Financial Investigations Unit (Europol)
GDPR	General Data Protection Regulations

ICANN	Internet Corporation for Assigned Names and Numbers
ICTs	Information and Communication Technologies
IPC3	Intellectual Property Crime Coordinated Coalition (Europol)
IoE	Internet of Everything
IoT	Internet of Things
ISA	Interoperability Solutions for European Public Administration
MMORPG	Massive Multi-player Online Role-playing games
P2P	Peer-to-Peer
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
PIA	Privacy Impact Assessment
POS	Point-of-sale
SIENA	Secure Information Exchange Network Application
SOCTA	EU Serious and Organised Crime Threat Assessment
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TCP	Transmission Control Protocol
TE-SAT	EU Terrorism Situation and Trend Report
UNIDAI	Unique Identifica (Number) Authority of India
US-VISIT	US Visitor and Immigration Status Indicator Technology programme
VoIP	Voice over IP
WSIS	World Summit on the Internet Society

2 The policy context

There are two core policy areas which have led the adoption of e-identity management and authentication assurance: border security and eCommerce. Often treated separately, they share common problems. Aries seeks to develop a scalable eID that would help to address specifically common problems associated with fraud, arising from identity theft and impersonation.

The two policy areas tend to be compartmentalised. This does not make sense: in practice, the value of personal data for business models lies in it being recorded, handled, re-configured, mapped and potentially linked. Data may have been obtained for a specific purpose. By linking it to other data and information (potentially for security intelligence and/or tracking and advertising purposes) core ethical principles are breached. This has raised concerns that create obstacles to citizen acceptance of inter-operable eIDs. The reasons for this are briefly sketched below as they have evolved in parallel with the development of e-security technologies and the EU's security union strategy; and the development of the European Digital Market. They show attachment to EU values which underpin ethics.

The broad policy context is outlined in more detail below. This is not coherent. Rather, it reflects the uncoordinated evolution of steps taken in different policy sectors to using ICTs to enhance efficiency, effectiveness, convenience and to lever the response and speed advantages of ICTs to better address policy challenges. Following the overview of two key sectors, the use cases are described along with important issues relevant to them. The emergence of solutions in distinct silos illustrates the need for an over-arching understanding and approach across the sectors in order to create coherence and trust in e-transactions in general. Difference is not always creative or productive and can lead unintentionally to ambiguity and contradictory approaches. This problem has been highlighted in respect of privacy and is even more acute in relation to ethics.

2.1 *What is meant by ethics*

There is no universal agreement as to what is meant by either ethics or 'ethical' ICT practices.

Ethics is largely conflated with observance of, and compliance with, legal and technical processes of data handling. Whereas, stakeholders and data protection professionals may understand these requirements, society at large does not. Instead, the public sees data theft scandals, concerns over spamming and privacy and fraud. These may deter future uptake of eIDs because there seems to be increasing wariness about the usefulness to citizens of trying to gain redress in the event of their data being mishandled, lost or stolen. Ticking boxes on Terms and Conditions is not seen as optional but essential if the service on offer is to be accessed.

Ethics defies definition: cultures differ over the relationship between the individual citizen and society, and the state and the people. This is sharply illustrated in respect of concepts of individual privacy. Privacy, however understood, is subordinate to ethics, and is arguably a tool to ensure try and ensure observance of ethical practice across the board.

Consensus over the ethical use of data and the kind of eIDs that may be adopted by the public are elusive. However, more easily recognised are applications or use of data that are seen to be improper and in conflict with commonly held standards of moral decency and appropriateness.

The use made of something, like an eID, occasions many ancillary questions about the person associated with it. This is problematic and has preoccupied legislators anxious to ensure that citizens (who have ambivalent attitudes to privacy protection in practice) (Satori,2017) do not inadvertently reveal and allow aspects of

themselves to be sold for commercial gain, including the data and associated information that they generate. Further ethical issues arise.

Cultures differ in the relative weight they give to privacy and private space. These are both concepts whose relevance has shifted over time. (Capurro). As a result, it is prudent to suggest how key ethical principles may be used to inform data handling practices that rely, at some point, on eID authentication on the part of the citizen or the service provider.

The dominant principle must be the precautionary principle of 'do no harm'. All others are subsidiary.
Precaution
Autonomy
Dignity
Purpose specification
Purpose limitation
Privacy
Informed Consent
Justifiability
Fairness
Transparency
Equality
Necessity

These core ethical principles inform and shape the design of a virtual eID ecosystem. They are not value-free but underpin good practice in the EU, and inform the ARIES eID which bakes in ethics and is as neutral as possible in its impact on societal values. That neutral eID is likely to have a higher probability of being accepted by citizens and of being scalable across cultures.

The Origins of the Core principles
The core principles of ethical practice have been extracted from philosophy and medicine which have grappled with *the impact of technical and scientific advance on what it is to exist as a human being*.

Central to this is the understanding that information does not exist in a vacuum: changing interactions of human communication mean that meaning is lived and defined in an ever-evolving dialectic between message and messenger. (Kelly & Bielby:5) Capurro focuses on the human-information relationship challenging traditional approaches to information science, and through his theory of Angeletics looks afresh at the relationship between information theory and the grounding of Being. This allows us to see how 'information interpolates directly with both our communal sense of being and our personal sense of disclosing meaning'. (Kelly & Bielby:6). This approach is informed by philosophy but is crucial to an appreciation of the impact new technologies on, and receptiveness to them of, society. It also helps us to better understand what may be the factors that encourage or inhibit uptake by society.

Identity, its personal revelation or concealment, are intrinsic to the contemporary focus on finding a convenient means to do so for specific transactional purposes using online means. The eID, as a physical or virtual token to represent the self, provides a medium to do this. The challenge is to determine a way to do this that is as neutral as possible on both the individual and society.

It is necessary but not sufficient, therefore, to identify the technical, legal and societal objections to eID adoption and to determine the associated boundaries concerning its use, including importantly the extent of concealment or exposure of linkable information it could enable. Determining appropriate limits is informed by what is loosely called 'ethics'. However, this is complicated because there is no universal acceptance of what is ethically appropriate or acceptable. Consequently, designing something that is 'ethical by design' implies designing something that minimizes objections to it from different societies and cultures because it

can work without transgressing their particular cultural norms. It implies, of course, a lot more than that but it is an essential building-block of an ethical e-ID eco-system.

Ethics and fundamental rights coalesce where policy and law are concerned. Their technical iteration is complex, intricate and intertwined. Interlinkage is inevitable as AI and IoE increasingly interact without human intervention. What may or may not be acceptable to consumers, and what therefore may deter them from adopting eIDs, is at the heart of divining ethical guidelines for an appropriate ecosystem. The EID itself is inseparable from the systems within which it will be used, all of which involve an exchange of digitized, possible sensitive and almost certainly personal and private information. How this is proceeded is both subject to rules on legal and fair processing and law governing data protection. It is also linked to public perceptions as to the legitimacy and purpose of processing, transferring and retaining/erasing such information and honorability of those doing so. Inferences about ethical underpinnings emerge in EU rules on cross border information exchange for law enforcement purposes, a recent iteration of which is that of 11 May 2016.

In September 2016, the European Data Protection Supervisor (EDPS) called for the establishment of an EU values based common area on the web backed by coherent enforcement of fundamental rights in the age of Big Data. He floated the idea of a network of regulatory bodies for enforcement in the digital sector voluntarily to share information regarding possible abuses in the digital ecosystem. (Opinion 8/2016). It is the issue of potential (ab) (mis)use that underscores the need for clarity over the purpose and meaning of ethical reflection in respect of ICTs in general and of identifying and authenticating individuals by electronic means.

2.2 *Ethics as a bridge between innovative technology & privacy*

The EU Data Protection Supervisor has stressed the need for ethical reflection on the digital environment, data protection and privacy. (Action 4, EDPS,2015a) The EDPS set up an Ethical Advisory Group on these and related issues in 2016. Both underline the need to implement data protection principles ethically, enforce legislation effectively, and ensure that main actors and private citizens are informed and able to respond fairly and ethically as digital innovation re-shapes public spaces and society in the light of data processing and in how society use new technologies.

What this means in practice is that businesses show to the public how ICT innovation and privacy are not anti-ethical but complementary by demonstrating their adoption of responsible, transparent and accountable practices informed by and reflecting ethical implications.

The tendency to rely on compliance with data processing and privacy regulations (such as the new GDPR and the revised ePrivacy directive transformed into a Regulation) is necessary but not sufficient. In October 2017, the European Parliament updated data protection rules to include new forms of personal communication (including Whatsapp and instant messaging) that reveal swathes of personal information that could otherwise be mined without consent (europarltv.europa.eu 17 October 2017; COM(2017)0010-C-0009/2017-0003(COD)). Its amendments, now under negotiation, included the following recommended amendment:

"*Metadata can also be processed and analysed much easier than content, as it is already brought into a structured and standardised format. The protection of confidentiality of communications is an essential condition for the respect of other connected fundamental rights and freedoms, such as the protection of freedom of thought, conscience and religion, freedom of assembly, freedom of expression and information." (p.6)*

Data protection and personal communication principles must be implemented ethically. They must to be supplemented, where necessary, by human ethical judgement. In an increasingly automated world, human intervention cannot be taken for granted. Therefore, engineering and code should incorporate ethical principles. Any bias must be transparent. Purpose must be clear, specified and limited and not facilitate by default or design an extension of use that may be ethical by today's standards.

The EDPS recognises that the law lags behind technological innovation and argues that new technology should incorporate ethics by design to reduce its potential negative implications on society.

Accordingly, the EDPS argues that digital ethics relate closely to human dignity, self-determination and autonomy.

How these are translated into daily use of eIDs poses challenges in terms of data processing, data handling, storage, linkage, big data, open data, future use. Liability and binding corporate rules do not sufficiently reflect the potential negative impact on society if digital innovation is not effected responsibly, accountably and hence, ethically. *The EDPS therefore urges innovators to assess how potential risk and harms* may come to the surface. This means there is pressure to reflect on and engineer in such a way as to ensure ethical concerns are built-in as part of a conscious process of innovating in order to realise the potential of the digital single market in a fair and open way.

2.3 *The precautionary dominant ethical principle*

There is one key ethical principle to which all other ethical principles are linked and subordinate. This is the ***pre-cautionary principle***, modelled from medical practice. It highlights the obligation to 'do no harm'. Loosely this means that just because something is technically possible to do, does not justify it being done if foreseeable harms are evident. Closely associated and derived from this precautionary principle are principles impelling proportionality, purpose limitation, self-determination and consent, autonomy, dignity, and necessity (data minimisation).

The **precautionary principle** is ancient.

Philosophers have discussed ethics for centuries. Contemporary interpretations are informed by the ethical codes common to medical science and practice. Refining accepted medical ethics for informational technology practices suggests that ethical practice and ethical technological applications need to be aware of, and in the case of eIDs, sensitive to how they will mitigate, avert or accommodate risks (or potential harms).

The precautionary principle of do no harm is about more than identifying potential harms, determining legal liability or redress for harm. It is supposed to inform design and practice from the start. This is something that has not been well-understood outside the medical sector broadly conceived. The focus on identifying and using legal remedies for harms is widespread. This detracts from, and to some extent ignores, the need for ethical reflection and baking in ethical design in algorithms from the outset. This helps to account for ethics being either neglected or not recognised as part of a business model. Consequently, where the dominant narrative derives from legal perspectives and litigation to provide financial recompense for harm (as in the USA), the understanding of what 'harms' may arise from new ICT applications has led to a focus on extending the scope of legal remedies and insurance to cover those new risks. For example, a theory of data breach harms focuses on risk and anxiety in law to suggest that where there is a prospect of informational 'injury', the intangible risk of harm and associated anxiety might be sufficient to establish risk and hence the likely increased danger of diffuse injuries if certain practices are adopted. Data breaches, for example, are known to trigger harm so risks and anxiety might be assessable, and liability computed. (Solove & Citron,

2016:1) . This crystallises in a reactive response approach to 'harms' and 'injuries' rather than in a preventive strategy.

This reactive approach contrasts with the preventive approach in the EU to highlighting ethical practice and baking in the precautionary principle of 'do no harm' which inform ARIES eID.

In the EU, the precautionary principle is expressed in guidelines and in legislation. They are reflected in ***duty-of-care provisions***, as in the case of the GDPR and the complementary ePrivacy Directive (soon to be Regulation). This duty-of-care has been marked in respect of privacy protection in both the GDPR and ePrivacy deliberations: e.g. both require importers and retailers of IT to distribute only privacy-by-design compliant technology. It is understandable, but no longer sufficient, for private and public sectors to assume that PbD protects against harms. However, the *temptation to assume that PbD compliance automatically implies respect for ethical principles must be avoided.*

The term 'ethics' is not unambiguous but has been possibly a less contested term than privacy, with which it is closely associated.

For the ARIES eID, ethics is seen in relation to when, how and by whom (or what algorithm) decisions are made, and for what purpose. This means that there are several points at which ethical reflection must occur to guard against baked in bias and ensure ethical principles are respected in terms of all elements of the design, from inception to roll-out and real-world practice to scalable use.

The following points in the design-to-use chain offer opportunities for reflecting on ethical matters:

1. Innovating from the point of an idea to the design of the medium/app, for example, in which personal information is to be held
2. technical rules governing handling or and access to that information, including the medium for transferring information in full or part (e.g. a person or a bot)
3. technical vulnerability to the integrity of the medium and its message
4. commercial opportunity opened by the use of the medium /app
5. impact on the individual providing information (knowingly or not) to access a service or commodity
6. necessity of adopting an e-medium to enable multichannel access

Ethical reflection cannot stop at the design phase because actual deployment (use) must also be ethical in practice in the real world. The EU draft ePrivacy regulation refers to 'personal communication' to cover all aspects of personal online life that previously would have been seen as something to be mined for commercial gain without the explicit, informed consent of the person to whom it related. Harms and consent are problematic but are central to understanding and addressing ethical requirements designed to uphold the pre-cautionary principle. Once again, the idea of baking in ethics by design is informed by and derived from medical practice. In medicine, the medium by which a treatment is conveyed (such as an oral medicine, tablet, etc.) must honour the overarching principle of 'do no harm'. Where harms are known and occur, they are to be minimized and the *ethical principle of necessity* determines whether on balance the harm outweighs the risk of not using the medicine.

The do no harm principle provides possibly the best initial ethical test to be applied to the design of a new algorithm or app. It is gaining acceptance among those developing apps for a digital society accustomed to automated decisions being driven by bots rather than immediate live human decision making on a human2human basis. However, this immediately raises additional ethical issues summarised by the principles of **purpose specification** and **data and purpose minimisation**: what might be ethically acceptable and desirable in one setting (or societal culture) may be undesirable or abhorrent in another. For example, society might see as legitimate and morally justifiable, therapeutic medical media that enable a person to

regain some personal **dignity and autonomy**. These might include deep brain implants to control involuntary, disease induced shakes or anxiety attacks or chips that permit remote online checking of glucose levels to warn a diabetic person and so help to prevent collapse. Their appropriation or misuse for other purposes would not necessarily be seen like that. In the context of eCommerce, eye-tracking citizens looking at goods in order to advertise directly to them raises ethical concerns: purpose specification and minimisation are compromised. The use of biometrics (which comprises virtually all kinds of information about a person) risk endangering dignity and autonomy, or commodifying the human body and so compromising personal integrity.

Dignity and **autonomy** are core elements of the concept of bodily integrity. Notions of **privacy** (in private and public transactions) relate to them. Privacy is a contested term. For some it has *intrinsic* value, for others it is *instrumental* in relation to other values, such as freedom (or autonomy), dignity and the development of personality (van der Sloot 2015). The need to engage in ethical reflection to protect them is illustrated in relation to the e-life and identity of vulnerable people and minors.

Children's online life experience (often begun without their understanding or consent by their parents, relatives or guardians putting them into social media) is believed to reinforce stereotyping in their real-life choices, notably where gender preferences seem to be strengthened in relation to commercial opportunity. (Hota & Derbaix,2016). However, ethically informed legal amendments to the ePrivacy draft Regulation in October 2017 suggest that data mining and related practices will be seen as compromising personal privacy, conflict with citizens' basic rights under the Charter of Fundamental Rights, and compromise dignity, autonomy and integrity. How necessary such splicing, reconfiguring, linkage or mining may be should therefore be subject to rigorous ethical tests.

Data mined from online worlds may be useful in informing decisions about public service provision and society's well-being. But, as a tradable commercial commodity, it gives rise to problems of ownership, litigation, autonomy, dignity and privacy concerns especially regarding future use in full or part with or without the originating citizen's informed consent. The 'right to be forgotten' and measures on e-data ownership after death do not sufficiently tackle the ensuing ethical problems likely to arise. Therefore, a neutral as possible eID enabling citizens to undertake transactions without necessarily being required to reveal more information about themselves than is necessary for that particular transaction may help to safeguard core ethical principles regarding a citizen's right to autonomy, dignity and privacy, for instance.

Baked in ethics

The EU requires the baking-in ethical principles into the design and articulation of artificial intelligence and automated or semi-automated decision making as well as manual processing of personal data. The Use Cases on eCommerce and the airport scenario reveal that different rules apply to eID based transactions in a common physical setting. This arises because of pragmatic and political constraints imposed by real-world contexts, real-time eID development and use. Determining what ethical principles can be realised is problematic and not value-free. In the EU, the rule of law is vital. New rules govern the fast-changing artificial world to whose entry points and services the eID will be crucial. For the Aries project, our baseline must be the ethical principles common to our societies in the EU28.

Applying ethical principles to the design and articulation of eIDs means being conscious of the moral problems and societal or personal biases that are baked into their design (therapeutic, or convenience gains, or generating greater safety certainty). (Rizza & Draetta,2015). It also means being aware of the need to understand what the public interest is; how it can be explained and how it can be realised and protected. It means confronting and going beyond the challenges posed by regulators trying to protect privacy by updating legislation within a context of disruptive learning machines, P2P (peer to peer) exchanges, AI and blockchain approaches to identity. (Yrcan,2016)

If 'learning machines' manage the identity ecosystem (whether it is focused on epayments, e-leisure or other specific issues) the direct role of human intervention inevitably shrinks. This makes it vital to ensure that ethics is central to designing algorithms. This may entail learning from and drawing on privacy assessment initiatives (PIAs), regulations (Prisco,2016), oversight mechanisms, audit, inspection and compliance arrangements and independent scrutiny to ensure accountability and redress.

That in turn means moving from implicit ethical principles of good governance to explicit ones. There has to be transparency of purpose, intent and effect, and openness regarding necessity. This places a premium on minimum disclosure requirements in terms of how algorithms are designed and used, phased and shaped (often by other automated processes). It does not mean simply assuming, especially in the case of eCommerce, that competition and anti-trust legislation, standards and regulations are sufficient to guarantee ethical use.

Accountability cannot be simply construed as an issue of liability for malfunction or misuse. This is why the baking in of ethics, and an ethics audit trail that includes early impact assessments, could help build awareness and appreciation of the real-world need to make accountability citizen-focused. It would also potentially augment designers' awareness of the requirements related to the principles of necessity, and the intended use and effect of using an eID.

Ethical principles have to be reflected in the algorithms designed to facilitate digital society, and hence in automated and semi-automated decision-making algorithms on which humans rely. The design must proceed from the basis of human-user ignorance : citizens may lack the technical skills, knowledge or time to override an algorithm. They may be unaware of, or disagree with, ethical principles they are using. This is illustrated in relation to eID use in self-driving vehicles, for example.

Ethical eID design therefore must reflect and 'bake in' principles of accessibility, dignity, equality and transparency. Ethical design suggests that in practice where eID use fails to be used, for whatever reason, there should be clarity over why this happens and, in order to preserve dignity and accessibility, alternative means of completing an intended benign transaction.

The GDPR Art 22 states that people have a right NOT to be subject to a decision 'based solely on automated processing'.

It is essential to recognise that algorithms are not value-free. Inbuilt are assumptions about the political values and societal norms that affect all aspects of life in a given physical territory. These values, so far, are shaped by human beings. Human beings differ. Diversity is the norm. Different cultures and polities attach different weight to the same principles. The example of privacy is illustrative. Capurro argues that in some societies privacy for one individual is the norm whereas for others disclosure is the norm. Privacy as a value varies over time in terms of how society sees and (ab) (mis)uses it. The adoption of ethical principles and their implementation is likely to be affected, in part, by prevailing privacy rules and laws that are not static. Relying solely on privacy rules and assuming that compliance with them ensures ethical practice is necessary but not sufficient.

2.4 *Broad policy context that conditions proprieties in the evolving eID ecosystem*

In 2017, EU authorities and the European Data Protection Supervisor (EDPS) stressed that ethics were no longer an optional after-thought or add-on. **Ethics is centre stage. Ethics is the first consideration in the design of any app or system.** These may be used across policy arenas whose drivers, purpose and goals vary considerably in scope and intent: the Aries scenarios illustrate this. In the real-world, the scalability of an eID may rely on its cross-sectoral application and relevance. Broad policy contexts that condition priorities will

not necessarily be identical across those sectors. Priorities will differ. What may be acceptable or justifiable in law enforcement/ physical border management may be far from ethically acceptable or justifiable in online commercial transactions.

The problem for designers and developers is that a technical 'solution' tends to be driven by a specific goal or set of objectives taken in isolation from how they may evolve and especially be linked. Linkability raises the ethical stakes. Designers, engineers, stakeholders and developers must be aware of ethical matters, policy drivers and goals as well as the values of society that are to be sustained, or compromised by their envisaged 'solution'. **They must be aware of how these can be potentially undermined by it and, where ethics is centre stage, recognise, identify and make explicit unethical potential linkage and onward use, in order to give effect to the precautionary principle at the earliest possible stage of the evolution of their 'solution'.**

The EDPS clearly stated that organisations must take into account the protection of the rights of individuals, both before and during their processing activities, by implementing the appropriate technical and organisational measures to ensure that they fulfil their data protection obligations. He insists that: technical choices that appear to drive political decisions can never be accepted (EDPS 6 April 2017); the 'main obstacles to a sustainable interoperability arise from the current legal basis of the information systems rather than merely from data protection principles; policy objectives must be specified before the core needs are analysed at all levels to determine the most appropriate technical solutions; and 'knowing that information exists without knowing what to do with it is useless in the decision-making process and contrary to the principle of data quality'.

Reflecting on the concept of interoperability in the field of migration, asylum and security, and the Commission's *Communication of 6 April 2016 on Stronger and Smarter Information Systems for Border security*, the EDPS made clear that **purpose specification and limitation to ensure dignity are critical**. The EDPS underlined the need for 'specifying the ultimate purpose(s) and core needs justifying the use of identity data; and analysing the various options to achieve stated purposes taking into account their impact on fundamental rights as an *important pre-requisite to allow a full assessment of the necessity and proportionality of the solution proposed*.'

The EDPS and Commission reflect the view that data protection and privacy legislation are essential but insufficient to protect citizens' fundamental rights in a digital age. This view challenges some other jurisdictions where disagreements with the EU continue, notably in respect of regulations and legislation.

The Commission also published a draft document on *Principles and Guidance on eID interoperability for online platforms* to encourage the adoption of more secure means of authentication by online platforms, including social media and internet big players. These are relevant to eCommerce as service providers as well as existing IDM platforms, IDPs, Aps and eIDAS for an ecosystem. Aries will in future consider and reflect on how to facilitate this interoperability from the Aries architecture approach and from other perspectives and is aware of how past projects, like the eJustice (2002) programme, inter alia identified interoperability challenges at the judicial levels.

2.4.1 Policy context 1: border security, mobility, biometrics and cybersecurity

The EU's approach to digital challenges and opportunities is increasingly cross-sectoral but not always well-integrated. Several of the issues that arose initially in respect of border management, movements of large numbers of migrants and asylum seekers, spill over into the eCommerce arena. The sectors depend on and use similar, if not the same, technologies. For all, privacy and ethical practice are problematic, ambiguous, fast-changing and complex.

This was illustrated by the tensions over complying with mutually agreed, enforceable privacy practice as illustrated by the tortuous EU-US Privacy Shield agreement. The EU, especially, felt that the Privacy Shield's effect was diluted, partly owing to the absence of a US Privacy Shield chief. The EU increasingly values independent overview to ensure privacy and ethical compliance. By contrast, self-certification is a preferred method for companies in the US to suggest they may be trusted owing to their commitment to privacy. Google and Dropbox, for example, signed up in September 2016, within the two-month window of it becoming operational, thereby avoiding the need first to update arrangements for sharing data with others. The EU's Art.29 Working Party decided against challenging the legitimacy of data transfer arrangements during the first year of its operation although it, and the Hamburg data protection authority, heavily criticised the Privacy Shield. Some months later, EU Commissioner Ansip stated on 26 June 2017 that the EU would update its cybersecurity policy overview by autumn 2017. EU certification and labelling were seen as necessary to boost trust and confidence, themselves prerequisites of ensuring the interoperability of cybersecurity products and services. It was noted that key to maintaining trust in a secure digital ID for eCommerce was strong encryption, effective cyber defence, and no backdoors, as is clear from the eIDAS Regulation (2014).

In September 2017, in an exchange of view with MEPs, EU Commission Dimitris Avramopoulus (responsible for Migration, Home Affairs and Citizenship) underlined that for information to be useful, it had to be inter-operable. He confirmed the need for interconnected centralised EU information systems, compatible with fundamental rights and data protection, especially in real time at the borders. MEPs' concerns over the retention of Passenger Name Record (PNR) data reflect disagreement over the risks to privacy that entails as well as database linkage. Intelligence and information linkage could be valuable, subject to observing ethical practice and legal requirements. Current pilot studies on realising a passport-free, smart gate free, airport (as in Sydney Australia) take database and especially biometric information linkage a lot further and beg numerous ethical questions relating not simply to privacy and autonomy, dignity and fairness but the values prioritised by and underpinning the society that enables such 'seamless' e-digital transactions to occur.

The Aries eID eAirport pilot is aware of the wider ethical scenarios raised by such innovation. (Lodge, 2013a,b; 2012 a,b). Aries recognises, but does not reflect on, either the additional costs of IOP, or on the extent to which existing relational systems are fully used, or whether blockchain (devised for different purposes to identity management and not relying on third party authentication) could be refashioned to help combat fraud at the borders, as some suggest. Instead, the Aries eID addresses in today's world a particularly acute airside opportunity for identity fraud.

The EU's member states differ in cybersecurity readiness and in their vulnerabilities, making all as vulnerable as the weakest link in some scenarios. Consequently, Aries works with different eID solutions informed by the pragmatic perspective of developing an eID that works in conformity with current legislative frameworks, is efficient, user-friendly, scalable and helps to increase citizen trust in, and hence take-up of, eIDs,. **Its ultimate aim is not to trade off security against privacy and vice-versa but to enhance them both simultaneously *while being informed by and respecting ethical principles*.** This is underpinned by the need to synergistically evolve an eID that establishes good practice and identifies pinch points where more effort is needed to advance a multi-purpose, cross-sector, cross-border and interoperable eID.

The immediate context for ARIES is the ever-expanding use of biometric tokens (notably on smart phones) to authenticate a person's claim to be who they say they are.

An eID that is inter-operable, reliable and trustable in cross-sector and cross-border use poses many technical issues. It also must take into consideration the different legacy challenges and the impact of it on socio-legal-and ethical traditions. A particular problem arises from differences which cannot be eliminated simply by uniform EU level legislation (such as the GDPR or e-privacy directive) or BCRs and mutual recognition. Data protection affects all EU policy areas and is key to legitimising and increasing trust in EU

policies and in citizens' claims to be who they claim to be. Both it and biometrics, however, are insufficient in themselves to protect citizens in the evolving eDSM. Exaggerated trust in either to 'solve' challenges arising as apps evolve and e-citizens' digital opportunities increase must be moderated. The context in which they evolved is not necessarily appropriate as a transferable model. This also applies to biometrics, a term that means different things in different jurisdictions.

Biometric eIDs originated in border management scenarios. They are now being extolled for domestic purposes (eHealth, epayments, and eleisure). The immediate context and demonstration scenarios are driven by the concerns for the evolution and realisation of the potential of the Digital Single Market. This is set within the wider strategic EU plan to realise a 'Security Union'. Whereas in the past the two areas have been somewhat artificially compartmentalised in EU policymaking, their inter-linkage is now made explicit by the EU.

A security union therefore has meaning in terms of combating fraud and ID theft for domestic, personal purposes in the daily environment of the citizen. It has a more generic meaning in terms of security for the purpose of maintaining the integrity of territory against external threats. Now this is tied to new developments in border management, action to combat international crime and terrorism, critical infrastructure protection, crises, general eID roll-out, and entry and exit monitoring for people and goods crossing physical, air and sea borders. In July 2017 the EU Asylum Support Office (EASO) became the new EU Agency for Asylum to assist Member States in crisis situations, to monitor compliance with EU legislation, strengthen the Common European Asylum System and advance the Blue Card and other key LIBE files. (http://www.europarl.europa.eu/cmsdata/123686/libe-newsletter-july2017.pdf) The European Public Prosecutor's Office will also play an important role as will associated agencies and operational units.

The issue of fake identities has particular salience in the above scenarios. It continues to preoccupy the security agenda. During the Hearing of 29 May on the report of the High final report Level Expert Group ("HLEG") on Interoperability[2] Commissioner Julian King explained that the primary objective is to fight against aliases and fake identity with the objective to improve quality and usability of data currently collected. Further analysis is required by the Commission and eu-LISA before new measures are transposed into legislative proposals. (HLEG,2017)
http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.).

Whereas security tended in the past to be associated with managing and securing physical state borders, now cyber-security presents other and additional threats to both physical and virtual borders. This is outside the scope of this project but the background and developments are outlined below to illustrate how *ad hocism* rather than a coherent overall strategy shaped today's context for understanding the probability that citizens will use and trust interoperable eIDs.

Aries is aware of the EU's cyber security strategy and policies. They form the general context for the development of a tool for the citizen designed to assist in securitising the citizen's identity.

Briefly, the EU's cyber security has been established since 2013 through the EU Network and Information Security agency (ENISA); Europol's European Cyber Crime Centre (EC3), the EU Computer Emergency Response Team (CERT-EU) and European Defence Agency. The EU's cyber security policy has five main priorities: (i) build resilience for information security; (ii) combat cybercrime; (iii) cyber defence; (iv) fostering industrial and technological resources; and embedding EU values in its cyberspace policies. This complements the Directive on Attacks against Information Systems and the Network and Information Security Directive (2016). The latter aims to enhance the preparedness of member states to: (i) respond to cybersecurity incidents via a Computer Security Incident Response Team (CSIRT) and competent national NIS

[2] The high-level expert group on information systems and interoperability was set up under Commission Decision C/2016/3780 of 17 June 2016 setting up the high-level expert group on information systems and interoperability

authorities; (ii) support strategic cooperation and the exchange of information on specific incidents and risks; and (iii) identify and encourage cybersecurity among critical infrastructure operators, including the introduction of reporting obligations for incidents. (EDPS, 2017a, Tasheva,2017) Cooperation to combat, investigate, educate the public, stakeholders, investigate incidents and enforce the law has progressed but there is still much to do.

The relevance of policy to combat cyber-security threats must not be under-estimated. ENISA's (2017) needs and gaps analysis identified four urgent priorities:

- Cooperation across Member States in matters related to cybersecurity
- Capacity to prevent, detect and resolve large scale cyber-attacks
- Cooperation and information sharing between different stakeholders, including public-private cooperation
- Protection of critical infrastructure from cyber-attacks

Both in administering these and in any H2H, M2M, H2M interaction, the authentication of the legitimate claim will become increasingly vital.

Governments are likely to continue to focus public attention on border security but for the citizen, these issues are somewhat intangible and transient. More tangible and visible are practical day-to-day issues of conducting e-transactions anytime, anywhere using an eID access to services, facilitated by mobile technology. The overlap between the two sectors is pervasive and informed by the history of the EU's evolution. This cannot be ignored if the emergent themes in the evolving policy context against which eIDs are rolled out is to be understood and used to develop sustainable, trustable, reliable eIDs for citizens
Border security itself is embedded in a broader and older European policy context of cross-border counter-terrorism cooperation. That predates the Single Market but was spurred on by its three pillars to widen the scope of supranational integration to policy areas previously deemed the sovereign prerogative of member states (borders, defence and judicial affairs). They were recognised and deepened in subsequent treaty revisions from the time of the Maastricht treaty (1991) onwards. (Lodge 1986,1992) German unification, the disintegration of the USSR and the broadening membership of the EU in the 1990s, also meant that the EU's physical external land borders became longer and included more sea areas. International crises also impelled EU action on migration, defence and rapid reaction capabilities. The Schengen zone became increasingly automated and continues to adopt technologies based on biometrics which have caused tension in reconciling EU liberties taken for granted with increased threats loosely grouped under the banner of security.

Identity documents (such as passports, ID cards, travel documents and machine-readable travel documents) grew in importance. The ability to verify and authenticate claimed identities as genuine matches to a genuine person assumed prominence as automatic processing and ICT advances to combat fraud and impersonation became to be seen as useful tools against international organised crime, terrorism, people smuggling and illicit trade in goods and substances. The more biometric identity documents were advocated by governments, public administrations and the private sector as necessary to combatting terrorism and security threats, the more the associated claims were scrutinised. A balance between privacy and security was initially seen as a trade-off rather than as part of a continuum (eJustice, r4eGov, Elise, Challenge projects). Citizen acceptance of biometrics was initially clouded by fears over the security of the technology against fraud, spoofing and impersonation.

Biometric eidentity documents and procedures were also seen as part of the evolution of Big Brother surveillance societies. It was perceived to be intrusive (in terms of enrolment procedures, as for example at embassies and consular offices for passport and visa renewals), authentication (such as body scanner at airports, and digital photograph requirements regarding whole face disclosure). It was also seen as potential divisive (digital divide where only the educated and wealthy might be able to afford the services enabled by

the biometric eID, such as travel), discriminatory (in allowing automated sifting according to predetermined criteria such as race, age, disability, background intelligence etc.), undignified (in being counter to some cultural practices, such as the burka), an infringement of human dignity (in exposing disabled people's incapacities to enrol for say iris recognition, or owing to metal prosthetics).

As ICTs advanced and biometrics were used for more domestic purposes (tracking in dementia homes, for example), eHealth, barcode chip implants, tracking of goods, chemicals etc., biometric identity algorithms became more widespread, especially in the financial sector. Whereas they all rested on the probability of a match between an eidentity and a physical live person, what specific characteristic(s) of that person should be recorded or stored led to citizen concerns that citizens were all suspects now; or rather that those citizens known to the state (because they had a birth certificate from a public authority, a rarity in over 70% of the world) could now be tracked and treated as suspects. (Lodge, 2007).

It was not just citizen scepticism over the ever-expanding purposes to which their information could be put that persuaded private sector developers to broaden their business models to eCommerce. Rather, difficulties in funding the wide and expensive roll out (from SIS to VIS II, for example, as well as AFIS and APNR) and complications from legacy documents and technologies, suggested that older developments designed for passports and border management could be used for virtual borders for all manner of transactions, notably in the delivery of egovernment and public services.

The Single Digital Market is more than the EU expression of this trend. It is the technological expression of the Single European Market. As such, legislation has been advanced by the EU since the 1980s in response to increasing innovation and digitisation. It is important to note that the EU applies to the ESDM principles such as non-discrimination, mutual recognition, inclusion, and upgrading the common interest (including higher standards) developed for creating and sustaining the internal market. Accordingly, diversity in practice, differentiated identity assurance levels and technology are to be accommodated providing the overarching principles and goals are addressed appropriately, and technological neutrality is upheld.

This is illustrated by art 8 of Regulation(EU)910/2014 as follows:

1. Article 8 Assurance levels of electronic identification schemes 1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.
2. The assurance levels low, substantial and high shall meet respectively the following criteria:
    a. assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
    b. assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
    c. assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

The EU acknowledges that its legislative framework needs to be adaptable and flexible to accommodate the speed of technological innovation. Accordingly, priority is given to facilitating convenient and efficient (ie speedy) access to services undertaken by organisations and especially by citizens as customers undertaking online transactions. This more 'domestic' focus to digital life and identity assurance complements but does

not supplant eborders. The reservations among citizens in respect of both (outside the scope of this brief) remain valid.

2.4.2 Policy Context 2: the Single Digital Market and eCommerce

The EU is committed to realising a Single Digital Market, complemented by advocacy of technological neutrality, strong privacy protections and respect for ethical principles. Its eGovernment Action plan 2016-2020 underlines the importance of accelerating the digital transformation of government. (COM (2016) 179 final). The Commission estimates that a fully functional digital market could contribute €415 bn per year to the economy. Mobile technology was estimated to account for 3% of EU GDP, worth €500bn in 2014 (GSMA). The EU Commission estimates that only 7% of small and medium-sized businesses in the EU sell cross-border and argues that putting the single market online can change this. It aims 'to create a digital single market where the free movement of goods, persons, services, capital and data is guaranteed — and where citizens and businesses can seamlessly and fairly access online goods and services, whatever their nationality, and wherever they live.' (https://ec.europa.eu/commission/priorities/digital-single-market_en).

As in the case of creating the four freedoms of movement (of goods, services, persons and capital) in 1992 to realise an internal borderless Single Market, technical, legal and regulatory practices in the EU28 are seen to obstruct the scaling up of the EU's digital market potential.

This was emphasized by the European Council in October 2017. Indeed, the potential for going digital was highlighted when on 25 October 2017 the first ever digital signing of an EU legislative act took place in Strasbourg. EP President Antonio Tajani and Matti Maasikas, of the Estonian Presidency of the Council, signed electronically the revised regulation on security of gas supply, paving the way for its entry into force. As the President stated the EU institutions are working together to make **digital transformation** a reality, illustrating the **EU's commitment to implementing "eIDAS"**, the EU-wide regulation which provides for a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. (http://www.consilium.europa.eu/en/policies/digital-single-market/), and which (under Article 11 on liability) stresses liability for intentional or negligent processing in a cross-border transaction. However, Article 13 places the burden of proof on the natural or legal person claiming damage and this remains problematic in terms of accessibility, time, cost and inconvenience. Penalties are to be 'effective, proportionate and dissuasive' (Article 16).

While online transactions continue to grow, direct cross-border eCommerce – without an intermediary such as Amazon, for instance – encounters barriers. These barriers are technical, language-related, and reflect anxiety over the trustability of the transaction process itself as well as the trustability, (including liability and related issues) of an unknown supplier outside the state of residence with which a customer may be familiar. In addition, cross-border interoperability of user authentication and verification has yet to be achieved: public services and the private sector rely on and use different legacy and new technologies and different biometrics. Using biometrics to boost trust in the eID seems less persuasive than advocating its convenience to boost citizen uptake. However, intrusion and theft deter and inhibit trust (HID, 2017) so industry has also to focus on how to combat intrusion, fraud and theft of data that include biometrics by making the biometric unusable to all but the legitimate, original, genuine person.

The EU has boosted R&D, and innovation. It has taken steps to remove barriers which restrict access to goods and services. Its 2016 report noted that:

- only 15% of people shop online from another EU country
- Internet companies & start-ups cannot make full use of online opportunities
- only 7% of small businesses sell goods or services across the EU's borders
- private and public sectors, governments and commerce are not sufficiently using and benefiting from digital tools

The EU's commitment to creating a *digital by default* society relies on progressing interoperability, cross-border and cross-sectoral transactions, the principle of once-only data entry and building in interoperability, trustworthiness and security by default and design. eIDs are seen as one of the important technical solutions to facilitating acceptance of those principles and using interoperable solution for public administrative purposes as well as private transactions. Context aware personal data management and trustworthy data practices are seen as vital to allow citizens to control access to and use of personal data, to develop and maintain personal autonomy and develop their identities. These views pervade the digital agenda and ethical assumptions underpin them.

In January 2017, the Commission published its *Citizens Report* which stressed the idea of a once-only enrolment of personal information for citizens seeking to use public documents regardless of where, in the EU, they happen to reside. The strong focus on convenience for citizens coupled with realising the anticipated benefits of the single Digital Market is prominent. (Citizens Report:24ff, 2017) On 10 January 2017, the Commission took steps to realise a service economy that works for Europeans by providing better online protection and new business opportunities. The ePrivacy Regulation updates the older Directive. It extends guarantees to e-communications, content and meta-data. The new draft Regulation includes the principle that consent will be required to access information on a user's device (terminal equipment), except for non-privacy intrusive cookies, such as those for recalling shopping cart history. This is important for eCommerce. However, unsolicited communication is ruled out. The aim is to guarantee the privacy of personal data and communications on social media and all e-communications whether processed automatically or manually. Such data processing by EU institutions is also covered. International transfers of personal data are also covered in a Communication.

The European Parliament is vigilant in this respect. Its Committee on Civil Liberties, Justice and Home Affairs commenting on a draft proposal for a new Regulation on Privacy and electronic Communications recommended enforcement of end-to-end encryption on all communications and a ban on back-doors, to protect EU citizen's fundamental right to privacy under article 7 of the EU's Chart of Fundamental Rights. It prescribes a right to personal privacy, as well as privacy in family life and at home. This includes, according to the Committee, privacy of communications between individuals. It stated: The principle of confidentiality should apply to current and future means of communication, including calls, internet access, instant messaging applications, e-mail, internet phone calls and messaging provided through social media. (LIBE report 2017).

The EU's rules are important considerations because agile eCommerce and customers' simultaneous multiple-channel use to research, shop, browse and buy online provides a resource for data mappers, harvesters, analysers across mobile and non-mobile channels, data resellers, ad targeting and ad tracking, even within one website or company. The seamless experience is seen as a driver of eCommerce in the US. (Oracle,2016) At the same time, the impact of the collaborative economy and blockchain are only beginning to be appreciated and inserted into deliberations by legislators. The Commission will make full use of alternative mechanisms under the General Data Protection Regulation (entry into force 25 May 2018) and Police Directive to facilitate the exchange of personal data with third countries with whom adequacy decisions cannot be reached. Bi-and multilateral steps will continue to promote the highest data protection standards. As ever, the pace of digital innovation far outstrips the capacity of lawmakers to devise and approve appropriate legislation. It is not surprising, therefore, that there is a tendency to rely on complying with privacy related rules and assume that it can be safely inferred that all obligations have been met. They have not. Cross border trade raises numerous additional problems. 'Solutions' may be feasible that are not necessarily fully compliant with ethical principles and practice. It is important to be aware of this tension and to address it from the start.

An ethical impact assessment may avoid high costs further down the line. An illustration of the scope for problems is revealed by the package of measures to cut barriers and costs for business providing services

across borders (representing 80% of the UK economy alone) launched under the Digital Single Market. A new 'e-card system' is designed to provide a one-stop shop for providers of a wide range of services to register in their own country to provide services abroad. The host will decide whether or not to accept applications in line with EU and national law. Highly sensitive services (health, legal services, transport and some others) are not eligible and will be subject to additional controls and are ruled out. The need for impact assessments, including application of the necessity and proportionality tests common to ethics codes, is advocated.
The relevance of these new measures to ARIES lies in the potential for different legal rules to apply in a single physical space that is an ARIES airport use case.

The Use cases for the Aries project link eID use where high confidence in authenticity is required (e-Airports) and where lower authenticity is common (eCommerce). There are several cross-cutting themes and generic issues linking both. However, the EU has a tendency to a silo mentality: it puts areas in boxes. While administratively this may be necessary, it does not assist linked-up policymaking where this would be beneficial and enhance effectiveness. For example, the recent 2016 proposal for a Regulation on updating SIS (COM(2016)883 final, p.5) calls for end-to-end SIS information exchange and thorough security assessment, based on ETIAS, using EU-LISA and including fitness checks on existing legislation, stakeholder consultations (p.9), parallel searches and biometric data processing (p.24). All have echoes in ecommercial and potentially other sensitive environments where possibly different approaches to alerts, access and retention, flagging, data protection, privacy and ethics may apply even though identical or similar eIDs are to be used. Customs checks, for example, cross over into eCommerce practice.

In 2016, the European Parliament reported on a European eID. It focused on the potential societal impact an eID could have. It concluded that the European added value of an eID was ambiguous. It argued that citizens needed to directly experience the 'strong advantages' that an eID could have on simplifying administrative burdens, travelling and cross-EU mobility. (European Parliament, AFCO, 2016:40). Political will, data protection and eID linkage and compatibility with legacy national systems were identified as potential barriers to swift uptake. (ibid:45) The minimum requirements needed to facilitate cross-border interoperability and an interconnected electronic service (including e-Trust services (-eTS)) were seen as: organisational, semantic, technical and legal. (ibid:51)

3 ARIES use cases: Challenges of eCommerce and eAirport

eCommerce exemplifies an arena where citizen interests and industry business models, including those driven by the disruption imperative of innovation, collide and mesh. Citizen ambivalence and confusion over what privacy means, its necessity or dispensability, its protection and sustainability, are pronounced (Satori 2017). For many, ethical considerations are secondary considerations or even an after-thought. Speed and convenience in proving who they claim to be are powerful drivers for citizens

The EU has looked at barriers to eCommerce growth from the perspective of the consumer as well as that of the conditions necessary, but not sufficient, for growth. It has done so from the perspective of the **citizen as consumer**, that of the **citizen as a business developer**, and that of the **regulatory environment**. This has been complemented by steps to advance technical solutions to create **resilient credentials and dependable eIDs**. Attention to the **barriers to eCommerce** generally have also been addressed.

The imperative of eCommerce derives from the business model premise that a commodity or service or product must be profitable. Maximizing commercial gain is the driver. Compliance with regulations and legal rules is accepted as a necessary precondition of developing and sustaining trust in the supplier and goods or services being sold. This itself underpins an implicit ethical consideration common to industry which derives from the precautionary principle: businesses know that reputational damage and possibly financial losses could arise if their businesses do adhere to regulatory standards and norms, especially those designed to prevent avoidable harms to citizens. That applies to data management, storage, onward use, security and privacy practices. This is reinforced by the Draft Opinion of the European Parliament in September 2017 (Towards a digital trade strategy (2017/2065(INI)). It:

1. Stresses that any European digital trade strategy or provisions for cross-border data flows and agreements on a free flow legal provision should fully respect the EU data protection acquis and comply with EU fundamental rights standards;
2. Advocates the use of all instruments provided for under the GDPR, while acknowledging the fact that EU rules on the transfer of personal data may prohibit the processing of such data in third countries if they do not meet the EU adequacy standard;
3. Underlines the need to tackle all forms of digital protectionism, including unjustified data localization requirements, as such protectionism is contrary to the EU's data protection rules;
4. Urges the Commission to act as the benchmark for setting high data protection standards on data flows at international level and to consult the appropriate EU data protection institutions and bodies during the negotiation process of international or trade agreements that may potentially impact data protection.

The monetarisation and commercialisation opportunities arising from collecting both trivial anytime anywhere data as well as mining Big Data do pose serious privacy and ethical questions.

Global retail sales are expected, according to some estimates, to reach €23.6 trillion by 2020 (Wallner, magazine.startus.cc 04/07/2017). Accordingly, technical innovation to exploit these proceeds apace to produce new algorithms, or combine common technologies (wifi, Bluetooth, geofencing). Associated marketing focuses on persuading potential customers that online shopping, on-demand delivery, and more eCommerce yield time, convenience and efficiency gains, especially for customers with access to mobile platforms. Sensor fusion, deep learning algorithms and computer vision have been harnessed (magazine.startus.cc 5/7/2017) Ad tracking is commonplace, if increasingly controversial: some businesses now target customers with online ads based on their real-world activity (that the ePrivacy draft Regulation seeks to protect). Online platforms facilitate the collation of Ad-IDs of any customer group based on geolocational and behavioral criteria, including contextual data, online ads and conversion level of ad to real

customer. Offline sellers can obtain information about their preferred would-be customers in their own store or nearby and create personalized marketing campaigns to boost sales.

The associated eCommerce potential is obviously valuable to sellers but potentially breaches citizen privacy, dignity, autonomy and many ethical principles, such as purpose minimisation and purpose limitation and specification. The practice of collecting 'everything' itself is valuable **if it can be linked to other data**. (e.g. Cluify use explained by CEO of Polish Datarino (Edward Mezyk) in interview(Wallner). While this benefits the potential market share of a retailer, it has serious implications for society. The convenience or irritation an individual citizen may experience from this is a secondary consideration for marketing. Someone out for leisure purposes does not have the opportunity, for example, to consent directly to any of this. From the point of view of PbD, PETs and ethical practice, questions must be asked: should this be legitimate and unregulated? How does this impact fraud? That question also applies to private sector and public sector bodies that exploit private sector re-use of digital identities. (Open Identity Exchange, 2017). In the UK, for example, reuse of a government endorsed digital identity is expected to modernize online customer verification for financial services. However, the EU Commission in October 2017 proposed a Directive designed to combat fraud and counterfeiting of non-cash means of payment (COM(2017)489) and sought public feedback on this. Its primary concerns relate to the threat to security arising from fraud and to the integrity and future of the digital single market. [See annex 3]

There is growing awareness and tension among legislators, consumers and business over what practices are ethical and legitimate, and what should be prioritized – commercial gain or citizens' rights not to have their data commercially accessed and exploited without explicit and full consent.

3.1 *eCommerce in society: concerns, impact and key barriers*

At the level of society, government and the individual citizen, there are many technical, financial and legal barriers to engaging in eCommerce. At the level of government and society, they cover infrastructure, terrain, access to services, financial capacity and technological readiness. At the level of the citizen, they include issues arising from the tension between the citizen who wants agile anywhere anytime access (to eCommerce and e-services on mobile devices that are the most convenient way to do an e-transaction), and concern over the trustability and security of a service or goods vendor against fraud and intrusion along the chain. Member states vary in the extent to which citizens engage in eCommerce already.

At all levels, there is a more general barrier of awareness and capacity to access and use such services. This is not restricted to citizens, but is common to government and private sector providers as well.

There is also a 'public awareness and understanding lag' (PAUL) of Fintech and AI's transformative impact on the conduct of public life and service delivery. Again, this is something the European Parliament's reflections on reinforcing ePrivacy in October 2017 begin to address under the rubric of 'personal communication' mechanisms. However, reflection must not stop there: when learning machines take decisions that affect the human, the issue of acceptability becomes obsolete. Trust becomes more important: potentially the service deliverer most able to preserve and protect the integrity of a person's identity will become crucial to adoption and sustainability. This is something the Aries Focus Groups and questionnaire tested.

3.2 *Definition and segmentation of eCommerce*

The following section discusses the main barriers that hypothetical clients might face when adopting eCommerce as a way of acquiring goods or services. The main eCommerce business models will be described as well as the different barriers for the adoption of eCommerce.

In its broadest sense, eCommerce concerns any commercial transaction between a supplier and a customer via electronic means. However, it is possible to segment eCommerce by type of entity that supplies the customer with the good or service, as follows:

- **Business-to-business** - Business-to-business eCommerce comprises every electronic transaction of goods or services done between to enterprises. In this type of eCommerce, the transaction is usually done between the producer and the retailer.

- **Business-to-consumer** - The commercial relationship is between the company and the final consumer. This is normally adopted by traditional retailers who want to acquire an extra sales channel to get their goods or services to their customers, and is probably the most common type of eCommerce. When compared to traditional retail, the customer usually has more information about the product or service and an underlying assumption is that this is cheaper without compromising personal service and the speed of delivery.

- **Consumer-to-consumer** - This type of eCommerce comprises every transaction between two consumers through electronic means. These transactions are often done with the support of a third entity that provides the electronic platform.

- **Consumer-to-business** - This business model is a complete reversal of the Business-to-consumer business model in the sense that in this case, the consumer supplies business with goods or services. The advent of this type of business model is mainly due to:
    - The lower cost technology that provides individuals access to technology that was once only available to large companies;
    - the opportunity to connect large numbers of people in a bidirectional network that were once a one direction relationship.

This type of eCommerce is usually associated with crowdsourcing where individuals offer their goods or services to be acquired by companies.

- **Business-to-government** - Comprises every transaction between a company and the government through electronic means. It can cover a great diversity of services and trade of information, regarding taxes, social security, employment, etc.

- **Government-to-business** - Refers to every electronic exchange of information between business and government. In G2B, government agencies and business use websites, procurement marketplaces, applications, web services.

- **Government-to-citizen** - This type of eCommerce includes any activities performed between Government and its Citizens or consumers namely paying taxes registering vehicles or providing information and services. It has also been depicted as eAdministrative or eGovernment service delivery in partnership with a private sector third party.

3.3 *Barriers to digital transactions*

3.3.1 Business to business

Internal barriers to the adoption of B2B e-commerce by SMEs relate to individual and organizational barriers (See study on Indonesia by Irma Janita et.al). External barriers relate to technology, market & industry, external support and government support.
The following table groups the main barriers when it comes to the adoption of B2B e-commerce regarding their type and category.

Category	Type	Description
Internal	Individual	Owner-managers attitude towards e-Business
		Benefits of implementing e-Business to the organization
	Organizational	Knowledge of adopting e-Business
		Expertise in ICT
		Organization culture and technology penetration
External	Technology	Technology penetration in the country
		The availability and affordability of the technology in the country
		Technology to support e-Business
	Market and Industry	The adoption of e-Business by supplier and buyers
	External Support	The number of IT service provider or consultant
		The awareness of those IT service providers and trust of the providers
	Government Support	The number of Telecommunication providers and supports
		SME's awareness of Government e-Support
		SME's perception of Government e-Support
		Government initiatives towards the implementation of eBusiness
		The availability of research centers to support e-Business learning
		Regulation and policies for e-Business

Table 1: Barriers to the adoption of B2B eCommerce

3.3.2 Business to consumer

A research done in 2012 by Santiago Iglesias et. Al was able to segment the non-shoppers in B2C e-commerce by characterizing them with the main barriers that would prevent them from shopping online and the drivers that might encourage them to start shopping online. That being said, 47% of the 1449 B2C e-commerce non-shopper individuals that participated in the research belonged to the Skeptical/distrustful non-shoppers group whose main barriers preventing them from shopping online regard their safety in terms of overall perceived security, personal information and payment methods.
The other two main barrier based non-shopper customer segments were the “infrastructure-conditioned” (18,7%), who highlighted the lack of internet connection and their perceived cost of shopping online as the main barriers to shop online, and “product-conditioned” (15,7%) who pinpointed the product and shipping

costs as well as its availability as being the main impediments for shopping online. Regarding the drivers that might encourage non-shoppers to shop online, the authors were able to identify five different main segments. The first and largest group identified (38%) were the "risk-avoiders" which stated that they would start shopping online if there was a significant improvement in the safety of online transactions, if less personal data was required, if they had more paying options or found cheaper products online.
Another relevant group for this purpose were the "Hesitant non-shoppers" (7,8%) which highlighted similar motivations that would encourage them to start shopping online as the "risk-avoiders" but in this case they also pointed the easiness of use and that fact that they would start shopping online if they knew the seller better.

3.3.3 Consumer to consumer

Trust in e-commerce has been defined as the belief that the other person will behave in a socially responsible manner, fulfilling expectations and not taking advantage of vulnerabilities, (McKnight et al, 2002) (Pavlou, 2003), and has been cited as a key determinant in adoption of e-commerce (Holsapple et al, 2005) and in purchase intentions via the web (Goles et al, 2009). As for risk, it regards the inherent risks in the online transaction which can include concerns about fraud or lack of product delivery, like trust, it has been found to negatively influence the consumer attitude towards using C2C e-commerce. With this in mind, Lori N. K. Leonard in 2014 developed a study about attitude influencer in C2C.
The hypothesis behind the research was that the trust in seller and the risk of seller would affect the attitude of the buyer towards purchasing, and that, the trust in the buyer as well as the risk of the buyer affect the attitude of the seller towards selling in C2C e-commerce. The research was based on a questionnaire made to both buyers and sellers in C2C e-commerce in which these could mirror their level of agreement with the statements shown.
The statements asked to participants of the questionnaire regarding trust and risk as influencers of buying and selling through C2C e-commerce can be seen in the following tables:

RISK
As I consider purchasing a product through C2C electronic commerce, I become concerned about whether sellers will commit fraud.
As I consider purchasing a product through C2C electronic commerce, I become concerned about whether sellers will deceive.
As I consider purchasing a product through C2C electronic commerce, I become concerned about whether sellers offer products that will not perform as expected.
As I consider purchasing a product through C2C electronic commerce, I become concerned about whether sellers will behave opportunistically.
TRUST
Sellers of products in C2C electronic commerce are in general dependable.
Sellers of products in C2C electronic commerce are in general reliable.
Sellers of products in C2C electronic commerce are in general trustworthy
ATTITUDE
I am optimistic regarding buying a product using C2C electronic commerce.
I am optimistic regarding buying a product using C2C electronic commerce.
I think it is a good idea to buy a product using C2C electronic commerce.

Table 2: C2C eCommerce; attitude toward purcharsing factor analysis

RISK
As I consider selling a product through C2C electronic commerce, I become concerned about whether buyers will commit fraud.
As I consider selling a product through C2C electronic commerce, I become concerned about whether buyers will deceive.
As I consider selling a product through C2C electronic commerce, I become concerned about whether buyers will not pay for products as expected.
As I consider selling a product through C2C electronic commerce, I become concerned about whether buyers will behave opportunistically.
TRUST
Buyers of products in C2C electronic commerce are in general dependable.
Buyers of products in C2C electronic commerce are in general reliable.
Buyers of products in C2C electronic commerce are in general trustworthy.
ATTITUDE
I am optimistic regarding selling a product using C2C electronic commerce.
The thought of selling a product using C2C electronic commerce is appealing to me.
I think it is a good idea to sell a product using C2C electronic commerce

Table 3: C2C eCommerce; attitude toward selling factor analysis

The results of this study indicated that a buyer trust in the seller and risk of the seller influence the attitude of the buyer to purchase through C2C e-commerce. Given the factor analysis results, trust and attitude are combined into one factor. Regarding the seller's trust/attitude toward selling is not influenced by risk in the buyer. This finding means that a seller in C2C e-commerce is not worried with, or is unaware of, any risk. This finding might be explained by that fact there regardless of the method of C2C e-commerce, the sellers are utilizing a reliable payment mechanism which might bring a greater sense of security to the buyer.

3.3.4 E-Government

Even though it is known that the data collection and transmission is less costly when using e-Government and that the benefits that arise from adopting this infrastructure range from the improvement in processing tasks and public administration operations to the improvement of the business processes and services, there are number of barriers that restrict the adoption of eCommerce. These barriers were organized into five large groups: (1) IT infrastructure; (2) security and privacy; (3) IT skills; (4) organizational issues; and (5) operational cost, Zakareya Ebrahim and Zahir Irani (2005). Some examples of barriers that comprise these five large groups can be seen in the following table.

Barrier Dimension	Examples	Reference
IT infrastructure	Shortage of reliable networks and communication	Dillon and Pelgrin(2002) Heeks (2001) Fletcher and Wright (1995)
	Inadequate network capacity or bandwidth	
	Lack resources standards and common architecture policies and definitions	
	Existing systems are incompatible and complex	

	Existing internal systems have restrictions regarding their integrating capabilities	Layne and Lee (2001) McClure (2000) Moon (2002) NECCC (2000) Themistocleou and Irani (2001)
	Lack of integration across government systems	
	Integration technologies of heterogeneous databases are confusing	
	Lack of knowledge regarding e-government interoperability	
	High complexity in understanding the processes and systems in order to redesign and integrate them	
	Lack of enterprise architecture	
	Availability and compatibility of software, systems and applications	
	Lack of documentation especially in the case of custom systems	
Security and privacy	Threats from hackers and intruders	Gefen et al. (2002) Lambrinoudakis et al. (2003) Joshi et al. (2001) NECCC (2000) Robins (2001) Zeichner (2001)
	Threats from viruses, worms and Trojans	
	Absence of privacy of personal data	
	High cost of security applications and solutions	
	Unauthorised external and internal access to systems and information	
	Lack of knowledge for security risks and consequences	
	Assurance that transaction is legally valid	
	Lack of security rules, policies and privacy laws	
	Inadequate security of government hardware and software infrastructure	
	Lack of risk management security program	
	Unsecured physical access to building or computers rooms	
IT skills	Lack of IT training programmes in government	Bonham et al. (2001) Heeks (1999 Ho (2002) Layne and Lee (2001) NECCC (2000)
	Shortage of well-trained IT staff in market	
	Lack of employees with integration skills	
	Developing web site by unskilled staff	
	Unqualified project manager	
	Shortage of salaries and benefits in public sector	
	Flow of IT specialist staff	
Organizational	Lack of coordination and cooperation between departments	Burn and Robins (2003) Heeks (2001) Lenk and Traunmuller(2000) Li and Steveson (2002) Themistocleous and Irani (2001)
	Lack of effective leadership support and commitment amongst senior public officials	
	Unclear vision and management strategy	
	Complex of business processes	
	Politics and political impact	
	Cultural issues	
	Resistance to change by high-level management	

	Time consuming for reengineering business process in public organizations	
Operational cost	Main supply come from central government	Bonham et al. (2001) Heeks (1999) Irani et al. (2003) NECCC (2000) Palvia et al. (1994)
	Shortage of financial recourses in public sector organizations	
	High cost of IT professionals and consultancies	
	IT cost is high in developing countries	
	Cost of installation, operation and maintenance of e-government systems	
	Cost of training and system development	

Table 4: E-Government; barriers to the adoption of eCommerce

3.4 *Barriers to the adoption of eIDs for eCommerce*

How obstacles can be overcome will depend, in part, about how effective interim technology is able to overcome existing barriers. There is a place for the kind of Fintech podcasts (such as those provided by American Banker) to raise awareness among industry professionals. But as yet the public and many governments are insufficiently knowledgeable or aware. Governments need to be better informed about future developments in order to plan better the distribution of limited public resources. Fintech, AI and agile e-service delivery based on agile e-identity management threaten to exacerbate existing societal divisions and compromise 'privacy' and associated fundamental rights.

eCommerce cannot be separated from Fintech developments that are largely invisible to the public. However, those that are visible or vaguely perceived by the public constitute potential barriers to public adoption of eCommerce. They crystallize around the concept of identity and Aries focuses on those. Existing barriers cluster around user interface issues and citizen mistrust.

User interface issues are related to ease of use of, and accessibility, to devices facilitating agile eCommerce transactions. Barriers to use may be age and education related. It is not universally true that older generations are the most reluctant to use eCommerce and most distrustful of the technology.

Mistrust centres on fraud and identity theft. Suspicions relate to sharing personal data that may be linked, used improperly or accessed by too many other people; the loss or theft of debit and credit cards, and purchasing history accessible using them fraudulently by unknown others. There is also reluctance to use ecommerce and especially ebanking owing to publicized denial of service attacks, associated fraud and feelings that transactions are insufficiently secure.

Biometrics is typically seen by vendors as a way of overcoming customer reluctance to use apps that rely on remembering passwords. They are sold as a way of providing both citizens and vendors of goods and services with greater reliability in the trustworthiness of transaction being undertaken. Biometric apps are advertised in tempting ways and the market for them is expected to grow exponentially again over the next few years. But there are significant risks that their reliability and trustability are exaggerated. (Biometrics Institute; Lodge,etc).

Suboptimal security and privacy may be marketed by businesses and services keen to persuade reluctant users of eIDs to do so. While voice banking, e-shopping and iris checkout are innovative uses of biometrics, they are not fool-proof.

Moreover, ethical issues are raised by any e-transaction that relies in full on them. Whether it is possible to instantiate ethics in code and encode ethics into decisions relating to the e-transaction is open to question. In Fintech, many decisions are machine led: e.g. e-histories of individuals' personal finances can be compared by companies considering, for example, insurance, banking, purchases on credit cards and mortgage lending.

3.5 *Societal concerns – real barriers to adoption: fraud and data loss?*

To explore citizens' perceptions as to contemporary concerns over eCommerce, Aries use cases were informed by an appreciation of current evidence identifying possible factors that may inhibit the uptake of eIDs, especially in the retail sector. Among them fraud, identity management and perceptions of the relative security of mobile payments were prominent.

Starting from the perspective of business, procurement and eCommerce eIDs are believed to be key to boosting citizens' engagement with eCommerce which is expected to grow significantly by 2020.

Growth of 7% between 2016-2020 is also anticipated in respect of eIDs for the military (Lee, 2016a), access to buildings and cars, as well as sensor-cards to manage remotely on mobile devices smart homes, wearables and the IoE. (Hoikkala & Magnusson). Biometric authentication is also used to monitor workforce activity with view to combating and detecting potential loss in income: McDonald's uses one such system for point-of-sale monitoring in place of passwords. (Lee, 2015).

Business sector analysts have suggested that multi-channel mobile epayments and ecommerce endanger market share for companies unable to see or adapt to security needs swiftly. (Taylor, 2016:159-177). Major public-sector organizations that lose citizen data or whose systems are subject to DDoS attacks or intrusion may be subject to fines from public watchdogs. Public confidence may decline in watchdogs having sufficient power to sanction effectively companies and governments for poor practice, and for very tardy notification of breaches or data loss. Where the government has a dominant stakeholder interest, it may decide that the risks associated with data breach/fraud/loss are acceptable or bearable with the result that they may not sufficiently protect their systems against events that potentially cause citizens harm. (One such example could be the UK National Health Service data theft, 2017). Or more cynically, the conclusion may be that redress is such a protracted, time-consuming, expensive business as to deter citizens from seeking it. That might be seen as an unethical or cynical position to adopt as it also undermines core ethical principles. It implies that observance of the ethical principle of equality is contingent upon wealth to invoke liability claims (an idea much canvassed when enhanced privacy and security were seen as commercial products rather than core requirements of ethical practice in the digital world). From the business point of view, it might encourage location in the state with the laxest and cheapest permitted practices. In either case, the citizen loses relative to other citizens; and competitiveness and a level playing field in the EDSM are compromised.

Both these dangers could be minimized if it were possible to build in ethics by design that make ethical practice the default, not the option.

This is perhaps all the more necessary now that different biometrics are becoming commonplace authenticator elements in identity management. There is a temptation to assume that having secure systems and methodologies is the most appropriate antidote to threats. While these are necessary they are not sufficient, even with linked multi-biometrics.

Nevertheless, eCommerce advocates suggest that biometric authentication models are seen favorably by consumers (as the Aries pilot confirmed) and retailers. From the perspective of a business model, the attraction lies with:

1. accessing new consumers (eg customers unwilling or unable to use traditional logins or epayments on mobiles devices, but potentially more willing to provide a fingerprint or voice to pay for an order, even though fingerprint reliability declines significantly with age or injury, and voice prints may change over time)
2. expanding the concept of the eshop to buying anytime anywhere with any smart device (eg using voice recognition, like Siri, Alexa etc to or buy things directly from home or on the go, or while commuting using voice selection and payment to order and pay for items. Again, reservations excist as to compliance with local laws forbidding use of mobiles when driving, or risks associated with speaking in a public space – such as a bus or train or café – to effect a financial transaction that can be overheard or snooped on by others)
3. helping create a safer and potentially more trustworthy ecosystem by adding properly enrolled biometrics as a means to provide additional security against fraud
4. using biometrics in real-time environments with the person present to unlock access (eg to a door; or phone, for instance with voice or iris scanning as advertised by Samsung and Appel in 2016-2018) pay for goods in any environment, like a school canteen (as in the UK), restaurants (Germany and China), supermarket (Germany, Japan), banking (Japan, UK)
5. using biometric data mining to target ads at selected groups (e.g. KFC China uses facial recognition to make recommendations deduced from making inferences (possibly wrong ones) about a potential customer's age, mood, culture);

In general, there seems to be little to limit the sale and the use of eIDs for all manner of domestic purposes, alongside egovernment services and those designed to uphold respect for ethical practices vis-à-vis citizens and vulnerable groups in general. Society is aware of eIDs for travel purposes. Generally, people from states who are used to having their identity recorded and validated from birth, at least in paper form, are used to complying with requirements regarding the acquisition and use of driving licences and travel documents for cross-border travel, and increasingly for banking and eCommerce.

The wider publicity given to the risks to the integrity of personal information being gathered by dint of online activity and the IoE has largely been framed as a concern with data protection and privacy. Legal requirements therefore pose a potential limitation to the use of eIDs under specific circumstances that relate primarily to the handling and storage of personal information. In November 2016, the French watchdog, CNIL, warned the government against establishing a central database with fingerprints, facial images and other personal information prospectively of all its citizens. The objection related to a central database for authenticating ID cardholders. The CNIL preferred the government adding a chip to the French national ID card to guard against infraction of a database or misuse of information provided voluntarily (as registration). While CNIL recognised the need for data forensics, it objected to the central database as a potential threat to individual privacy. (cnil.fr). The German government and data protection authorities have also been vigilant in these respects (bmvi.de) and attention to the vulnerability of personal data using or linked to biometrics and cloud apps has grown, notably since 2012 when Nordic countries especially focused on this. (https://www.pcworld.com/article/2041184/google-apps-deal-disallowed-by-swedish-data-regulator.html). Biometric vulnerability assessment is a concern of independent bodies, governments and private stakeholders.

Societal acceptance of eIDs may be compromised by the inappropriate use, potential loss, misuse or impersonation of an individual or cluster of individuals whose data has been fraudulently acquired through hacking (as in the case of Yahoo, and hacking of 'smart appliances and toys). Society as yet has been less persuaded by the claims that biometric eIDs can assist in identifying people holding multiple identities. For instance, in September 2016, the Canada Border Services Agency noted that a cyberattack on their facial recognition or fingerprints data bases could prevent innocent travellers from entering the country or allow people with false identities into the country. However, its databases had revealed a match between two different valid eIDs (travel document and driving licence) under two names yet held by one illegal immigrant. (Lee, Biometricupdate.com 15/09/2016)

There is a tendency for citizens to compartmentalise their use of online services and to see privacy and related issues as context dependent. Therefore, until and unless the linkages become clear, it is possible that citizens will hold different expectations and values for different apps. The eGovernment and physical border management scenarios are those where citizens probably became most aware of the opportunities for online convenient transactions, as well as Big Brother: PNR and eCommerce began emerging after 1998[3]. Today, there is increasing vigilance of the potential ethical and privacy harms to children watching cartoons and playing games online with no or little understanding of the implications for the autonomy, integrity and dignity of their future selves. Clicking unwittingly in games that in effect encourage gambling sites or on complicated, lengthy terms and conditions also compromises individual integrity. This raises profound ethical issues and is one reason why there is a growing disquiet about link ability, eCommerce and online life.

3.6 *Citizen uptake of eIDs*

The uptake of mobile eIDs for eCommerce purposes by citizens has grown by stealth. Emobile transactions, and especially payments are increasing but at different rates across the EU28. What deters take-up differs from state to state. In the UK, eCommerce is approximately 20% higher than elsewhere in the EU. A poll of 18-34 years old smart phone users in Britain in 2016 revealed that 80% used their device for online purchases, whereas 40% of over 35 years old did. The share of smartphones however is highest among the younger age group so too much cannot be deduced from those statistics suggesting that the older respondents prefer using laptops, PCs, or tablets: they may be their only device to do etransactions. (Ipsos Mori Tech Tracker Q4 2016, 19/12/2016).

eCommerce covers both goods and services. eCommerce is linked to areas where ethical concerns dominate. For instance, private health systems (and related issues of insurance, liability, implants, and innovation). Citizens may be readier to use eCommerce tokens for the former than for the latter. Or vice versa, especially if they are convinced of the value claimed by Big Data mining to address health issues. Generally, however, it is unlikely that the average citizen understands how privacy and ethical principles can be protected by technology (such as anonymization and encryption). Education on protecting privacy and credentials from misappropriation, and on how vital they are for authenticating a citizen's claim to be who they say they are, is ongoing.

While readiness to take up eIDs is linked to convenience, the growing awareness of the value of digital data to business and governments has raised citizens' awareness of the privacy and ethical issues this poses for society.

Accordingly, it can be expected that businesses and public authorities who implement high standards of privacy and ethical practices may enjoy higher levels of public trust in their products. This means that compliance with appropriate technical, legal and ethical standards becomes an important part of the business model as well as a part of aware citizens' decision making in choosing (where they have the option) whom to trust with their credentials. That is not simply a matter of enrolment and eID use but crosses over into the wide data protection and privacy arenas where 'consent' and the right to be forgotten are crucial components of the GDPR and DSM. (Cross reference to WP on privacy law)

Ethical compliance with technical standards, laws and guidelines used by and enforced in practice involves openness over the sustainability of trust. Breaches in security and vulnerabilities must be immediately

[3] eCommerce originated possibly with the attempts in the run up to the Single Market to facilitate crossborder electronic invoicing and transfers of funds (EDI) and (EFT). Tele-banking followed ATMs, then business models grew around data storage, mining, resource planning. From the mid 1990s onwards high speed internet made ecommerce accessible to growing numbers of citizens as opposed to businesses, and large public and private sector interests.

addressed, preferably without inconvenience to the citizens concerned. The precautionary principle associated with ethics code must be honoured.

The EU has considered innovation and technology for decades. Obstacles and opportunities to capitalising on technological innovation have been outlined in line with new developments and policy goals. The exponential use of biometrics, notably fingerprint and facial image scans, for official documents such as driving licences, visas and passports paved the way for business models applying biometric authentication to other tokens to validate the claimed identity of a person presenting an identity token. eHealth is one such area which is related directly to eCommerce, but which is subject to different rules and exemptions under the ePrivacy. It dovetails too with AI, robotics, rights of robots and function and mission creep meaning that built-in ethical reflection and awareness are critical.

There are contradictions and complexities in the Single Digital Market strategy that the Aries Use Cases illustrate. The Aries pilots were informed by concerns over fraud, privacy, authentication and onward use.

3.6.1 Societal concerns over fraud and mission creep privacy as barriers to eID adoption

Barriers to adoption arise primarily from societal scepticism over the vulnerability of eIDs to impersonation, onward misuse, fraud and theft.

- **Privacy intrusion**

Given the revision of data protection rules, and recognising this, the EU Commission launched a public consultation on the review of the ePrivacy Directive between 12 April and 5 July 2016. The review is one of the key initiatives under the DSM aiming to reinforce trust and security of digital services, 'with a focus on ensuring a high level of protection for citizens and a level playing field for all market players' (ec.europa.eu DMS Objectives: Summary). The highest number of responses were from Germany (25.9%) UK (14.3%) Belgium (10%) and France (7.1%). Concerns were raised over omissions regarding VoIP, email apps. Instant messaging; and opt-ins (favoured by public) and opt-out (favoured by industry). This fed into the deliberations on the draft Regulation discussed by the European Parliament in October 2017.

Some high-level intrusions and thefts involving banks (Wells Fargo and Tesco, for example) led to distrust of the technology. As long as the banks recompense their clients for any financial losses arising from data breaches and theft of funds from their accounts, it is likely that eIDs will continue to be taken up. However, customers who have been impersonated and whose data has been fraudulently used may have a different reaction.

- **Re-establishing authenticity**

If re-establishing the authenticity of their claim to own their own eID is difficult, takes a longtime, is expensive in time and money, is inconvenient and incurs financial harms, they may become less inclined to use eCommerce services.

Overall the public still has some issues regarding e-commerce but those are fading, namely when considering the timeline of future technologies' potential and implementation. These were explored in the Aries Use case pilot focus groups. [See Appendix 1]

4 eCommerce and the consumer

In the eCommerce area, by 2017 there was growing consensus that realising the Single Digital Single Market (DSM) by facilitating cross-border transactions, both physically (in terms of the delivery of parcels) and virtually (by enabling transactions via eIDs) could boost EU prosperity and competitiveness. The DSM is seen as the counterpart to the Single European Market. A number of polls on different aspects relevant to the DSM have been conducted. They have focused on internet access and speed, geo-blocking and e-commerce.

In summer 2016, the Flash Eurobarometer poll produced a consumer scoreboard. It noted that while the frequency of e-commerce has grown and half of online consumers bought goods and services online in 2014, fewer claimed they felt confident buying outside their home country (38% to 61%), and awareness of cross-border online purchases was ambiguous. Cross-border e-commerce was seen as causing disproportionately high number of problems regarding delivery issues and product conformity. Country of residence discrimination was among the majority of complaints about cross-border e-commerce received by European Consumer Rights centres. Low awareness and knowledge about consumer rights remains problematic, especially among the young. This is an area where Aries would recommend efforts in educating econsumers.

Eurobarometer noted: 'Investing in enforcement does pay off. There is a high correlation between retailers' perceptions of enforcement efforts on the one hand and their assessment of compliance and of the prevalence of unfair commercial practices on the other hand, which suggests that monitoring efforts do translate into better outcomes for consumers.' Even so, a quarter of consumer do not complain in the event of a problem, largely owing to insufficient information, belief in a low likelihood of success and long procedures. Alternative Dispute Resolution (ADR) was welcomed and needs further development. (http://ec.europa.eu/chafea/consumers;) Consumer scoreboards are regularly updated (http://ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/11_edition/docs/ccs2015scoreboard_en.pdf).

The EU Commission revised the Consumer Protection Regulation (CPC) to broaden its scope and strengthen the powers of the national authorities cooperating on cross-border EU consumer-law infringements. Following three trialogues in June 2017, the proposed changes were sent to the European Parliament for a first reading in November 2017. The Commission has reiterated the importance of consumer protection to the DSEM. Confidence among consumers about buying from across borders is some 20% lower than buying from domestic producers, although it is unclear that consumers always recognise the origin of the seller. However, the Commission found in 2014 that when it looked at 2 500 ecommerce websites, 37 % were in breach of EU consumer law, costing consumers some €770 million per year. 68% of all cross-border consumer complaints related to ecommerce according to those recorded by the European Consumer centers in 2015. The May 25 2016 proposed revisions of Regulation 2006/2004/EC as part of the e-commerce package would facilitate better cooperation beyond alerts and mutual assistances by allowing cooperation on infringements that have already, and introducing new notions of widespread infringement (affecting at least two Member States) and widespread infringement with a Union dimension (affecting at least three quarters of Member States with three quarters of the EU population). The regulation would apply to a broader set of consumer-related legislation, and allow national authorities to have extra minimum powers, such as the right to do mystery shops on behalf of consumers and to order restitution of profits or compensation to consumers. For its part the European Parliament's Committee for Internal Market and Consumer Protection (IMCO)[4] in its report of 21 March 2017 went further in suggesting that national authorities be allowed, as a last resort, to take down an infringing website.
(http://www.europarl.europa.eu/committees/en/imco/subject-files.html?id=20160917CDT00881)

[4] IMCO is responsible for legislative oversight and scrutiny for EU rules on the free movement of goods and services, free movement of professionals, customs policy, standardisation and the economic interests of consumers. It seeks to reduce barriers to economic trade and simplify legislation to enhance competitiveness across the Single Market while taking care of consumer interests

The EU also has multi-annual Consumer programmes to address these issues, most recently running up to 2020. The aims are to: help ensure a high level of protection for consumers and fully support the ambitions of Europe 2020 regarding growth and competitiveness by integrating specific concerns identified in Europe 2020 on the digital agenda for Europe; to ensure that digitalization leads to increased consumer welfare, on sustainable growth by moving towards more sustainable patterns of consumption, on social inclusion by taking into account the specific situation of vulnerable consumers and the needs of an ageing population, and on smart regulation, inter alia, through consumer market monitoring to help design smart and targeted regulations. Consumer interests are to be supported on a horizontal basis across all policy sectors to protect and educate, strengthen consumer rights, and ensuring legislation is enforced.

Of particular interest is the commitment to eliminating 'remaining unjustified and disproportionate barriers to the proper functioning of the internal market and improving citizens' trust and confidence in the system, in particular when buying cross-border, are essential for the completion of the internal market.' (Regulation (EU) No 254/2014, pt.6).

Less attention has been paid to how consumers feel about eCommerce that is disconnected from interaction with a human as opposed to a bot over the longer term. It is possible that convenience will not induce loyalty to a particular brand, and that is something retailers seek. (Lee & Dubinsky,2017 :2039). Aries recommends that attention be paid to this facet of eCommerce.

4.1 *eIDs, eCommerce payments and cyber security*

ENISA has evaluated the most widely used payment applications to define good practice models. It concluded that customers and vendors shared responsibility for adopting minimum security measures for e-payments (to boost e-payments without cards). The mobile payment chain itself requires resilient security regardless of the players involved. Mobile payments are expected to grow by 80% percent annually up to 2020[1]. ENISA suggests that 'Mobile OS provide good security when applied, but many customers are not aware of these, and therefore do not use them'.

In the context of the NIS Directive, ENISA assists Member States and the European Commission by providing expertise and advice, as well as developing and facilitating the exchange of good practices, with the ultimate goal to enable higher level of security for Europe's critical infrastructure, including finance. This subject and the capabilities of facial recognition are intricately connected with the digitalisation of retail: the assurance of security correlates with consumer trust. Retailers therefore have an interest in mastering technology and applying it in the real-world. For example, Alibaba is testing facial recognition to allow its customers to open their lockers (http://www.asiaone.com/digital/alibaba-testing-face-recognition-technology), another sign of how important these technologies are in the pursuit of omnichannel retail and its digitalisation. In another initiative, British start-up Yoti, linked up with UK supermarkets to enable shops to check the age of customers buying age-restricted products such as alcohol and knives, without human intervention (http://www.bbc.com/news/technology-41981983). The free-to-consumer app works by pairing a selfie with an official document such as a passport. This is a subject covered in the E-Commerce scenarios section.

4.2 *Resilient e-credentials and the DSM*

In 2007, the Joint Research Centre's Institute for Prospective Technological Studies, noted the need to facilitate eID uptake. It drew attention to the need to separate the physical device (such as phone, laptop, smart card etc.) from the digital identity credentials that could be electronically loaded onto the device and later erased from it. The credentials 'have no physical existence in themselves, being composed of electronic

ecoding of personal data'. It went on to state that from a security perspective, 'clear means of separate are required to ensure that multiple digital identities retain their integrity within a single selector…EUfp6 'InspireD' programme developed a tamper-resistant personal authentication device (Trusted Personal Device) to 'permit its holder to collect and use soft credentials in the course of their daily activities.' This was seen as potentially very useful for the future. (JRC,2007:27).

The rapid growth of biometric apps, including the uptake of voice recognition technology by banks, is expected to boost consumer confidence in eCommerce and enhance citizens' trust in their data being held securely, subject to annoyance over DNS attacks.

A study probing consumer perceptions of privacy in business-to-consumer (B2C) ecommerce reviewing data up to 2006 noted that demographic factors (age, class/wealth and gender) contributed to how consumers viewed privacy: older people being less likely to believe their data would be sold on, wealthy consumers wanting more information about this than others; and men being more trusting of online commerce and less concerned with privacy than women (Kaapu & Tianen, 2009:6). Structural components about ideas about privacy were related to the product and e-vendor, technology, societal norms (distrust of e-sellers outside home country, consumer self-perception, and views as to context (ibid., 17). Where eCommerce is concerned, privacy is not stable but 'constantly under social construction'. It is linked to risks concerned with logistics and performance: the more consumers are familiar with a site, the more attention they pay to privacy when multi-channel commerce is involved. (Bezes, 2016:300).

These conclusions were tested by Aries both in the initial Focus Groups and via questionnaires. (See section 6.1)

4.3 *Overcoming barriers to DSM*

The European Digital Single Market (DSM) demands infrastructure and business models that promote innovation and take-up. The EU Commission believes that Europe lags behind the rest of the world. It identifies significant barriers to DSM resulting from infrastructure weaknesses (net speed and accessibility, digital illiteracy, cost to consumers and cyber-security risks). It has pushed the DSM to address these over the past few years and in 2017 focused also on rolling out 5G and mitigating cyber risks.

The DSM communications from the Commission initially focused on physical barriers to access (slow internet in rural areas, for example), anti-competitive positions by dominant players (like established telecoms, Microsoft, Google, Skype, Facebook etc) and vested interests. Regulations and directives associated with this have proven controversial. They relate on the one hand to industry and technical standards, spectrums, algorithm transparency, copyright, intellectual property (IPR Enforcement Directive), licensing; and on the other hand to competition law, updating data protection and privacy law (such as the European Data Protection regulation) EDPR and ePrivacy Directive (whose repeal was sought by EuroISPA in July 2016) and Privacy Shield which EuroISPA welcomed).

These are outside the scope of this deliverable. However, businesses seeking to increase their eID market share have to be aware of them, their duties to comply with technical and industry standards, as well as the Regulations protecting citizens' rights to privacy and data protection.

A strategic issue linked to these is the EU Commission's push to cut digital illiteracy (estimated at 40%) (EurActiv.com 10/06/2016) among EU citizens, including school children. Accordingly, it seeks significantly faster or ultra-fast internet speeds. As the costs to do so for every household exceeds €500bn, the Commission wants to target schools, universities, hospitals, transport hubs and local government authorities. The estimated cost is €46bn (Euractiv.16.10.16). In all, eID use is expected to increase.

Mobile access and signal reception are not universally reliable or secure and therefore provide vectors for fraud and potential barriers to the creation of sustainable citizen trust in eCommerce and eIDs.

Action to combat internet fraud is also urgent. Whereas biometrics is presented as a solution to eidentity fraud, biometric apps by themselves are not fool-proof. They are not a panacea to poor practice or neglect of ethical good practice. Data linkage is problematic for everyone.

The biometrics industry undertakes periodic surveys on biometric uptake. The *Biometrics Institute* produces an annual survey of industry, research, users, and buyers from the private and public sector. There have been different views as to which biometric(s) may be the least vulnerable to spoofing, the easiest to enrol, and the least acceptable to the public. Fingerprint identification in some countries has aroused suspicions among citizens as the biometric evoked the idea of being a potential criminal. It was also associated with fraud, ease of spoofing, tracking, and especially the surveillance society (Lodge, 2007). Subsequently, multi-modal biometrics has gained prominence, as well as other single biometrics (such as iris and especially voice recognition). The business case driving biometric adoption lies in part with the relative slowness it was rolled out and taken up by public sector agencies for the purposes of physical border management but more recently with mantra of convenience via the fast pace of mobile adoption and smart gadgets.

Industry sees growth to be robust across the board and across the world. Consumer attitudes are expected to affect adoption rates. For physical border management and some public egovernment services, they may not have a choice. Where consumers have any choice as to whether they provide or use biometrics, their view of biometric data storage practice, ease of enrolment, support, practicality, trustworthiness and reliability of the biometric is likely to affect take-up. (E.g. in respect of the US market, Mercator, 2017) However, which biometric a consumer is most likely to trust remains open and subject to experience and marketing. (Mercator, 2017, Figure 3). Industry feels that the password is obsolete and distrusted, owing to widespread losses such as Yahoo. Yet, denial of service attacks is what consumers experience and having a biometric eID does not overcome that.

E Identity is both a potential tool for engaging in transactions in a digital single market and a commodity in its own right. The intersection between the two throws up ethical questions as to the appropriate use of eIDs for specific purposes. The challenge is to find a workable solution that encourages eID use and which is acceptable to society.

Identity assurance programmes have not enjoyed universal success from either a technical or societal perspective. The UK provides a salutary example of failure by government to replace face-to-face identity assurance services with digital services. Costs have spiralled. Deliverable service reliability has been unreliable. The digital by default strategy lacked appropriate levels of security and identity assurance (e.g. the National Health Service in 2016 was still 90% reliant on Windows XP (The Register accessed 12.12.2016). Costly and confusing proliferation of user-accounts continued (p.5) and the £25 million programme to design and develop a single, cross-government identity assurance service had yet to reach scalability. The federated approach, relying not on one government central database but instead on several smaller providers, was supposed to allow citizens to choose their service provider[5]. The UK relied on a hierarchy of 4 level assurance level criteria, only requiring biometrics for higher security or 'more convenient assurance' (such as visits to high security prisons). The Technical overview states that identity assurance is designed to enable a citizen to be identified at a service provider with a required level of identity assurance, without revealing anything to the service that it did not already know about the individual. (p.19 Appendix 2). The High-level

[5] The GDS signed contracts with 5 providers in Sept 2013: Digidentity, Experian, Mydex, Post Office and Verizon.

architecture to facilitate that is SAML2[6]. This approach is out-dated and pays scant regard to the kind of essential security and ethical safeguards needed to sustain societal acceptance.

Identity assurance and identity verification place different and tougher demands on providers in societies where fast internet access is the norm but also where scalable collaborative open innovation builds smart societies across isolated communities anywhere empowered by digital technology, and boosting human capacity.

4.4 *eIDs and inter-operability*

The FIDO Alliance (Fast ID Online www.fidoalliance.org) not-profit industry alliance was formed in 2012 to address lack of interoperability among strong authentication technologies. It aimed to develop strong authentication while keeping up with technological innovations as the IoT and connected things. In December 2016, it announced a roadmap to end dependency on passwords by introducing simpler, stronger FIDO authentication, including 'improving online authentication by developing open, interoperable industry specifications that leverage provide public key cryptography for stronger security and device-based user verification for better usability'.[7] It suggests that this entails improving:

1. FIDO 1.1 specifications (including 'support for smart cards, Bluetooth Loaw Energy (BLE) and Near Field communication (NFC), and an expanded authenticator metadata service to better service the risk management requirements of online service providers'.
2. W3C (World Wide Web Consortium) Web Authentication specification (https://www3c.github.io/webauthn/) to define a standard web API 'to enable web applications to move beyond passwords and offer strong FIDO authentication across all web browsers and related web platform infrastructure.
3. Client-to-Authenticator Protocol (CTAP) – a new release is planned in 2017 to enhance user authentication experience, removing the requirement for users to re-register on every device they use so that they can use their wearable or mobile device to log into computer, IOT, device etc.
4. User Verification Caching Specification to provide a standard way for mobile wallet providers and payment application developers to support Consumer Device Cardholder Verification Methods (CDCVM) 'enabling consumers to conveniently use on-device FIDO certified authenticators – such as fingerprints or 'self' biometrics – to securely verify their presence when making an in-store or in-app mobile payment.' [8]

FIDO specifications and certifications are designed to enable an interoperable ecosystem of on-device authenticators that can be used with compliant mobile apps and websites. Service providers include Google, eBay, Paypal, Bank of America, Samsung, Gov.UK, Qualcomm, Dropbox and Github etc.

The Commission's initiatives of eIDs and interoperability are especially relevant in this context. (https://ec.europa.eu/digital-single-market/en/news/principles-and-guidance-eid-interopability-online-platforms-finalisation-and-way-ahead)

[6] SAML2 is 'Security assertion Markup Language version 2.0. It is an XML-based (Extensible Markup Language) protocol that uses security tokens containing assertions to pass information about the service user between the identity provider and the service providers. NAO (2014, p.21)

[7] FIDO Alliance (2015) Response to NIST RFI on the framework for Improving Critical Infrastructure Cybersecurity, February 2015 www.csrc.nist.gov accessed 11 December 2016.

[8] https://fidoalliance.org accessed 11 December 2016.

4.4.1 eIIDs and anytime, anyplace eCommerce – multifactor authentication drivers

The US Department of Commerce, through its National Cybersecurity Centre of Excellence (NCCoE) and the National Institute of Standards and Technology, has a Retail project team collaborating on multifactor authentication (MFA) for e-Commerce. FIDO believes that the adoption of multifactor authentication will address weaknesses that enable cyber-attacks. That, in turn, is believed to encourage eID use. However, some developers suggest that only when users believe there are significant risks will they opt for multifactor identification[9]. Industry sees a big growth potential in the DSM. Yet, apart from boosting dependable, secure eID uptake, additional barriers may hamper anytime, anyplace eCommerce. There is a discrepancy, for example, in the approaches of major market players even though there is general agreement that eID use would boost commerce and cut the potential for fraud.

eCommerce Europe represents 25,000+ companies selling online services in Europe. It is the voice of the e-commerce sector in Europe. In 2015, it noted that only 15% of consumers shop online from another EU country. It identified market and policy priorities to stimulate cross-border ecommerce in Europe. It concluded that the main three barriers are legal frameworks, logistics and taxation/VAT. Others include online payments, competition issues (such as geo-blocking), language, client relationships and marketing. It advocates boosting consumer trust through a pan-European Trustmark, and a web-platform on e-logistics to support more transparency in parcel delivery. As indicated below, eID use in the whole eCommerce chain may be complicated after the purchase of a product. eCommerce Europe seeks progress on e-dentification and authentication. It seeks a pan-European framework for online payments leaving room for innovation at fair cost, citing 25% of sellers saying online cross-border payments are problematic, burdensome, obsolete, lack e-ID which create burdensome consumer authentication and identification, complicated checkout processes requiring too many steps, problems with third party service payments, and need for interoperable e-mandate to facilitate SEPA direct debits. At the policy level, eCommerce Europe has advocated full harmonisation of legislation on privacy, security and consumer rights without additional burdens on industry, simplifying consumer rules (Consumer Rights Directive CRD) for online Business-to-Consumer (B2C) sale of goods, services and digital content, standard information rights for e-communication, fast rollout of a common European online complaint and dispute resolution system, European contract law approximation of national rules, harmonising privacy and data protection legislation, recognition of the need for e-communication and data driven marketing. Electronic signatures and trust services are now valid throughout the EU. EU rules on electronic signatures, electronic seals, time stamps, electronic delivery service and website authentication apply directly across the 28 Member States.

Cross-border digital transactions will be more convenient and more secure in the Digital Single Market. The eIDAS Regulation has helped to create a European internal market for electronic trust services by ensuring they will work across borders and have the same legal status as traditional paper-based processes. The eIDAS Regulation introduces the principal of non-discrimination in the legal effects and admissibility of electronic documents in legal proceedings. (EU-Forum Electronic signatures and trust services now valid throughout the EU) eSignatures, eSeals, eDelivery, time stamps and website authentication all form part of a scheme to repeal the eSignatures Directive and promote a EU trustmark for qualified trust services. The Connecting Europe facility (CEF) to allow member governments to connect directly in respect of eidentification mutual recognition is making progress, and some are to pilot it and notify their eIDs schemes by 2018.

Meanwhile, the German eID that is in the process of formal eIDAS notification (for the mutual recognition by all EU Member States enters into force in September 2018 for public sector services requiring LoA level Substantial or High). A successful roll out and uptake of eID and trust services across borders and across different sectors is essential for realising a Digital Single Market and digital transformation of organisations. While this has been on the EU's radar for some long time since the start of this century, it is only more

[9] SecureAuth,2016.

recently that the implications in terms of ethical practice and impact on society have come to be taken more seriously. This is both necessary and an essential precondition for the success of a trusted digital single market's evolution and sustainability.

4.5 *Lessons for society*

The challenges facing public authorities and commercial enterprises in persuading the public to use eIDs for eCommerce and eAdministrative purposes have been recognised by the EU. The cost of building sufficient infrastructure to build a European gigabit society by improving internet connectivity using optical fibre and wireless networks. The aim is to help overcome the digital divide across the EU has been addressed in part by the April 2017 WIFI4EU initiative to mobilise EU funding through its Connecting Europe Facility (CEF) in order to offer free wifi in public service buildings such as libraries, administrative offices and hospitals, and may be beyond (European Parliament Report (ITRE)on the proposal for a regulation of the European Parliament and of the Council amending regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities (COM(2016/0589 -C*-0378/2016-2016/0287(COD), A8-0181/2017 and debated OJ 12/09/2017-44).

At the level of the citizen, there are contradictory trends (i) ready uptake of online transactions by users in some EU states (ii) unequal enforcement and a high level of non-compliance (five sectors clothing, electronics, recreation, consumer credit and package travel accounted for 37% of non-compliance in 2014,(including non-delivery, defective products, contract problems, unfair practices of eCommerce in 2014) with key Union consumer protection laws (COM(2016)283 final). The cost to the eCommerce market was estimated at €770m per annum (p.5) and pressure for enhanced legal and regulatory consumer redress has grown since then (iii) concern over fraud among users, vendors of goods, and sellers of eID solutions.

There is some recognition that fraudsters' ability to outwit all exceeds the speed at which new, more intrusion proof, solutions come on stream for public adoption. For instance, the growth in alternative payments methods and systems (APM) reveals the many different vulnerability points. APMs cover anything from mobile payments, bank debits and credit cards, money service businesses, prepaid cards, crypto-currencies, to peer-to-peer (P2P) payments, and eWallets. In the US alone, it has been estimated that APM payments will grow by over 32% in 2017 (fraud.net-the alternative-payments-explosion, 13 March 2017)

Apart from the technological responses to combat money laundering, fraud and theft, banks and financial bodies have to go beyond due diligence procedures and now re-think their strategies regarding knowing their customer (KYC) or their customer's customer (KYCC). This may mean knowing a great deal more about payment chains, changes in business models and company structures and not just payments methods.

It is vital to distinguish between eID use in different contexts for different purposes. What may be ethically acceptable in security related circumstances (where 'exceptions' to legal requirements are important up to a point) may be unethical and deter societal acceptance in others. What may be unacceptable to able-bodied users (such as facial recognition in photo tagging and geo-location identification) without express consent, may be very informative and useful to those unable to see. Facebook, for example, does not collect geo-locational data although it might be shareable, with consent, among 'friends' in future. Similarly, what may be acceptable as a sufficient privacy safeguard for facial recognition in some places (e.g. a state in the USA) may be inadequate and insufficient elsewhere (as in the EU and Canada, for whose users Facebook does not hold facial templates).

The issue of consent is also problematic: contextual 'opt-ins' for sensitive personal data provide an illusion of data being under the user's personal control but in practice companies may differ significantly in how they generate, use (transparently or not) or modify and commodify 'personal' data. The effect is to weaken

privacy safeguards and create an expectation of only rudimentary 'consent' being necessary for transactions that a company may deem 'non-sensitive'. Projecting to 2020, the tagging of people in live videos and photo clusters may enable commerce to identify people and identify them as they enter and exit a shop, for example and re-use that data for other purposes. The effect is to allow mission (also called 'scope creep) and function creep without the express consent of the user who provided the data, knowingly or not.

The implicit merging of public/private boundaries in the management and delivery of eGovernment services as well as physical border management gives rise to additional issues. The ethical implications of certain types of eID in such contexts therefore have to be carefully considered.

The technical ability to facilitate cross-device interoperability – something likely to appeal to users in terms of convenience at least – for cross-border transactions is feasible. How the associated eIDs reflect underlying values and ethical principles in automated and manual practice requires conscious engineering at the outset.

In a digital society online all the time, the eID has a particular value in enabling all manner of interaction. The likely use of a mobile eID for private and public transactions (such as BYOD) highlight the ethical challenges arising from device sharing for the whole transaction chain within and across work and family environments. Where eCommerce is concerned, for instance, ethical concerns may arise at the point of the physical retrieval of an item from a named delivery point that is not the same as the purchaser's address. For example, someone picking up a parcel from a shop on behalf of a neighbour, whether or not age restrictions apply to the item being picked up. What society might see as normal, may not be recognised as such in a chain reliant upon the eID even at the end-point.

In short, the questions for society are:

- How much information is enough to conduct the transaction in any environment, using an eID?
- How can that be limited to what is essential for the transaction?
- How can onward use of that, and any linked, personally identifiable information, be prevented if either human or M2M interaction takes place?
- Under what conditions and circumstances would it be ethical for all (or part of) such information to be linked and shared without the data subject's explicit consent?

4.5.1 Lessons for ARIES: Can built-in ethics by design learn from privacy by design?

Insofar as there is a sense that privacy has been lost and may be irretrievable, PETs and PEDs have been seen as a means to ensure that eID development, use and sustainability are accepted. Their more widespread acceptability and adoption by citizens for private and public transactions may be boosted if they are informed by ethical principles. However, to seek to market ethical compliance as an optional 'extra' to inspire 'trust' immediately faces ethical hurdles : it would be inherently divisive and contradict basic ethical principles, starting with the precautionary principle. Ethics is not therefore commercialisable in quite the same way that privacy has been portrayed.

Privacy itself has, however, been increasingly developed as an e-commerce in its own right. The EDPS indicated that lack of competition over privacy implied market failure (Opinion 8/2016:13). This was probably not meant to spur a market as such in selling higher levels of privacy protection to those most able to afford it – something that conflicts with ethical principles. The suggestion that privacy is irrelevant, or an optional add-on rather than a first principle in the design of apps and processes, compromises ethics. (Cross, 2016). Wellknown people who have argued that privacy is obsolete, nevertheless, seek assurance for their physical privacy. (Boingboing.net, 19/01/17). Similarly, OpenData reveal inherent contradictions in weighing up one set of priorities over others. The ethical implications of opening data, use practices and users have led to

efforts to build replicable, credible and sustainable methodologies to develop common assessment methods. Ethical issues and the impact of how wearable devices and virtual identity management impact society has become mainstream and helped to raise awareness indirectly of the expanding scope for using eIDs ethical and in ways that protect personal privacy. (blog.okfn.org, 20/01/17). Moreover, the idea that a zero-sum outcome is inevitable (e.g. the idea that any gain in privacy has to be at the expense of security, and vice versa: a gain in one area means a loss in another) is outmoded. Where ethics is concerned, application of the precautionary principle has to be a core and first principle. There is no trade-off that is ethical.

Aries eID is informed by ethical reflection. It starts from the ethical viewpoint that human autonomy and dignity can be preserved as eIDs are adopted. It recognises the vast cultural and societal diversity. It seeks to show that socio-economic-political differences need not be a barrier to the adoption of eIDs even if those differences are so vast as to defy the adoption of uniform legislation in a coherent and timely manner across the world.

Aries eID demonstrates that privacy and security can advance in tandem. The Aries eID aims therefore to develop a neutral privacy enhancing, ethical and secure ecosystem optimising public trust.

Addressing declining public confidence (and trust) rests on building and sustaining a demonstrable, reliable, dependable, privacy enhancing and secure eID. It has to be culturally and societally neutral; non-discriminatory, accessible and affordable to all, regardless of socio-economic status; easy to enrol in and easy to use; and something that reduces the likelihood that further deductions about the eID owner can be made automatically and used for unconsented to purposes.

Aries eID is informed by ethical commitment to preserving autonomy, dignity, purpose limitation, purpose specification, data minimisation, security, privacy, accountability and traceability.

The Aries eID approach is designed to be neutral, specific in intent, dependable in use and a means to combat the disclosure or linkage of information associated with a physical human being that is not essential for the transaction. This enables it to fulfil the ethical obligation of a duty of care towards users and stakeholders and to help create a reliable ecosystem in which ethics by design is embedded.

To demonstrate how Aries innovates and moves beyond the state of the art, focus groups in two use cases (eCommerce and e-airport) considered both the pre-Aries and post-Aries scenarios.

It is important to be clear that the SoA scenario accepted the general view that scalability of eIDs for generic use depended on overcoming barriers which we have shown typically divide into:

- Regulatory ecosystem
- Technical ecosystem
- Commercial ecosystem
- Socio-political-ethical ecosystem
- Within them, are infrastructural constraints, costs, and transformational opportunities.

The creation of eIDs is, as ebanking initiatives insist, a reasonable way to try and enhance and ensure user safety in online transactions. There are many ways to create an eID. In Aries the eID is created from an identification document such as the passport. The problem is an authentication of people when creating a virtual identity. This authentication can be by password, fingerprint, voice recognition, face recognition, etc. Associated with each form of authentication are advantages and disadvantages so choosing one that poses the least risk to users is important. In this context, facial recognition has the advantage of linking a personal document such as a passport with the face of the person, something that is not always possible with other forms of authentication. Aries recognises the limitations and problems associated with facial recognition (including privacy and potential misuse of personal information) large scale adoption of eIDs with facial

recognition in retail may be acceptable, especially in developed markets where privacy concerns are paramount.

4.5.2 Lessons for ARIES: Airside in the eAirport: risks, deception, theft and fraud

For citizens, concern over fraud and intrusion are paramount. There is well-founded concern over the relative robustness against theft and fraud of personal identity tokens (Commission 2015, 192 final). Public and SME trust in the technology and confidence in social media and marketing companies assuring privacy and using their data responsibly fluctuates but is worryingly low. (Special Eurobarometer 431, 2015). Public confidence in the dependability of eIDs and alleged privacy protecting code (such as barcodes designed to conceal alpha-numeric data) is not as robust as might be assumed. Barcodes are readily read by commercial apps. If users carelessly discard boarding cards or luggage tags, or download barcodes to mobile devices, email or social media (such as Facebook or the #boarding pass on Instagram), personal identity information is put at risk of theft. Combatting that may be a matter of educating consumers who engage in cross-frontier travel but that does not cover society at large. All data generated by individuals online is potentially commercial sable by someone without the knowledge of the original data subject.

Passenger Name Record (PNR) information has been criticised as privacy intrusive in terms of the scope of the information collected by (aggregated, spliced and commercialised by the new data owner, such as airlines and travel insurance companies). PNR encountered objections from society in view of its associated connotation with Big Brother surveillance tracking. Bigger challenges relate to obsolescence and weak privacy protocols: authenticating a booking by using just two pieces of information (the six character PNR, and the user's surname). Its display, in the past, on luggage and boarding passes also presented identity thieves with opportunities. This has been criticised by Hern who argues that the six-character code is easy to guess owing to the age of the technical ecosystem used by each GDS provider (the biggest two are Sabre, founded in 1960, and Amadeus, founded in 1987). They generate the six characters differently but are more vulnerable than a simple password (Hern, 2016). Moreover, certain codes are readily linked to specific airlines; other providers issue the first two characters sequentially on one day. This cuts the number of guesses available to attackers. Many portals into the GDS system had minimal security: 'Some websites that have access to the system and allow you to use your PNR and last name to check the status of your flight offer no defenses at all against an attacker guessing thousands of combinations a minute (to) access multiple records.' He notes that researchers looking for bookings under the name "Smith", and using a thousand randomly generated booking codes, found active bookings. Apart from misappropriating and misusing access to cancel and rebook a flight, phishing attacks could be enabled by deriving enough personal information from the flight booking to engage in fraud. The weak technical ecosystem also means that access controls are inadequate and tracking is weak, so that a variety of people can view a booking.

The two drivers of reform are privacy breaches and rising cybercrime. Without tackling the underlying ecosystems, dependable trust cannot be sustained nor extended to other eID uses. Privacy legislation by itself cannot remedy deficiencies in the technical or commercial ecosystems. The EU's ethical duty-of-care principle is firmly entrenched as a guide for technical artefacts and data handling.

This duty of care in the case of privacy has, until relatively recently, been seen as a burden or a cost to businesses. Coupled with duty of care, showing compliance and dynamic observance of legal rules and an ethical approach becomes a business enabler, especially if ethical provisions, security and privacy are seen as first principles rather than as after-thoughts by engineers and app designers. With 5G on the horizon, this is imperative not optional.

4.6 *Aries at the airport: eIDs, fraud and the ethical duty of care*

Even in the airline/airport settings, neither privacy, nor technical nor commercial ecosystems can be seen as distinct. The growth in smart environments makes tackling them in a holistic way imperative and crucial if societal acceptance is to be sustainable. The IoE's susceptibility to intrusion and fraud is a growing concern to aware citizens but there is some anxiety that business-models do not sufficiently take on privacy and ethics considerations: Artificial intelligence (AI) pricing mechanisms are expected to lead to collusion in an anti-competitive and probably unethical way. (Ezrachi & Stuecke,2015). This leads to pressure for anonymity and no-tracking.

The EDPS has suggested that therefore services without tracking and profiling should be developed as a model (Opinion 8/2016) to preserve privacy and sustain trust. Discerning what ethical principles are key is vital, especially if cross-border transactions are to grow as part of realising the DSM. Preconceptions and biases are implicit. They should be made explicit and technical innovations developed to ensure sustainability, bolstered by regulation and law (Lodge 2012) and human intervention.

The Aries airport case study presents a snapshot of a part of daily societal interaction to help understand and illustrate the actual and potential barriers to eID use and uptake.

How this may relate to denial of access to a service or a physical space is readily shown by eGates.
At eGates in airports, a border control officer mitigates the individual's sense that a machine (a bot or app) is denying him access and can be especially important for vulnerable, disabled, infirm people and babies. Ethical principles of dignity, accessibility and equality are thereby honoured.

The eAirport case study is a microcosm of potential transactions people with eIDs engage in. It hones in on one aspect of the eairport : the loss of an identity document/passport necessary to fly. However, the potential use of an Aries eID in such a setting also illustrates potential convenience and time savings to passengers choosing or having to use an eID in the following:-

- eCommerce (buying goods; tickets; services, such as foreign exchange, spas/showers on site; and buying web access)
- automated ebanking (foreign exchange, checking banking online, online shopping)
- border controls (tickets and boarding passes on physical paper documents or on mobile devices)
- luggage deposit and collection

The primary ethical duty to 'do no harm' is difficult to reconcile with the sometimes conflicting challenges of using technologies to maximise safety and security. Accordingly, Aries is aware of the tension between ethical considerations and security but it does not accept that they are polar opposites, rather Aries takes the approach that security (citizen trust, reliable and dependable eIDs) is likely to be strengthened where ethical design and practice are prioritised. Scalability is the challenge.

For public services concerned with surveillance for security purposes (crime prevention, immigration control, policing, customs, money-laundering, trafficking, vehicle identification for parking, anti-terrorism, for example), the actual and virtual eIDs for verification and authentication are useful.

They are seen by society as means of tracking for legitimate and disproportionate purposes. Herein lies both a potential barrier and an ethical dilemma as to the limits of using these for tracking.

The potential for the multiple eID uses to be tracked and linked for legitimate purposes by public authorities (not private authorities to whom that role has been outsourced) leads to some scepticism on the part of the public and is generally subsumed under 'Big Brother' claims-making.

More problematic is the linkage of an individual travel document eID to other behaviour and transactions by an individual in the airport. Again, society seems to accept linkage for combatting crime by legitimate authorities. It does not when private-public security services are involved; or when physical or online retail outlets are able to access such services for wider purposes. Geopolitical advertising, for example, may seem like an annoyance and to be turned off like ad-blocking. However, personal awareness of how one's personal digital trail can be tapped into without one having given explicit consent to that is growing and may prove a barrier to sustaining the use of eIDs. Disproportionality, purpose limitation, purpose specification may be breached. Mission and function creep inevitably pose ethical challenges regarding the priority attached to the use of data. Is the priority that defined by the private owners of the physical space in which the transaction occurs (as in the case of the airport confines?) or are all commercial interests subordinate to the primary right of the individual to have sole ownership of his data, however generated?

This is a muddy area because different rules apply to different elements of the eID (biometric capture being a prime example) and associated travel documents (like pre-enrolment for boarding). Airlines from some states see that data as commercially privileged data that they own the moment the individual buys a ticket. Mining that data to sell the individual some product (like another holiday) may be commonplace and not seen as overly intrusive. However, those 'suggestions you may like' raise ethical considerations concerning both wider onward use for additional purposes (whether or not re-spliced), as well as more fundamental ethical issues about an implicit intention to compromise freedom of choice by shaping the parameters.

AI, wearable devices storing personal information and the Internet of everything increasingly rely on bots to make decisions. The ethical implications of this need to be clearly understood, as has been attempted by ethical reviews of robotics. There is a significant risk that over-reliance on the automated decision will lead to sub-optimal results, discrimination (which is central to automated decision making algorithms) injustice and a loss of human analytical decision-making skills (such as the informed hunch of a policeman).

Further risks attach both to technical failures and vulnerabilities (e.g. outages and data and eID degradation, poor enrolment and capture) and to underlying implicit assumptions about people in society.

A commonly overlooked risk concerns public expectations of cross-border information exchange in general. The tendency to assume that such exchange is simply executed by all public and private authorities is contradicted by experience and politics, the consequences of which are unexplained to the public. For example, Denmark has an opt-out on Europol now which means that even though it is one of the most active users of Europol data bases (recording 24% of robbery interrogations, 16% on terrorism and 13% on illegal immigration (EUObserver.com 25/01/2017) it no longer will have direct access to Europol databases like SIENA. This undermines efficiency, convenience and effective security through IT. In this instance, no matter how robust eIDs are to allow officers to verify and authenticate each other for administrative purposes, there is a risk to the delivery of operational efficiency gains. The same applied to the UK in 2014-2016 when its various opt-outs and opt-ins were tested by political vacillation: the UK was in the top four for introducing new cases into the Europol system and its use of Europol-based systems (including for tracking terrorist finance, and top three using Europol information systems, and led use of the law enforcement data network in 2015) (House of Lords, 2016#28, p10). The UK is a heavy user of Eurojust for real-time work.

Reliance on different standards is a risk to eID efficiency in any sector. Reliance on an eID informed by cultural traditions, politico-ideological priorities and discriminatory practice are unlikely to generate sustainable trust and public confidence. These require a neutral as possible multipurpose eID. Scalability depends on ethical design.

5 e IDs -Ethical discrimination

5.1 *Ethics by design*

Ethics by design may be a desirable first principle for designers. The need to apply the ethical precautionary principle (of do no harm) is important as a starting point when considering the construction of an eID. Since harm can arise owing to the different circumstances a citizen faces (such as socio-economic, educational, political, health and age), a technology that is 'neutral' in those respects would provide a significant ethical gain.

The use of eIDs in different scenarios requires awareness of policy context and objectives. Any design of an eID therefore requires that the designers are aware of those and conduct ethical impact assessments as they design an app. These too need to be as neutral as possible if they are to be scalable and usable across devices, societies, products and eID based services.

Most IT use is discriminatory and relies on a citizen user being self-motivated and having the capacity and opportunities to access and use it.

It may be seen as ethically acceptable for machines and/or humans to 'sort' and 'categorise' people with a view to preventing or deterring certain kinds of crime that present severe risks to physical spaces and groups of people (such as terrorism). 'Security' and 'risks' are concepts informed by cultural and historical preconceptions and goals. These are outside the scope of this report so we focus on the issue of when is eID use, or the requirement to enrol in, possess an eID, likely to have discriminatory impact on certain groups of people in ways which may be regarded as unethical.

eID use relies on access to the web and mobile devices. It potentially excludes the vulnerable and the less well-off who are among those who may benefit the most in terms of access to services by having an eID at their disposal and under their control. Their own vulnerabilities may place them at distinct disadvantages (magnifying their exclusion from society) and especially heighten their vulnerability to being opted into and out of things by other humans and bots; and to their information being linked by and made visible to a host of unknown others (eg in social care and service settings) thereby compromising their right to privacy, dignity, autonomy, self-determination, equality and respect for their human rights.

eID use that disadvantages certain people and groups, discriminates against them, causes them harm (or greater difficulty to enrol and access eIDs (cost, net access etc) are unethical if it prejudices their ability to access services. What alternatives are easily and readily available, at no cost to them, to compensate them and enable them to use those services as easily and speedily as possible. It should not be assumed that access to, and use of the net or mobile phones is universal. Nor should it be assumed that across the EU28 and beyond, older people do not use it. Evidence suggests otherwise.

The EU's ambitious commitment to realising a Single Digital Market underlines the goal of increasing efficiency, convenience and trustworthiness of e-transactions across all walks of life. Accordingly, the goal is to make it digital by default. This is to be enabled by the once-only principle (to cut multiple entry of same data several times), inter-operability by default, inclusive and accessible practices. Openness and transparency and security by design are to become as ubiquitous as PETs and privacy by design (ISA,2016). The importance of trustworthy data practices, and context aware personal data management is advocated to allow citizens to control access to and use of personal data in ways that give them sufficient autonomy to determine, maintain and develop their personal identities. Clearly, there is an important role for eIDs in this but the report, itself, devotes only 12 lines to the idea of invasive biometric IDs (ISA,2016:72). eIDs,

eSignatures, eDelivery and eInvoices are central components of eCommerce, eProcurement and e-public administration within and across physical and eborders.

The EDPS' call for ethics by design, supplementing privacy by design, is important and signals EU ambitions to lead in terms of creating a fair and competitive digital eco-system for society. (EDPS,2017)

Big Data and Open Data are areas where ethical principles clash head on. Information got through ad-tracking and suggestion gives rise to concern as to the sanctity and ownership of that data (the individual generating it) or the agency mining it. Robust anonymization and encryption are not necessarily perceived as understandable or sufficient by citizens distrustful of government in general, and increasingly of private businesses (including banks) prone to losing personal data.

At the heart of understanding ethical issues raised, is the implicit view that technological advances outstrip both legislation and citizen understanding of what happens to personally identifiable data once 'out there'. The question of proportionality – how much information is essential to authenticate a person, and critically how much of that needs to be stored on a device or data base and shared with a service provider has yet to be resolved. This is. However, central to ethical eID use.

Ethical eID design and use requires more than respect for legal requirements, PETs and PEDs. It needs to build in and into ab initio something that allows the citizen to determine what kind of personal information can be released by it, in what precise circumstances s/he chooses, and prevents onward use and linkage in full or part by humans or automated processing. This is about more than the somewhat misleading concept of a right to be forgotten, erased on request or at death as being mooted for a prospective legal requirement that digital data held by various companies, agencies private and public-sector bodies revert in full to the originator's legatees.

Public trust is falling in the technology and use of personal information linked to an eID. The scepticism of the public to eIDs potentially overrides acceptance based on the convenience of being able to use the eID for all manner of online transactions societal implications of eID adoption and roll-out are linked to political risks, contrasting national interests and legacies, legal and political obstacles.

The scope of the EU's legislative power to introduce minimum standards for national ID cards, something indicated following the adoption of The Hague Programme in 2005, has hampered transforming technical advances into legally binding measures. (ibid:55). Similarly, there is scepticism over the extent of information that might be stored on an eID card.

The GDPR has specific requirements regarding automated decision making (e.g. by M2M bots). However, that sets legal parameters which must inform views as to whether and under what circumstances an eID may, could or should lend itself to general exploitation (built in mission and function creep and linkage). That in turn must be explained to the public.

Similarly, the life-cycle of data, linked or discrete, is not necessarily dependant on 'liveness of the originator tests'. An ethical question arises as to whether it should be.

For individuals, this implies that the citizen is somehow in charge or in control of how much data he reveals, when and to whom and for what specific purpose. This is often rolled up in notions of privacy.

For commerce and policing, the value of a digital identity lies in its potential to be exploited and linked to other data.

5.2 *Ethics in practice – Issues in the real world*

By comparing eCommerce and airports the clash in understanding of ethical principles raised and arising in practice can be better appreciated.

In the airport setting, for border management, ethical principles focus more on dignity and autonomy, equality and discrimination in relation to controls for border management. The challenges dovetail with those for eCommerce, however, in relation to the use of eIDs in the wider private space of retail outlets across the airport.

It is also vital to realise that the airport setting is a microcosm for wider issues arising through the use of eIDs. The airport setting illustrates both the contextual demands for eID processing (law and order, counter-terrorism, fraud prevention, border control, security) and the societal potential for interlinking information through eIDs for multiple purpose uses.

Aries is aware of eborder control and management issues. Aries focuses on the airside opportunities for committing eID fraud by people using or deliberately 'losing' an eID)such as 'loss' of a passport; airside transfer of an eID to an alternative 'passenger'; buying goods with someone else's eID; claiming to be someone else. So, the ARIES focus is fraudulent use of a legitimate, authenticated and pre-accepted eID by border managers (human or bot). The eID has therefore been accepted at the border control point BEFORE the airside fraud is attempted.

In 2016, the EU underlined its commitment to realising eIDs for those border purposes, by strengthening its information systems, evaluating how law enforcement used VIS (with nearly 23 million visa applications and 18 million fingerprints registered up to March 2016) to prevent and detect and investigate serious offences, assess the use of biometrics and fingerprinting, and strengthen the quality of Schengen border management. To complement existing interfaces, it agreed to set up a Single Search Interface to create a single technical portal to system run by EU-LISA (the EU Agency for the operational management of large-scale IT systems in freedom, security and justice).

The October 2016 European Council supported the Commission proposal for a regulation (tabled in November) on a **European Travel Information and Authorization System (ETIAS**) to allow advance security checks on visa-exempt travelers based on an automated pre-clearance system used to identify possible immigration or security risks prior to the arrival of visa exempt travelers at the EU´s external border. (Commission Communication 2016). It stated:
"While today the information of visa-holders is registered in the Visa Information System (VIS), the only information on visa-exempt persons comes from their travel document when they arrive. Currently, no advance information is available for visa-exempt persons entering the EU through land borders prior to their arrival at the EU's external border. The Paris attacks highlighted the weaknesses of having multiple self-standing information systems making it impossible for those on the ground to ensure a comprehensive check of an individual across all databases. The Commission is working on how to improve the interoperability of information systems for borders and security through the process that it initiated earlier this year." COM (2016) 732 final p.5)

VIS remains one of the most advanced systems of its kind but only half of all issued visas is being checked by Member States against VIS at external borders. The use of VIS for law enforcement purposes remains fragmented. Best practice by individual Member States is to guide improvement.

Undoubtedly controversial have been disagreements between the EU and the US over the exchange of personal data for transport and law enforcement purposes. The arguments over the GDPR highlighted data privacy and reciprocal safeguards for EU citizens regarding the enforceability of their rights in the US. At the time of writing, deliberations over tensions regarding the Privacy Shield had been partly 'resolved' in the

shape of the EU-US 'Umbrella Agreement'. The Judicial Redress Agreement is subject to approval by the US Congress.

As of January 2017, the core principles remained. They reflect not simply legal rules but commitment to ethical principles:

- **EU-US 'Umbrella Agreement' principles**
- **Data protection principles in law enforcement exchange**
- **Purpose Limitation: Clear limitations on data use** personal data may only be used for purpose of preventing, investigating, detecting or prosecuting criminal offences, and may not be processed beyond compatible purposes
- **Onward Transfer -** any onward transfer to a non-US, non-EU or international organisation must be subject to the prior consent of the competent authority of the originating country transferring the data
- **Retention** – retention period is limited. Data may not be retained for longer than necessary or appropriate. Criteria must be published. Decision on acceptable duration must take into account the impact on people's rights and interests.
- **Right to access and rectification** - right to access personal data, subject to certain conditions, given the law enforcement context. Right to request correction of inaccurate entries.
- **Information in case of data security breaches** - a mechanism is to be put in place to ensure notification of data security breaches to competent authority, and where appropriate, data subject.
- **Judicial redress and enforceability of rights –** EU citizens have right of judicial redress before US courts in case of the US authorities deny access or rectification, or unlawfully disclose their personal data (subject to Congress adopting Judicial Redress Bill).

(Source European Commission Press Release Fact Sheet 1 December 2016 Q&A on EU-US Data Protection 'Umbrella Agreement')

5.3 *ARIES scenarios*

The Aries scenarios show how an eID may be used and how Aries eID can create a trusted and dependable eID that is system and culturally neutral. As a result, the myriad legal and regulatory problems that may inhibit adoption of an eID in one country or region but be unimportant in another are irrelevant to the processing of an eID claim.

That means that the Aries eID has the potential to be scalable readily.

The Aries scenarios will test two propositions: (i) eCommerce and mobile eID uptake; (ii) re-establishing an identity when the host document is loss of fraudulently used airside in an airport.

5.3.1 eCommerce

Digitalization of social behavior

One of the key purposes of the Aries project, aside from the securitization of online processes, is to improve the usability and ease which people use online platforms. The usage of these platforms includes the online commercial and non-commercial transactions which are growing and are expected to account for a significant part of all transactions in the near future.

People in developed countries spend, on average, 3 hours per day using the Internet. Studies and surveys focusing on people aged 16+ are very consistent (https://officebrowsinghistory.com/information/how-we-spend-3-hours-per-day-on-the-internet):

- Ofcom estimate: 2.9 hours
- Global Web Index estimate: 3.2 hours
- Nielsen estimate: 2.6 hours
- IAB & UKOM estimate:2.9 hours.

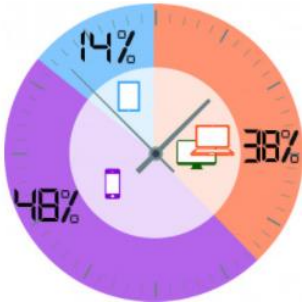

Figure 1: Online time distribution per device [10]

Also interesting is the fact that almost half of the time spent online is through a mobile phone. Online operations and consequently mobile phones are, and will continue to be, an important part of the everyday life.

E-Commerce as part of everyday life and Risk Groups

E-Commerce is on the rise and there is a lot of economic evidence to support this fact. Not only is e-commerce set to reach 4 trillion $ in 2020 as it already has a significant penetration in some sectors (in the clothing market e-commerce already accounts for almost 30% of sales).

The business indicators are encouraging, society-wise the numbers are revealing: Two thirds of internet users in the 12 months prior to the survey promoted by Eurostat, made online purchases in the same period. Overall, the share of e-shoppers in internet users is growing, with the highest proportions being found in the 16-24 and 25-54 age groups (68 % and 69 % respectively). (http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals)

This age group poses a big challenge for all e-commerce players, namely retailers. People under 18 have access to a wide variety of items no suited to their age and often they make the most of the loopholes easily found on both the e-commerce industry and the regulations regarding trade outside the EU - Eurostat reveals that arising trend is observed for purchases from sellers in the EU (from 13 % in 2012 to 20 % in 2016).

Online retailers like Amazon and Instacart have faced problems selling alcohol online. The problem involves verifying the age of the buyer. The retailers must also comply with several other state laws. Regulations that govern the direct shipment of alcohol vary among states. For instance, in April 2015, AmazonFresh withdrew wine and beer from its offerings. (http://marketrealist.com/2015/05/alcoholic-beverage-industry-reluctant-embrace-e-commerce/).

[10] *https://www.iabuk.net/research/library/time-spent-online-jul-dec-2016*

Taking into consideration all of these findings, 3 different scenarios were considered:

- Scenario A – With the objective of measuring the quickness of the enrollment and checkout process with and without Aries;
- Scenario B – With the goal of inhibiting the selling of alcoholic beverages to people under 18.
- Scenario C – with the goal of capitalizing on the recognition of the consumer and its behavior.

Scenario A – Quick and Easy

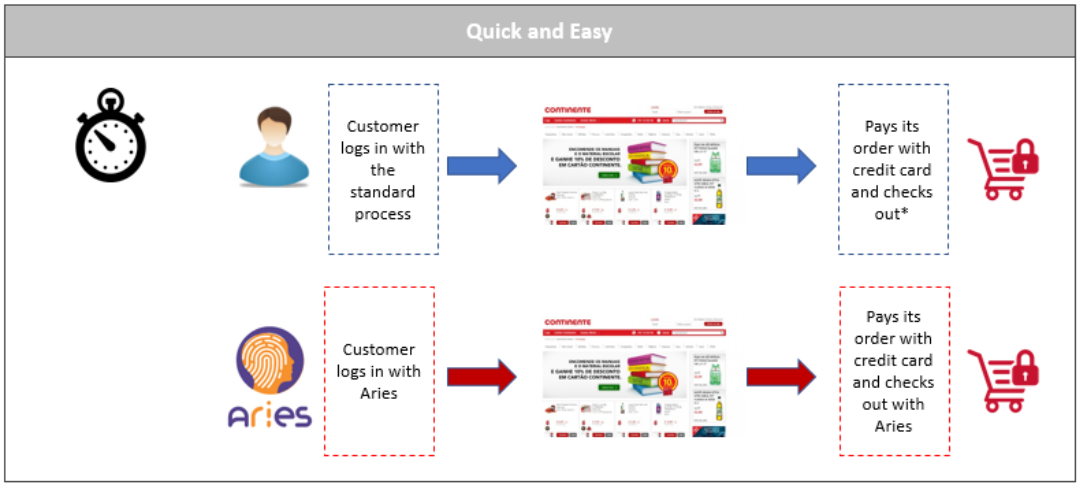

Figure 2: Scenario A – Quick and Easy

1st part

1. Access Continente's website via the traditional process (e-mail and password);
2. Placement of an order of 2 items;
3. Checkout and pay with the standard payment methods;
4. Clock the process;

2nd part

1. Access Continente's website via Aries process;
2. Placement of an order of 2 items;
3. Checkout and pay with the standard payment methods;
4. Clock the process;

The ultimate goal of this scenario is to prove that a biometric enrollment will be more intuitive and quick in comparison with the traditional method.

Scenario B – Alcoholic Beverages

Figure 3: Scenario B – Alcoholic Beverages

1. Access Continente's website via the Aries process
2. Browsing the alcoholic beverage section;
3. Placing an order for 2 alcoholic beverages;
4. Accessing the checkout and payment area;
5. Choosing a slot and being stopped by the system

Scenario C– Recommend Assortment

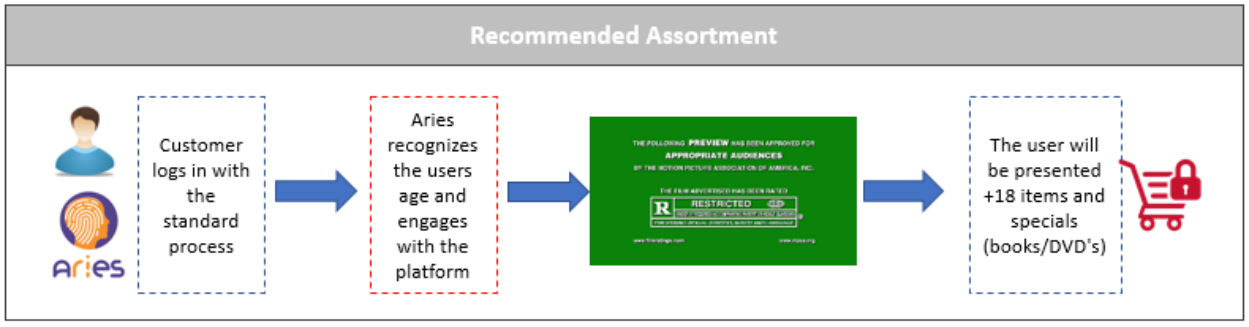

Figure 4: Scenario C– Recommend Assortment

1. Access Continente's website via the Aries process;
2. Browsing the website;

Being presented with pop-ups featuring aged restricted items, eg for people aged 18 or more and special deals, namely books and DVDs.

5.3.2 Airport

The airport scenario illustrates the complexities involved in end-to-end etravel and the potential points all along the chain at which socio-legal and ethical issues arise. Aries is aware of the EU's smart borders (2017) steps (http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586614/EPRS_BRI(2016)586614_EN.pdf) and of the EU's PRADO system (the public register of authentic travel and identity documents online) as a reference point for new designs of potential breeder documents.

The Aries use-case eAirport takes one aspect of the eID and seeks to ascertain how the eID may help to detect and cut fraud and impersonation.

It is important to stress that the Aries eID itself attempts to break the existing problems that arise from the linkage of several pieces of information about a claimant asserting an identity as genuine. It seeks to do so by establishing the connection between an authentic legacy document and an Aries ID relating in real-time to a live human claimant.

In that respect, the elements of the Aries eID do not rely exclusively on a single biometric or data base. Instead, Aries proceeds from the assumption that legacy systems are diverse and incompatible and that a means to overcome that incompatibility must be established to make future eIDs useful in all kinds of settings.

The cultural and societal background is relevant to the human but not, therefore, to an eID that Aries intends to be neutral across cultures and people, legacy documents and administrative systems.

The Aries eID recognises that whereas a biometric may enhance the probability of matching (eg at airport gates), the biometric is not a panacea. Biometric vulnerability must be assessed in relation to privacy and ethical processing: purpose minimisation, purpose specification, and purpose limitation are core requirements informed by common concerns relating to intrusion and fraud. The vulnerability of a biometric system rests on how secure it is against intrusion: even the most reliable systems (in terms of matching a claim to a person) may be vulnerable if they are insufficiently secure. According to the Biometrics Institute (Australia)

The vulnerability of a biometric system to a determined attack depends on three interrelated factors: a secure computing infrastructure, trust in the human operators of the system, and factors that are specific to biometrics. It cannot be safely assumed that a biometric eID system is robust just because communications and data storage are secure, devices are optimized against tampering and protected against external infiltration, and there are robust requirements on auditing and usage policy. 'The nondeterministic nature of biometric matching opens up a number of different security issues, and related vulnerabilities' (BI, 2014).

Biometric matching rests on probabilistic science. However, a biometric measurement and deduction vary every time an individual presents their biometric to a biometric sensor. 'This variation is caused by a combination of user behavior, environmental conditions and physical changes to the biometric due to aging and other factors. Most large-scale testing results on biometrics measure false match and false non-match rates, the former focusing on the chance that a random person has biometric characteristics that are sufficiently similar to pass as that of another individual… This might be by mimicking physical biological characteristics, or by bypassing or altering the information used as part of the matching process.'

From the point of view of the traveller or an airport official, the issues are readily discernible by a superficial overview of a stop-over to change planes, even on short haul, European travel (eg Copenhagen via Amsterdam or London to Manchester). Taking just the one departure airport, the potential efficiency and convenience of using a single eID become obvious, over and above the processing gains which eIDs for physical border controls are expected to deliver as cross-border travel grows as expected. The EU itself first focused on such eID use in February 2008 when it considered an EES. The additional benefits that biometrics, singly or in combination, are believed to offer, were assessed in target operating models (TOMs) differentiated primarily by the number of fingerprints used: the more used the slower: identification is (PE544.477v01-00, p.4). Yet, technological progress eclipses these rapidly. With 5G on the horizon, there is a pressing need to harness the best in eID practice. Trials envisaged for Australia's Sydney airport with Singapore airlines seek to test the feasibility of paperless eAirport experiences for the traveller.

Trustability of the eID depends on its features that render it secure, ethical and privacy protecting. The risks to the integrity of an eID used for multi-purposes are extensive.

5.3.3 The Aries test- eAirpot: theft or loss a passport or identity card

The eAirport scenario envisages a passenger travelling with hand luggage only who has acquired a boarding pass (online paper copy, or e-copy stored on his smartphone; and who then loses his boarding pass – and potentially passport or identity card airside, along with his smartphone).

He wishes to establish with the boarding gate officials that his identity is genuine and identical to that used to gain access from the departure airport to the airside part of this same airport; or the transfer gate at transfer point in a stop-over airport. He discovers his boarding pass is missing. How can he do this?

If he has lost his boarding pass, but retains his passport and has the additional Aries eID, does he benefit from convenience and time gains in re-establishing his claimed identity is genuine? Do the officials trust and gain reassurance from the combined passport and Aries eID to allow either (i) a re-issue of the boarding pass immediately, and the traveller to board the plane/proceed; or (ii) greater belief in the reliability and trustability of the claimed eID? Is this tantamount to increased trust in security, at least among airline staff checking his boarding pass at pre-boarding gates?

In the case of the passport loss, he has to report the loss of his identity card/passport to the appropriate authorities at the airport (most commonly, the airline flight boarding checkpoint; border guards or police at the security checkpoint (if necessary re-tracing his steps to the security clearance area).

Those authorities must then liaise with border and police at the control gate between the land-side and airside entry points to the airport and typically duty-free and shopping areas.

Assuming that those steps can be undertaken easily (which is not yet the case), the passenger then seeks to establish both the legality of his claim to be the genuine human person legally entitled to claim and hold that identity.

The Aries test is to establish how a temporary eID can be generated for immediate use from a pre-existing enrolled Aries eID.

Whether authorities would then accept the temporary/new eID for onward travel is a matter for future research and outside the scope of this project.

However, the Aries project is aware that there are legal and ethical issues that this technical process raises:

- the Aries eID is generated from previously enrolled data in a civil data base
- checking the loss/theft of an eidentity card/passport involves checking specific EU databases derived from reported crime
- civil-criminal data base interrogation by a third party (eg official at an airport) is problematic even though the EU is trying to facilitate appropriate information exchange. Real time live interrogation is not yet sufficiently advanced. Memoranda of understanding/binding corporate rules are not sufficient to cover mutual recognition of different authorities' rights and processes.
- The mere fact of an identity being generated within and from a civil administrative data base (with or without biometrics) and cross-referenced against a criminal database raises ethical and legal issues, especially in relation to by whom and whether this check is registered and held for a specified or unspecified period of time, erased, or retained indefinitely for unspecific purposes

- Biometrics may be held in different databases. They may be embedded in a chip in a paper passport, or recorded in a smartphone. Their enrolment/re-enrolment in an airport setting raises ethical and legal as well as technical issues regarding feasibility and quality of enrolment; what to do in the event of failed enrolment, enrolment for vulnerable or disabled passengers or for potential imposters
- How long and by whom a biometric may be stored differs across jurisdictions
- Single versus multi-modal or multiple biometrics are not fool-proof. Enrolment processes for acquiring the biometric(s) may rely on different technical standards and equipment than those available at a particular airport
- an airline (run for profit by private shareholders) would have difficulty in being allowed access to such information. At the very minimum, the training and background checks on its boarding desk staff and their claims, at the desk, to be who they say they are, would require constant revalidation

Using the Aries eID to purchase say alcohol without revealing more information may be privacy protecting, ethical and convenient for that limited purpose, but re-establishing the legitimate claim to that eID immediately may also be done with an Aries eID.

The Aries eID is intended to remain robust against intrusion because it focuses on linking a live human being claiming an identity to a token that has been already authenticated as genuine. It does not rely on access to vast tracts of additional information or information that is not relevant for the transaction at hand.

Its impact on consent and privacy is therefore neutral. Consent does not have to be sought each time a person uses their Aries eID.

The Aries eID relies on the consent derived when a person applies for an Aries eID and rests on non-linkability of information and purpose minimisation and purpose specification. Only that aspect of information that is relevant to the transaction is to be checked (eg age in respect of buying alcohol checked against destination where the age of majority may vary from state to state; actual match between a biometric and a claimed travel identity, etc).

It is tempting but ultimately self-defeating to evaluate an eID divorced from the wider context of its potential value to all stakeholders. Considering the citizen travelling from Lisbon to Helsinki via London and Copenhagen using their mobile eID for the complete trip, multiple stakeholders have an interest in their digital track starting with*:*

- Online ticket search
- Online ticket purchase
- Online check in
- Online printing of border pass or downloading to smart device
- Association of the travel documents with passport /eID at border control
- Purchase of goods or services at airport (currency, drinks, food, pharmaceuticals, duty free gifts, clothes, sauna)
- Tracking around the airport
- Boarding (from pre-boarding online before arrival land-side to pre-boarding at the departure gate after passport control)
- Luggage from check in (online and/or physical) to physical reclaim
- Onward travel booking (cabs, trains etc)
- Hotel reservations (where relevant, possibly bought online along with the airline ticket)

The traveller does not know who has access to any of the information that s/he provides at any one point. Nor is s/he generally aware of what use will be made of that information; whether it is to be stored; simply used as an 1:n check; linked to other information; or is easily stolen, recorded, re-used for ad-tracking or other purposes; or sold on).

eIDs or epassports are not universal. Ethical issues arise in connection to their acquisition as well as regarding their actual use.

Potential ethical issues that arise include:

- Autonomy and dignity (e.g. harm from rays used by full body scanner as used in Schiphol in the past)
- Inequality – fast track for richer travellers (lounges, fast check-in)
- Profiling & Sifting – whether by eID token or multiple biometrics such as behaviour, age, gait or sifting by dress, colour, race, (no tobacco, alcohol to under 18s, burkas, face coverings, tattoos or masks to deter recognisability by bot/automated gate)
- Indignity (from insufficiency of enrolment, medical impairment, pat downs, strip searches, isolation from main travelling group)

Ethics is a key to gaining public trust in the eID for multi-purpose use. The EU is keen to see the incorporation of ethics as first principle of technical design to ensure trust.

6 eIDs and Citizens – findings from a test for eCommerce

6.1 *Focus groups for eCommerce*

6.1.1 Proof of concept

As an integral part of the ARIES consortium meeting in Porto in September 2017, a specific time was allocated to gather feedback on the features and functionality of the ARIES solution to date and to utilize this feedback to shape future technological enhancements.

This feedback report uses the KPIs defined as a benchmark tool, focusing on the non-technical aspects such as usability and citizen acceptance aspects which align with D2.2. More detailed evaluation of ARIES is undertaken within WP4 later in the project. A video with the Nexus 6 demo workflow was made available online in the private part of the project repository.

This activity took place in two distinct phases. Phase 1 looked at the barriers to adoption / societal issues from 4 different perspectives / contexts defined as personas and highlighted main concerns and potential solutions. The following shows the different contexts and perspectives that were studied and a summary of some of the key problems identified, along with possible solutions.

Context one: A retired person:

Figure 5: Proof of concept -Context one: A retired person

Problems	Solutions
No Credit Card / Prefers Cash	She lets family members shop online for her
Hears bad news on TV about the internet	She goes online and shops and then allows family to access shopping cart to pay using credit card
Doesn't understand terminology used	She has prepaid card with limit
Likes to look at goods before purchase	System sends sms to trusted family member to allow them to approve
Lack of trust paying online	Gadget – to allow voice communication to store if needed
Not tech savvy	Uses smart TV to allow purchases
How to tell a bad shop from a good shop	
No smart phone or tablet / Old Technology	

Table 5: Proof of concept - Context one; problems and solutions

Context two: A middle aged commuter (by car)

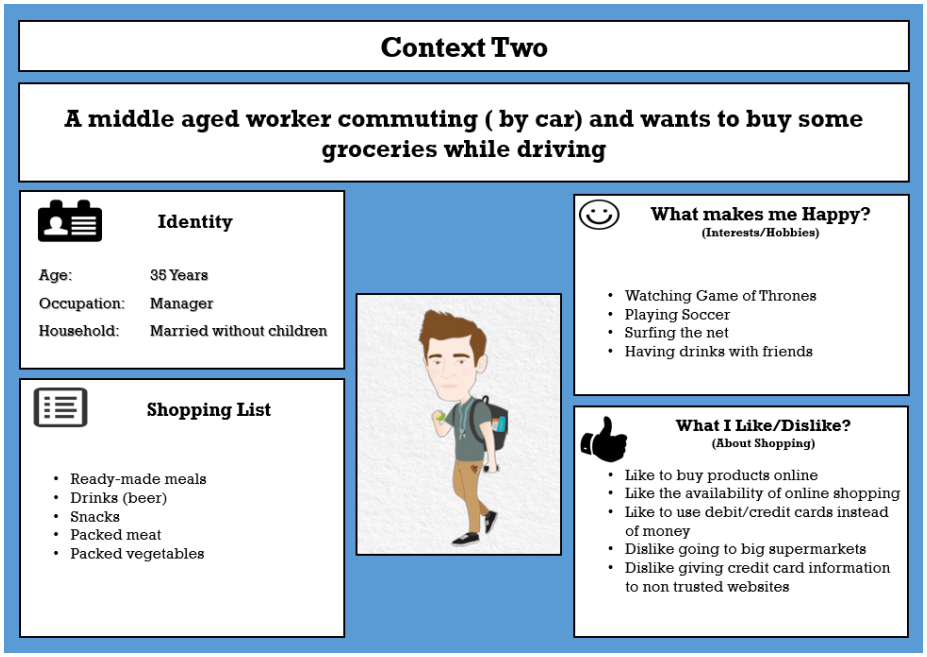

Figure 6: Proof of concept -Context two: A middle aged commuter (by car)

Problems	Solutions
Too much time during purchase might log out / lose the shopping	System has to let user know about stocks; voice app connection
How to narrow the search via voice recognition	Personalised suggestions based on profile
Possible to change address via voice recognition	Pick up in store;
No hand mobility	Voice control
Time spent to make purchase	System has to let user know about stocks; Proof of age: system knows from your profile data

How to prove age in buying alcohol	Voice activation of authentication; AGE proof from system profile stored
Item not in stock -how to offer alternatives	Use personal profile IF ONE ExISTS; system feedback on stock availability
Initiate connection	Pre saved credit card
Can't focus on a screen	Initiate connection : App up and running

Table 6: Proof of concept - Context two; problems and solutions

Context three: A family man:

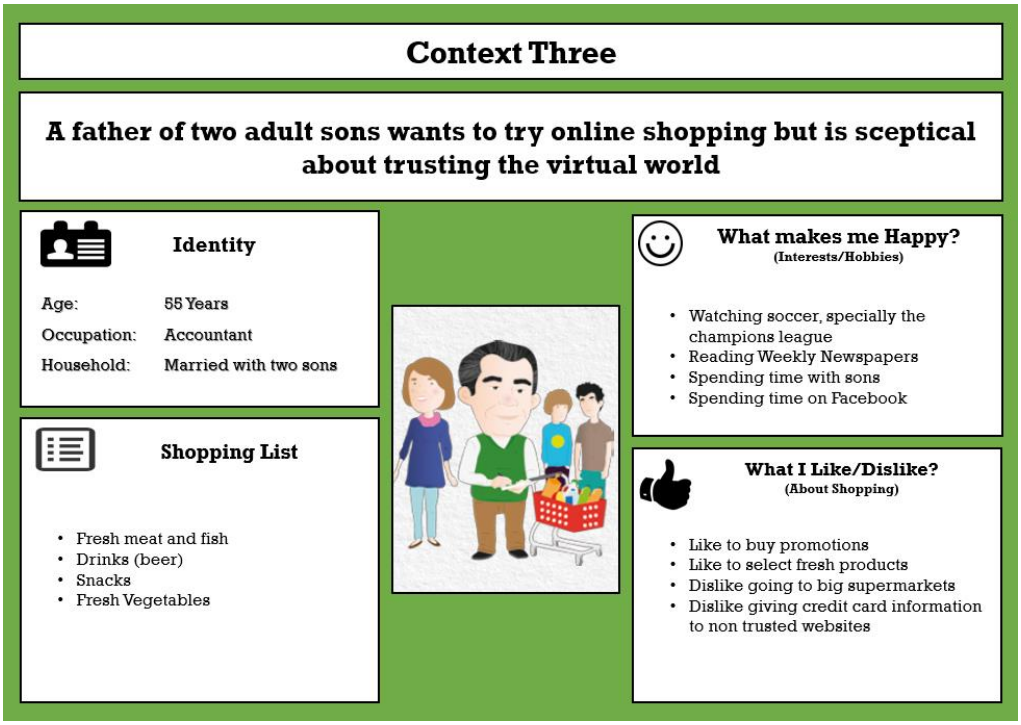

Figure 7: Proof of concept -Context three: A family man

Problems	Solutions
Not having a secure intermediate way to pay at any website	Mass use no consequences - influences
Avoid impersonation by children	Continued use
Lack of concern with digital	Trusting only one player
Conservative	Privacy assurance
Need for factors of trust	Use of digital ID
Having to trust a lot of players	Familiar look and feel
Check out is scary – not trustworthy	Management of payment info single use payment card
Afraid of financial damage (credit card)	Legal obligation on commerce company (liability)
Candidate for age verification	Different payment options (Payment on delivery)
Intuitive eye sight	Incentives after first use
	Security privacy seals
	Feel supported in case something goes wrong

Table 7: Proof of concept - Context three; problems and solutions

Context four: A middle aged commuter (by metro)

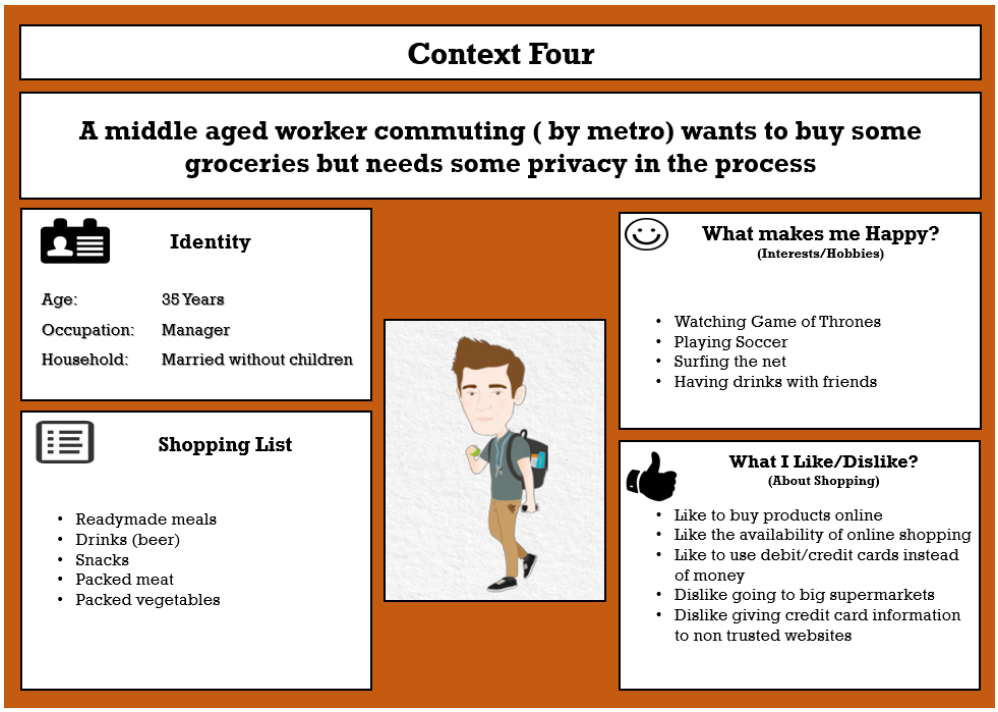

Figure 8: Proof of concept -Context four: A middle aged commuter (by metro)

Problems	Solutions
Control of data to be disclosed	Anonymous baskets
Someone sees where I live	Plastic protection film (phone screen – privacy)
Easy to initiate	Privacy by design software
Secure storage in case of losing phone / device	Level of assurance
Credit card usability in metro	Pay on delivery
Someone sees your PIN code	Personal passwords in crowded places
Time for first registration website	Learning buying patterns from specific websites
Having to confirm age	Importing profile for other websites
Interruption of internet connection	Automatic log out/deletion of order details
Time	LOG out automatically without transaction being completed
Typing and been seen	
Unlocking phone in public	
Anyone can see credentials	
Having to choose personal items in public view	
Trust in the sender and entities	

Table 8: Proof of concept - Context four; problems and solutions

Following this part of the workshop, the second Phase of the workshop was undertaken. The ARIES "mocked -up" solution was demonstrated to a group of people who were not actively involved in the project but did understand e-commerce. They ranged from frequent on-line shoppers to occasional shoppers and were a

mix of men and women aged from early 20s to late 40s. Feedback on look and feel and enrolment were sought.

Each person tested the ARIES solution using their own passport / electronic ID. Passports from Portugal, Spain and UK were tested on the system.

The Mock up test used two different Apps as part of the ARIES solution. The first consensus from all participants was that these two APPs must be integrated into a final ARIES app covering both registration and authentication.

All participants felt the registration process was too long and some steps must be removed – in short, the process must be optimized and be quick. All also felt more guidance and "how to" including video clips and "help boxes" were needed to avoid issues.

If the system failed at any time, it was suggested that a reason should be provided in order to prevent repeat attempts. The reasons for this related to such things as the passport chip being unreadable, possibly owing to damage/ not working, meaning that registration would never be possible.

All participants were satisfied with the authentication process: it was much quicker than anticipated, and acceptable to all participants. However, while it took on average one minute, participants agreed that a faster process would be better in terms of customer satisfaction and confidence.

The QR code reading and MRZ code were problem free and fast, taking less than 1 sec to process.

The chip reading process was not altogether smooth: it was the process that resulted in the need for the most guidance to be given during enrolment to help avoid errors. These errors were mainly due to the operator not holding the phone in the correct position over the passport. The next main issue occurred in relation to the placing of the phone correctly to allow the facial recognition technology to work.

In summary, the look and feel was scored at 9 out of 10; with usability, as 7 out of 10 (where 10 was the highest score possible).

All felt that additional biometric aspects should be investigated to allow citizens other options – voice / fingerprint and iris were all specifically mentioned, in addition to the current facial technology used.

When fraud prevention was discussed, the secured vault was deemed to be a good idea if it helped police investigate crime but more importantly helped people recover from an ID loss or ID related crime. However, security was a concern and reassurance that access was only to be allowed to agencies such as Law enforcement within an ethic-legal framework.

One last point raised during feedback concerned ensuring that a citizen's details once supplied to the ARIES app were secure and could not be changed by the individual. (HOW would change of address/bank be notified?)

During the testing process an attempt was deliberately made to commit and ID fraud. One participant used their passport to register on the system and then a person other than the passport holder tried to authenticate using the facial recognition system. This was immediately rejected by the system as the passport photograph did not match with the individual using the facial recognition authentication. This rejection reassured the participant of the system's operational functionality.

At the end of the tests all data was deleted from devices and the Apps deleted from the NEXES phone used to ensure compliance with EU law.

Overall, this mock test provided positive feedback. All could see the benefits of using an ARIES solution

6.1.2 Scenarios deep dive

Regarding all the contexts of usage and applicability of the Aries solution, the *"Metro Commuter"* has the most potential of impacting the development of the project and the acceptance of the technology by the market. The relevance of the context is proven by the results of the questionnaires, in which the privacy of the processes seems to be an issue with consumers overall.

The contexts were developed in line with the consortium hypothesis of pain points of consumers, these hypotheses which were later tested by the questionnaires were as follow:

- **Context One** – Senior citizens have issues performing the current and traditional log in processes;
- **Context Two** – A hands off authentication is a promotor of online sales;
- **Context Three** – Lack of trust in current online certifications are a detractor of online shopping on 55+ consumers;
- **Context Four** – Privacy is key in an ever-increasing number of people who perform online operations on the daily commute;

After a preliminary analysis of the results it was possible to rate how severe the pain points were for the consumers:

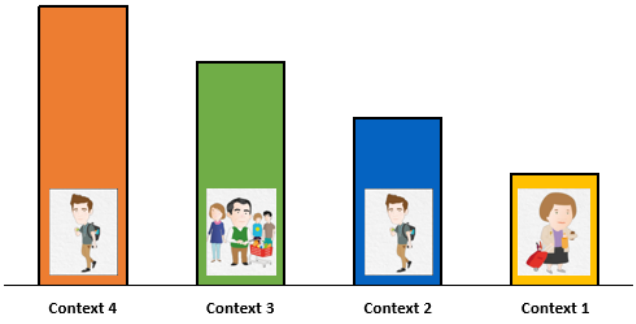

Figure 9: Contexts rate

Moving forward with the project it is clear that much of the focus should be on developing and marketing Aries as a state of the art private and secure technology for the consumers.

- The predominance of **privacy** in online operations may be strongly correlated with the aspects of a urban and busy lifestyle, which often results in people having to perform personal tasks in public and crowded places, may they be trains or cafes/restaurants. This is typical mainly among younger people more familiar with and attuned to the digital world;

- **Security** against fraud is an obvious concern, regardless of age as everything from buying groceries to money transactions can be done, and are being done, online. Such things require trust in the process, however, there is both a demand for enabling technology and implicit acceptance of insufficient knowledge related to this pain point.

- **Intuitivity/Speed** Consumers are interested in having solutions which speed up the current processes and are as intuitive and simple as possible, something valuable to all age groups. However, having instinctual log in detached from an equal intuitive website has less value to less tech-savvy people. Moreover, ethical principles of equality and accessibility are undermined by financial constraints that deter people from buying the relevant technological devices, and/or among those who do not wish to conduct transactions online.

6.2 *Lessons - Prevention as best practice*

ARIES ethical principles relate to three main areas in respect of eIDs

- enrolment of citizen information, especially 'biometric' data (autonomy, dignity)
- technical reliability (limiting falsifiability, fraud, misuse, degradation, robustness against intrusion, vulnerability and transferability across multiple settings)
- compatibility with societal values relating to online life (IoE, accessibility, cost, purpose specificity, doing good for society, preventing harm to the vulnerable, ethics).

The overriding ethical principle is 'do no harm'. Doing no harm to a data subject or to society is a matter of judgement and may change over time. Principles of fairness, self-determination, necessity and proportionality are designed to inhibit wholesale, unthinking collection of data for imprecise purposes. Problematic for citizens is the idea that a person's information may be used sometime in the future by someone or something (a bot or agency) unknown to him when the data was originally generated from the genuine living person himself. The future use for unspecified purposes generates distrust.

Distrust inheres in potential use; potential mandatory costs; and probable inconvenience of enrolling data for eIDs which will inevitably have to be renewed periodically, probably at the personal cost of the citizen.

The unknown creates a sense of suspicion that leads to distrust if there is an absence of honesty and transparency from the outset by those requiring that a citizen generate and use an eID.

If eID use is to be sustainable, then demonstrating its ethical design, ethical enrolment, handling and use for purposes deemed legitimate and ethical by citizens would seem advisable.

The best practices in tackling ID crimes start from the premise that prevention is highly desirable but in practice often unattainable owing to numerous factors. These include:

- poor user 'security hygiene' and/or awareness in terms of protecting passwords, devices, updating software which may result from a lack of knowledge, or more often, a lack of resources to spend on updates
- antiquated software and hardware use by cash-strapped agencies, including government departments, as in the UK and its National Health Service, 90% of which relied on Work XP in 2016 for which automatic security updates had ceased in 2014.
- Organized crime
- Availability of law enforcement resources
- Generalized cybercrime and attacks by state sponsored agencies at all levels

eID adoption for payments for goods and services online is compromised by eCrime and poor data handling and security practices (as evidenced by rising data breaches, the lucrative market in data, and rising ecrime statistics). Barriers to adoption arise primarily from societal skepticism over the vulnerability of eIDs to impersonation, fraud and theft. For citizens, if re-establishing the authenticity of their claim to own their own eID is difficult, takes a longtime, is expensive in time and money, is inconvenient and incurs financial harms,

they may become less inclined to use eIDs). Preventing harms and inconvenience are important elements of establishing a trustable, dependable eID.

Public adoption of eIDs for eCommerce may depend on just how convenient and easy their use is in practice, and how convenient and straightforward re-claiming an identity that has been fraudulently obtained or used is. A future test for ARIES eID would therefore be how citizens can use it to re-establish their legitimate, authentic identities derived from legacy eIDs or paper documents.

Overall the public still have some issues regarding e-commerce but those are fading, namely when considering the timeline of future technologies potential and implementation. [see Appendix 1]

Previous and contemporary work on eID use has focused on interoperability and encouraging eID uptake by citizens primarily for the benefit of eID vendors. Privacy was seen as the major barrier to adoption, and PETs and privacy by design as possible solutions. The *Future eID* project concluded that there was a need to cut upfront investments in eID and costs for businesses to setup or move to eIDs and avoid prohibitively high transaction costs; boost functionality; and support user-friendly eID use on multiple devices to augment uptake by citizens, coupled with trustworthy, strong authentication and signature for application and service providers. The necessary security infrastructure to provide reassurance on security, trust and privacy concerns society may have was also seen as crucial. The challenge remains to integrate existing ID services into a universal authentication service.

ARIES seeks to go beyond these to provide a technically acceptable solution with due attention being had to recognising the ethical concerns that digital life and digital eIDs pose for society.

6.3 *Ethical privacy as an opportunity to overcome societal barriers to adoption*

Societal barriers to eID adoption are often conflated with privacy issues. Privacy itself has been commodified. In the EU, it is part of the underlying commitment and legal framework designed to protecting citizens' fundamental rights. It also has implications for other states handling EU citizens' data. This is where the privacy-ethical links and barriers become clearest perhaps: barriers in one member state may not be as intense in another member state. Some barriers are generic. As the use cases show, perhaps the biggest ethical concerns arise not from the eID itself but from the use to which information about behavior and transactions can be inferred, re-purposed, spliced, re-configured, re-used and linked.

The ethical clash: industry v the citizen?

An implicit judgment of those mining and extracting information from data (and not just Big Data) is that the work is ethical in and of itself because of it will realise the claim that the results will benefit mankind. Again, this is contestable insofar as there are areas where citizens (whether well-informed or not) may not be comfortable with their data being accessed, or may disagree as to the legitimacy and ethical nature of the work being undertaken. Moreover, how any such may be used or mined in future, when citizen values may have changed, is unknowable.

There is an explicit view that companies generating insights from Big Data can both legitimately appropriate, use, 'own' and sell the results and that itself is legitimate and ethical. Some term this a libertarian-inspired 'finders, keepers' ethic. (Sax) This rests on unconvincing assumptions which are increasingly challenged by the public as they remain to be convinced that the greater good of society is subordinated to that of the profit motive for commercialisation of Big data insights derived from personal information. Challenges arise as to the relative weight to be given to the right to privacy (that some see as non-existent and redundant) and to the principle of autonomy, upon which the right to consent and the 'right to be forgotten' rest.

However, the European Parliament is not concerned about the privacy erosion that metadata facilitates. Equally, ethical use cannot be guaranteed. This puts at risk the 'right to be forgotten' and the principle of 'informed consent' designed to enforce the precautionary principles.

Digital tracks and identities themselves present further ethical challenges since anonymity ultimately ceases to be meaningful in digital transactions. However, the right to be forgotten has been interpreted to imply an ethical obligation to grant the same respect to the digital identities and data of deceased people as to the real physical person. Stokes (2015) argues for a distinction between persons and selves and suggests that social network services offer a particularly significant material instantiation of persons: the 'experiential transparency of the SNS medium allows for genuine co-presence of SNS users, and also assists in allowing persons (but not selves) to persist as ethical patients in our lifeworld after biological death.'

The continuing growth in the development of technologies to mask aspects of biometric identities, in the name of purpose limitation, data minimization and preventing mission and function creep, poses additional challenges. Society may be inclined to welcome and wear masks to confound automated facial recognition schemes. The latter are able to extract and soft biometrics (such as age, gender and race) from a face image and make further deductions about that person from stored data without getting consent from the person for wider interpretation (unethical in itself). A PET may, however, facilitate 'differential privacy' by allowing face matching in an automated gender estimation facial recognition scheme while simultaneously suppressing progressively the gender information. (Othman & Ross, 2014). However, while facial recognition software for mobile devices (like phones) seems to offer convenience gains to users, the robustness of the underlying algorithm to combat fraud varies: some phones authenticate on the basis of a genuine photo presented by someone other than the legitimate phone owner, for example.

While facial recognition technology has been advocated by those primarily combating terrorism and crime, its potential for eCommerce eID use is recognised by mobile phone developers. Convenience is a commodity but as the Use Cases' feedback reveal, a contradiction persists - citizen want convenience and do not want to be inconvenienced by intrusion, identity theft and fraud. Increasingly, too, ethical privacy protection is a concern.

Consequently, facilitating ethical use and ethical privacy protection become potential commodities and also features that may encourage citizen acceptance of the underlying applications.

6.4 *Risks, Limitations and further considerations: trust and vulnerability*

The issue of trust is key. A generic vulnerability and risk exists regarding citizens' concern over eiD misappropriation. This breaks down into a loss of trust in the security and robustness against fraud in the event of misappropriation, misuse, loss or theft. This is no longer mitigated by claims that one or several biometrics may guard against fraudulent use of an eID token. Cynicism among citizens as to industry claims relates to:

1. Where technically (token, data base, implant, card) the biometric is stored
2. Distrust over outsourcing any part of data storage to third non-trusted host countries, regardless of to which company or companies, or state enterprises
3. Confusion over liabilities for re-instating eIDs for the genuine person to whom it belongs that arise in the event of loss, theft etc.

There is marked confusion that eID private-public partnerships compromise the trust that an individual person can place in the reliability of his own eID that may be linked to other information without his explicit knowledge or consent. (Link to WP on Law)

Experience elsewhere shows that sensitivity to individuals being unwilling to enroll a biometric for an eID which becomes obligatory by default (at the risk of exclusion from access to vital services) is problematic. In the case of the Australian Card, in September 2016, this was highlighted as a risk to adoption and as necessitating a response which demonstrated ethical application from the outset. Once again, the issue was not the technical feasibility of using the eID but the ethical applications and data linkage possibilities that might undermine privacy and inhibit societal trust.

The Australian Privacy Foundation noted: "The imposition of biometric identifiers may be the measure that completely destroys the social contract between government and the public…"Any discussion of biometrics in government service delivery must commence with an iron-clad commitment that, with the exception of criminal investigation contexts, biometric measures capable of identifying individuals will never be in the possession of a government or a corporation, and that all biometrics will be handled only within the equivalent of a secure PIN-pad."

A generic concern regarding eID uptake has been identified by the EU as Terms & Conditions (T&Cs) which it sees as often being tortuous, too long, and impenetrable to the average e-service user, rendering them 'meaningless' until a person needed to rely on them to seek redress (eCommerce) or reclaimed an eID (travel or bank documents).
(www.ec.europa.eu/consumers/strategy.../policy.../consumer_policy_report2014_en.pdf)

While it is generally assumed, including by the EU, that users will be attracted by the convenience of anytime anywhere access facilitated by an eID, the convenience factor is undermined and renders eID less sustainable if the eID is unreliable across services in terms of access to that service; and if it is relatively vulnerable to attack and misappropriation. eID uptake and sustainable use depends on it being dependable and trustworthy in terms of an individual's ability to establish and easily reclaim a lost eID; (cost, ethics, convenience, vulnerability); reliable in terms of alternatives to eID enrolment for the vulnerable; dependable, reliable, convenient and easy to use in areas with slower internet connections (ie doesn't rely on ultra-highspeed connectivity) and for cross-border transactions (such as epayments).

The cost of acquiring an eID can also be a risk to uptake. Enrolment of biometrics is problematic if there are few quality biometric enrolment offices (in the case of visa enrolment being required at specified foreign embassies, often in a capital city hours away from citizens requiring the visa). Poor quality enrolment of biometrics makes them unusable, for instance, at eGates.

The service provider has a responsibility towards the public regarding ethical practice, and generating confidence in the service provider. This applies throughout the chain and service providers must create and sustain public trust in their assurances about privacy, and onward use of potential linkage to associable data if the eID is to be a sustainable token for e-service access and delivery.

Whereas, data protection professionals may understand these requirements, society at large does not. Instead, the public sees data theft scandals, concerns over spamming, intrusion, privacy and identity fraud. These may deter future uptake of eIDs because there seems to be increasing wariness about the usefulness to citizens of trying to gain redress in the event of their data being hacked, spoofed, mishandled, lost or stolen. Ticking boxes on Terms and Conditions is not seen as optional but essential if the service on offer is to be accessed.

Scepticism on the part of the public presents designers of universally applicable biometric eIDs with problems that must be overcome if the eID is to gain widespread sustainable acceptance.

Through an exploration of biometric eID use in respect of two use cases: eCommerce and Airports, this project identifies points at which ethical issues in the use and onward use of eIDs may arise in order to help designers address those problems with a view to finding technical means to overcoming them.

A socio-ethical analysis helps to isolate key factors that affect (i) the probability that citizens will take-up, retain, see as dependable and reliable, trust and use a biometric eID for the wide range of public and private transactions it could enable across services, legacy systems and virtual and physical borders; (ii) public perceptions of an eID. For citizens and stakeholders an eID must guarantee the integrity of the information and the dignity and autonomy person to whom it relates, and ensure integrity in its use.

Ethical eID design and use requires more than respect for legal requirements, PETs and PEDs. It needs to build in and into ab initio something that allows the citizen to determine what kind of personal information can be enrolled onto it, released by it, in what precise circumstances he chooses, and prevents onward use and linkage in full or part by humans or by automated processing.

Legislative measures to inform and re-assure both stakeholders and users, notably the citizen, are helpful, effective and necessary up to a point. But they are not sufficient to guarantee that practice conforms with ethical standards. For example, the GDPR has specific requirements regarding automated decision making (e.g. by M2M bots). It sets legal parameters which must inform views as to whether and under what circumstances an eID may, could or should lend itself to general exploitation (built in mission and function creep and linkage). That in turn must be explained to the public.

The idea of 'informed consent' is important but insufficiently enforceable for every live transaction and potentially meaningless where automated decision making is concerned. Public trust could be eroded moreover by failures in automated threat detection, so what matters to the public is how, when, by whom and under what conditions an element of their identity may be invoked, shared and used reliably to facilitate a given transaction.

7 Conclusions - Ethical Impact Assessment: fit for purpose eIDs for citizens

The overriding barriers to societal acceptance of eIDs for both national identity schemes and multi-purpose use relate primarily to what is loosely called 'security' but when disaggregated refer to concerns about potential future use by unknown others for unknown purposes. While society may be prepared to make an exception of criminal investigation and international security threat (defined primarily as terrorist threats to personal and territorial integrity and cybercrime) investigations, the idea is resisted that government agencies, PPPs or private companies should retain or access eIDs and biometrics that link to and identify a specific individual. Important as privacy is, the problem for the suppliers and users of eIDs is the relative uncertainty and unknowability of how data could be linked. It is however insufficient to rely either on data protection legislation or on terms of service on the part of all parties to give effect to ethical practice. All must be clear, universally applicable, open, accessible and precise. Ethical principles must be observed and practiced with priority being given to the precautionary principle to ensure fairness, inclusiveness (non-discrimination), proportionality, respect for human dignity, autonomy, accessibility and equality. Ethical practice requires defining and realising precise, specific and limited purposes. ***This limitation may constrain business models that implicitly are based on mission expansion***.

Defining the security exception is also problematic because it changes according to: what falls under the remit of 'security' as contingently defined overtime in different settings; context; and political imperatives. Currently, the single digital market strategy goals, ePrivacy reforms and the GDPR provide the context for the evolving use of eIDs for multiple purposes. There is a duty of care on the part of all to ensure that eID design, handling and use are ethical and comply with ethically informed goals and practices.

7.1 *Recommendation*

Feedback from the focus groups and questionnaires suggest that there are technological gaps and weaknesses in the creation and prospective use of eIDs (uni-purpose versus multi-purpose anytime anywhere) and gaps, confusion and conflict among citizens already using eIDs for travel and eCommerce.

It is clear that citizens are motivated, as individuals, to use eIDS primarily as a convenience. Usability, ease of use, speed of enrolment, and convenient access to a device enabling fast enrolment encourage eID use on smart devices. Current and prospective convenience for the individual reflect an individualistic approach to e-transactions of all types. The impact primarily on the self, not on family or on society, condition this. However, there is an inherent contradiction in this generally fairly uncritical approach to accepting eID use for convenience and speed, with a less cogently articulated concern over security and privacy. Individuals as consumers do not want to have to take responsibility for security and privacy, or for ensuring and checking a vendor's compliance with legal requirements and ethical practice. Instead, the want to take for granted that all vendors comply with the highest standards: they expect ethical and legal compliance to be 'baked-in'.

What this means for business models is that a business case must acknowledge from the outset that claims regarding ethical practices in respect of secure data handling and privacy are genuinely robust. A business model that relies on robust, independent ethical impact assessment s and privacy impact assessments might, therefore, be expected to generate higher citizen uptake if the claims are:

- Credible
- Sustainable
- Trustable
- Dependable
- Independently validated

- Current

These apply to private and public service providers. It is no longer credible or justifiable for providers to place the onus on the individual citizen for checking T&Cs and compliance and adherence to PIAs and EIAs.

Educating consumers to be more aware and better informed about the eIDs they buy or use may be desirable in its own right. However, it is not feasible short term. Individual responsibility is not credible as a goal or an excuse for non-compliance given that an eID purporting to be as neutral as possible must not implicitly assume a degree of tech savviness on the part of the user, nor discriminate against the vulnerable or disabled. Justice requires fairness and equality. Ethics requires attention to the precautionary principle being realisable and implemented.

Technological innovation has not kept pace with the need for ethical reflection and policy awareness of the impact of technology on individuals and on society, or on the obligations of public and private sector providers of technology. Ethical reflection is rare. Ethical design is an afterthought all too often rather than baked in from the start. How might this be remedied? Ethical design practice may be confirmed by identifying and predicting potential:

- linkage opportunities
- privacy harms
- ethical harms that may impact personal dignity, equality, accessibility, consent
- harms that may arise if identity management is insufficiently informed and robust
- ethical harms that could be predicted and mitigated from up-to-date awareness of the incompatible legacy technologies, law and practices in different states

Defining an ethics code and implementing a realistic ethical impact assessment where principles retain their practical relevance and meaning in a changing world of physical and virtual eborders means that it is necessary to disaggregate existing laws (such as GDPR) from business practices (couched in terms of fair competition, IPR, non-discrimination).

Creating a persistent and unique citizen identifier to enable citizens to use and trust their eID for multi-channel access is far from a technical, value-free process. Wearable tech may change the way consumers shop and mean that sellers need to have a means to target and tailor ads to customers in line with analysis of their past behavior. Wearables also store passwords, past purchases, spending, wish lists, payment history etc. The lure of behavioral information deduced as part of biometric enrolment for an eID is growing. It is problematic in the EU where a stricter definition of biometric has existed compared to the USA, and where advertising tracking and unsolicited ‘suggestions’ based on past behavior or NFC deductions have provoked data and privacy protection concerns. Moreover, as the ECRIS-TCN discussions have shown, even where criminal law is concerned, the cross-border exchange and/or interrogation of fingerprint data is problematic given the different legacy systems of the EU27: states diverge over whether or not such data is held separately from other criminal data as well in terms of the technologies, law on whether prior convictions are held (alphanumerically or not) and local practices.

Regardless of the type of biometric(s), for the developer and user, the challenge is to ensure that the integrity of information on the eID token is preserved and safeguarded from intrusion and degradation, for example. Both could potentially compromise the ability of a citizen relying on an eID to access services and participate in the digital market. For *all* citizens to use and see an eID as dependable, reliable, secure and trustworthy, (and see its supplier in the same way), there must be assurances that the personal information associated with the eID cannot be used in compromising ways; in a manner that allows unethical onward use; or for any purpose that may have undesirable consequences for the citizen as an individual or as a part of society. In practice this would mean designing a neutral, universally usable eID that

1. Allows the eID owner to determine the release of relevant information (in full or in part);

2. Designs ethical practice into the neutral eID in recognition of differing, complex terms of service that vary from supplier to service supplier, and from system to system, all of which are diverse. A neutral eID would also recognise that legacy systems and legal rules, compliance and implementation are not uniform across the EU.
3. Allows citizens to rely on the eID as being robust and ethical in any setting (within the EU) to access goods and services
4. Allows to use alternative access means simply and at no extra cost if their eID does not function, is unusable or is incompatible with legacy system
5. Enables citizens to opt not to access a service using an eID and not be disadvantaged if they do not wish, or cannot for whatever reason, use the eID. This may also happen if they feel uncomfortable with the terms of service (assuming they read and are aware of them. Most of the time, the terms of service are far too long and complex so users/customers do not give informed consent but feel they have to 'agree' in order to use the platform for e-transactions.
6. Addresses the potential for harms that may be anticipated (or predicted) as eIDs become, as per business model, the dominant way that citizens access services (private and public)
7. Has robust security against third party misuse for whatever purpose. (It is unethical and unsafe to assume that competition law, intellectual property rights law, or privacy laws are sufficient to protect citizens from risks arising from third party platforms used in eCommerce
8. Is open about bias that is baked into the design and application of algorithms (designed and used or misused for good or ill)
9. Is open about moral problems baked into quality standards governing the design of apps: a code of algorithm ethics implies some consensus over how trust in eIDs is to be baked in, regulated, supervised and enforced
10. Builds robust accountability and transparency requirements into eID use.

From the practical perspective of the private and public sectors relying on eID, it is clear that ethical reflection and EIAs are only beginning to be on the radar. Due process has also to be taken into consideration.
The ethical principles of necessity and proportionality must be taken into account when considering the monetization of eIDs but 'unethical' uses will eventually deter uptake. Ignoring ethics may jeopardise the sustainability and expansion of eID use.

Ethics implicitly drive transparency and accountability demands. Citizen expectations change and recognition of how everyone creates data but big layers, corporation, governments and monopolies tend to make commercial gains from it, could be problematic and lead to citizens doubting the legitimacy and acceptability of eIDs and technologies developed ostensibly in the public interest. At the same time, it is important to avoid creating the impression that an unbiased 'ethical algorithm' could be a substitute for human judgement informing design, terms of service and decisions. Getting clarity over how ethical boundaries can be defined and enable public acceptance and trust is necessary. Safety critical limits and human-to-machine and automated decision-making failure need to be explained to citizens, along with the ethical reasoning behind their use, machine-learning and its implications.

Exaggerated claims as to the infallibility of a given technological application (as in the case of eIDs used with biometrics) are inappropriate: they potentially endanger public and societal acceptance, use and trust in them in the following circumstances:

1. Poor enrolment of biometrics
2. Weak storage of data that results in degradation
3. Poor data handling practices locally
4. Data transfer/ re-sale processes
5. Corruptibility of biometrics: poor enrolment, degradation, loss, theft, cloning, impersonation irregularities

6. Absence of appropriate, alternative and proportionate alternative verification and authentication processes in real time in the event of system failure or of system being unusable for a person (for whatever reason e.g. erosion of finger print, physical deterioration, infirmity, age, capacity). Alternatives must be available if multimodal biometrics are to be trusted and used.
7. Reliance on eIDs being recorded on smart devices associated with the person: alternatives are needed in event of device malfunction, loss, theft, info-cloning (NFC) or of a person not possessing such a device. The mere presumption that everyone has and uses a smart phone raises ethical concerns since large sections of society are unable or unwilling to afford such devices and their running costs.
8. Inconsistent functioning of the eID resulting from the different terminals that may validate them in different locations (commerce or airports within same region or beyond state borders)

It is vital to define precisely the limited purpose for which an eID algorithm has been created; and to be open about issues around how inter-operability and portability promise convenience gains to citizens IF certain conditions are met. Insufficiently resilient eIDs, and those not informed by the principles of ethics by design risk allowing greater scope for intrusion and manipulation (mission creep, info-seep). Information linkage has commercial advantages. It is key to security intelligence. At one level, this may be desirable (eg linkage of info for public sector service delivery, maximizing Big Data and Open data potential). At another level, it is risky and potentially harmful.

Automated decision making (bots, AI, 'smart' interaction) could deny a person a necessary service or puts them at risk of physical harm (non-entry through a smart border gate, inaccessible bank account, or a smart self-driving car being unable to decide whether to swerve or hit a person or animal). The GDPR may cover automated decision making but does not cover the potential harms consequent upon actual physical harm. Instead, developers have looked to issues about liability, and liability insurance. Both are necessary but insufficient. Built-in ethics by design may eventually deal with this, just as PETs, de-identification protocols, quantum proof encryption and privacy by design are to improve cyber security and boost smart resilience against cyber-attacks. (ENISA,2017).

The cost and complexity of monitoring compliance makes more vital the development of a trustable, dependable technical ecosystem to guarantee privacy, build and sustain sufficient trust. Demonstrating trustable, dependable and resilient eID is needed so that society adopts eID use more readily. The EDPS's emphasis on ethics by design for a digital society cannot be ignored. (EDPS,2017). Public trust in eIDs will also be undermined if citizens find their eIDs are easily compromised once they realise that they have lost control over much of the data their digital footprints generate.

It seems that the EU values the concept of auditable ethics codes reflecting openness and honesty regarding compliance with good administrative practice (including audit trails, accountability, disclosure and transparency), high technical standards, robust security, and timely compliance with legal requirements. In realising the DSM, however, it is insisting on baked-in ethics by design.

Towards Ethical Practice: from code of conduct to Ethical Impact Assessment

The EU has considered how ethical practice may be required and applied in smart environments. Looking to voluntary adoption of good practice, a code of ethical conduct for robotics engineers has been devised in 2017. It offers a set of principles and guidelines for actions for all stakeholders. The preamble stresses responsible action 'with absolute consideration for the need to respect the dignity, privacy and safety of humans'. (PR\1095387EN.doc 15/22 PE582.443v01-00 EN) It encourages, from the outset, risk assessment of the future implication of the technologies or objects being researched and the development of a culture of responsibility vis-à-vis future challenges and opportunities. Given the prospect of automatic decision making, it notes that the code of conduct should consider humans, not robots, as the responsible agents.

Fundamental rights are to be respected and design, implementation, dissemination and use are to respect the interests of individuals and society.

The code of conduct is designed to ensure the highest ethical and professional conduct by humans upholding specified principles. These can be adapted to the eID scenarios. The principles are:

- Beneficence – action in the best interests of humans;
- Non-maleficence – the doctrine of 'first, do no harm';
- Autonomy – the capacity to make an informed, un-coerced decision about the terms of interaction;
- Justice – fair distribution of the benefits, and affordability.

The code of conduct is instructive because it provides guidance to the engineers behind the technological developments, requiring them to be aware of potential uses and risks. It places responsibility on them to implement the:

- precautionary principle, anticipating potential safety impacts of outcomes and taking due precautions, proportional to the level of protection, while encouraging progress for the benefit of society and the environment;
- Inclusiveness and transparency to guarantee respect for the legitimate right of access to information and participation;
- Accountability for social impact on current and future generations;
- Safety – meaning that as well as preserving wellbeing and respecting human rights, prompt real-time disclosure of potential harms is essential;
- Controllability and reversibility as conditions to enable safe and reliable applications, allow stakeholders to undo the last action or sequence to get back to the 'good' stage of their work, and so build trust;
- Privacy – as per GDPR, secure information storage and use, and commitment from developers and stakeholders to develop and follow procedures to ensure use with legitimate and appropriate valid consent, confidentiality, anonymity, fair treatment and due process, including the destruction and/or of related, linked data.

The code refers to the need to minimise harm (and defines the risk of harm as being 'no greater than that encountered in ordinary life, i.e. people should not be exposed to risks greater than or additional to those to which they are exposed in their normal lifestyles'). This is too fluid an idea to be implemented for eIDs. Consequently, the focus must be on respecting the precautionary and proportionality principles uncovered in a risk assessment of how the system operates. This should extend to organisational and governance structures and be undertaken by competent people in an independent, multi-disciplinary ethical review system.
A licensing system for designers may be appropriate.

7.2 *Ethical Impact Assessment- a Guide*

An EIA must start from the commitment to upholding the overarching primary precautionary principle of ethical practice – that of 'doing no harm'.

The precautionary principle means going beyond privacy impact assessments and compliance checks. It means awareness of how ethical principles may be inadvertently compromised in practice, through business case models, scalability, built-in back doors allowing additional functions or actions to be performed in future for vague purposes. It means awareness of how, why and to what ends potentially more information may be

collected than is necessary for the initial specified purpose, how it may be disclosed or linked, and how necessary or justified (and under what circumstances) any linkage may be.

Privacy Impact Assessments typically cover issues of necessity and proportionality, compliance and liability, privacy by design of technology, through privacy enhancing technologies (and their antithesis – privacy intrusive technologies), by intent of legal regulations, and steps to prevent negative privacy impacts. They cover issues like good data management and handling practices, quality controls, peer and independent audit trails, reviews, updating, access controls, encryption, accountability and transparency, obligations regarding breach notification and reporting, error correction, compliance with legal requirements, privacy risk mitigation and issues of direct or implicit consent and the 'right to be forgotten'.

The above is relevant and necessary to EIAs but are not sufficient. For the precautionary principle to be safeguarded, assessment must be current and checked against technological developments which may accelerate identified risks or which may mean that a business case for doing something has to be re-evaluated (and possibly ditched).

The second guiding principle therefore is just because something can be done, does not mean it should be done. What is technically possible may be highly unethical. Unethical use and practice must be identified openly and, preferably at the design stage, steps taken so that it can be prevented. An EIA potentially could complement data protection and privacy impact assessments. Under the GDPR, data controllers must carry out data protection impact assessments (DPIAs) to 'evaluate, in particular, the origin, nature, particularity and severity' of the 'risk to the rights and freedoms of natural persons' before processing personally identifiable information. The DPIA must include measures, safeguards and mechanisms envisaged for mitigating identified risks. The same applies to an EIA. For neither would it be acceptable to omit identifiable risks to try and evade such responsibilities. Trust, reliability and dependability are key to sustaining eID use and interoperable rollout across sectors.

Conducting and EIA should help to avoid that. Coupling a neutral eID, as envisaged by Aries, would be a contribution to constructive an ethical digital ecosystem for citizens.

7.2.1 EIA Template

An EIA template should be developed in conjunction with the Aries Ethics Principles Guidance Sheet

Summary	Precise purpose of the project Reason for the EIA (including review when a new or more intrusive or unexpected app/use of data and purposes become apparent) Overview of Information flows requiring EIAs Key findings Reference to any remedial action recommended
EIA Methodology	Overview of approach to the EIA, reference to groups consulted, stakeholders and any relevant legislation or guidance
Description of App/project/ business case	Outline objectives and rationale, scalability potential and cross sectoral relevance, time frame and likely life cycle of app
Information management	Outline the source, mechanisms by which information is collected, used, transmitted and stored; state what kind of and how information is handled; how and why it can be shared; how sensitive information is protected; map potential linkages; highlight goals of ethical practice; and state how information is protected from inappropriate disclosure and

	mission creep
Analysis	Refer to precautionary principle and say how it is addressed; Impact evaluation (state positive and negative features) and include compliance with ethical principles (eg as in Aries Ethical Guidelines); and refer to independent ethics audit, accountability and transparency trail.
Recommendations	State how risks might be remedied, minimised, and prevented
Conclusion	Summarize response to feedback and findings. Define next steps.
Documentary evidence	List of participants; legislation; consultative exercises; and cite relevant sources for more detailed information

Table 9: EIA template

When should an EIA be conducted?

- When a new app/ data collection, re-use, splicing in full or part by human or bot or use is under discussion, including any automated analysis/use/decision making relating to existing data
- When personal data is used or collected for verifying authenticating, profiling, analysing or using biometric data for any purpose, or where it is to be linked to other data that exists or is to be created or accessed
- When a common platform is to be established to be accessed by (for specified purposes) or used by several different parties, including government departments alone or together, and when they work in public-private arrangements with outside agencies to whom parts of the business are outsourced, or involve a common processing arrangement across an industry sector or segment or countries and industries; or involve horizontal information access, processing or sharing.

Why conduct an EIA?

- To evaluate the likely impact of a new app or innovative use or data linkage potential on society or individual citizens; and to assess the probability of risks (ranking them from low to high), and taking the nature, scope and content of all processing associated with the business case and the sources of potential risk into account
- To mitigate risks of automated decision-making compromising or harming citizens
- To mitigate risks to citizens
- To demonstrate openly trustability, dependability, accountability and reliability
- To demonstrate awareness of the impact on society of the steps envisaged by the new process and/or app/tech
- To increase legal certainty of compliance with highest standards of practice and highest quality standards
- To give a trustable face towards citizens as well as stakeholders
- To develop or enhance and sustain reputation as a respected, trustable, reliable market leader

Who should conduct and reflect on an EIA?

- Initial EIAs should be conducted in-house by all parties and stakeholders involved developing and rolling out any new process/app/technology adopted
- Independent audit trail potential should be piloted inhouse and then submitted to an independent Ethics Body to evaluate any potential impact on citizens and society
- Independent Report feedback should be taken into account as the app/process is developed or modified or abandoned. That report should pay particular attention to identifying and mitigating risks, and make appropriate recommendations relating to the risks, regardless of potential cost implications to the developers

Potential benefits

- Early identification of potential pitfalls and points that might lead to breaches of the precautionary principle and/or compromise the integrity of the original specified purpose associated with the innovation
- Early recognition of the above means that remedial action can be taken immediately and this, early on in the design of a process/app are less costly than modifications that have to be taken later on in order to comply with ethical requirements
- Increased awareness of ethical practice and obligations for technical, administrative and sales staff
- Respect, trustability and reliability gains to the developers and stakeholders which may enable them to help shape future related policy and practice
- Sustainable trustability and dependability as a business case
- Society and citizens gain confidence in using and accessing the service(s) and the provider associated with the eID

8 APPENDIX 1: ARIES survey

About you

1-Please rank yourself in terms of your internet use:

- Very Confident
- Confident
- Somewhat Confident
- Basic knowledge
- New User

2- Does your home have any 'smart' device (eg. smart phone or table) which allows anyone in your house to buy goods or services online (eg. Amazon's Alexa or Googlehome)?

- I don't have any device of that sort
- Yes, and it is only used by me/by one person
- Yes, and it is used by the whole household

3- Do you use the same device for all your online activity (eg. social media, online shopping) regardless of the main purpose of your devices (work/personal)?

- Yes
- No

4 - Does your employer have a policy on using your own device at work? This is known as the BYOD (Bring your own Device)

- Yes, and it enforces it
- Yes, but it doesn't enforce it I don't know
- No/Not Applicable
- I'm self-employed and have separate devices
- I'm self-employed and only use one device

5 - From the list of online operations below, is there any which you wouldn't do using public wi-fi?

- Online banking
- Online shopping
- Social networks
- E-mail
- No
- Other

6 - I use my smart device to pay for goods and services because...

- I trust it to keep my information safe as it's with me
- I forget passwords and it is convenient
- I prefer it to using debit/credit card
- I don't use any device to pay for goods and services
- Other

7 - I don't use my smart device to pay for goods and services because...

- My device doesn't have that capability
- I prefer using cards or cash
- I worry about how safe my stuff is on the phone if I lose it or if it's stolen
- I use my device
- Other

8 - Which online payment are you most comfortable with/use the most? Please tick all relevant ones you have used:
Credit card
Debit card
Paypal (or similar)
Virtual wallet
Other

Your views on privacy

9 - How concerned are you about your privacy when using the internet to search and pay for goods and services?
- Not concerned
- Somewhat concerned
- Very concerned
- I don't use the internet to pay for goods and services

10 - On a scale of 1 to 5 (5 being completely and 1 being not at all) please rate how much you trust the following entities with your data:
- Social networks
- Popular Internet Companies
- Banks
- Insurance Companies
- Public authorities
- E-Commerce Sites

11 - I have the location function active on my device because:
- It makes me feel safe
- I like getting location-specific suggestions (eg. Traffic Information)
- I don’t know whether it’s active or not
- I don't use it

Online Shopping/ Ecommerce

12 - How concerned are you about security in relation to making purchases over the Internet?
- Not at all concerned
- A little concerned
- Somewhat concerned
- Very concerned
- I don't make purchases online

13 - Have you ever been a victim of ID fraud (eg. Phishing emails) online?
- Yes
- No

14 - Are you willing to share personal information on a website provided that you will benefit from special offers and discounts?
- Yes
- No
- It depends on how well I trust the brand/site

15 - How concerned are you about buying goods or services online from an EU country other than where you currently are?

- Very concerned
- Somewhat concerned
- Somewhat unconcerned
- Completely unconcerned

16 - Does the location of the supplier influence the level of trust you have when making an online purchase?

- Yes
- No

17 - What do you like about buying goods or services online?

- Convenience
- Privacy
- Speed
- Price
- I don't buy goods and services online

18 - Do you know how to check if you are dealing with a secure site?

- Yes
- No

Usability and Security

19 - Have you ever abandoned an online operation due to the complexity of the authentication process?

- Yes
- No
- I don't remember

20 - If biometric readers replaced all your inputs in online shopping (clicking, credit card input, and email verification) would you be more likely to shop online?

- Yes
- No
- I don't know

21 - How accurate do you think the following biometric systems are? Please rank from 5 to 1, (5- being very secure and 1- insecure).

- Iris scanning
- Username and Password
- Fingerprint reading
- Voice recognition
- Secret codes (like those provided by banks).

22 - Would you be willing to share more of your personal data if that made online activity easier for you?

- Yes, but only if secured by public entities
- Yes
- No

23 - If you answered yes in Q22, please tick the information you would be willing to share.

- None

Name, Surname, address, phone number, email
ID number (Passport, National ID card)
Driving Licence
Credit/Debit card or other payment methods
Social Network profile information
Other

24 - On a scale of 1 to 5 (5 being completely and 1 being not at all) please rate how clearly service providers inform about:

The information collected from you
The use of the information collected
If they share the information with other providers
Your rights to the information (correct, delete your data etc.)
Compliance with the EU legislation

8.1 *Notes about the ARIES survey*

The Aries Survey was designed to ascertain citizens' expectations of the ARIES eID and inform the project about which issues needed to be addressed. We divided the questionnaire into four sections: "About you", where questions were asked about preferences and knowledge about online shopping; "Your View on Privacy" focused on personal privacy; "Online shopping/E-commerce" about concerns, confidence and safety of the e-commerce pages; "Usability and Security" about ease of use and views about biometrics as an enhancer of security against fraud. There were 222 respondents.

In general, people are confident internet users. Over 70% have one personal smart device they use to buy goods and services online, but the use of credit and debit cards (including in online transactions) is also very popular. Online banking and online shopping are avoided when using public Wi-Fi.

Respondents were concerned about their privacy in searching for and paying for goods and services online. There is greater confidence in sharing some personal data with banks and public authorities rather than private businesses. E-commerce sites and insurance companies had a medium level of trust (3 of 5 points).

Respondents were concerned about the security of making purchases over the internet, 75% of people knew how to check if the website is secure or not and 70% had never been victims of ID fraud. The location of the supplier influences the perception of the security of a potential transaction. Respondents saw the greatest advantages of buying goods/services online as convenience, speed and price. People are willing to share personal information on a website if they trust the web site to be secure.

Regarding Usability and Security, 60% abandoned an online operation due to the complexity of the authentication process, but some 50% would like to do more shopping online. Regarding biometrics, respondents consider iris scanning the most secure system but voice recognition and fingerprint reading are also seen as relatively acceptable and trustable security features. The easier a purchase is, the greater the likelihood that people are willing to give personal information. Name and ID number are the data that people most readily make available. Other conclusion of this topic is that the information provided by the service providers is ambiguous, especially in relation to the use of the information collected and if it is shared/ sold to with other providers.

From the answers, we conclude that ecommerce has great potential for growth, but many problems remain to be solved. Within the Aries project, we expect to address some of these problems, especially regarding enhancing security against ID fraud and usability issues.

Respondents were provided with information, as follows, on Aries and on how their responses would be handled.

reliAble euRopean Identity EcoSystem"

ARIES INFORMATION

-for participants in the FOCUS GROUP
-for respondents to the Aries Questionnaire online

ARIES is a research project supported by the EU's Horizon2020 research programme. The project will end in 2019. Aries aims to find a way to reduce identity fraud for the benefit of all citizens; and to find a means to make citizens' online transactions convenient, accessible, reliable, dependable and trustworthy.

Aries is a project that is designed to benefit society at large as citizens do more and more things online, and the European Digital Single Market becomes a reality.

As part of the project, ARIES seeks the views of citizens about an ARIES eidentity. The Aries eID is designed to maximize a citizen's privacy by disclosing the minimum of necessary information about him/her when s/he seeks to prove s/he is who s/he claims s/he is. For example, if you need to prove your age to buy alcohol, the information that is revealed about you, should only relate to you being above the minimum permissible age.

How easily and conveniently this eID can be used, will be tested by voluntary participants using a smart phone provided by the ARIES project.

Views on eID use will be collected via an online questionnaire accessible to citizens across the EU.

The research will be conducted with integrity and transparency. Participants will be asked to consent to participation. They will be informed and briefed about the project at the outset, and given the chance to ask questions. Lines of accountability in the project will be explained. Participants and respondents will be able to access a report online about the findings of the Focus Group and questionnaire at the end of the project.

The findings of the Focus Group and questionnaire will be shared securely within the Aries project to enable the research team to check that the Aries eID matches citizens' expectations and addresses effectively any concern that may be raised.

A participant or respondent is free to withdraw at any point. No data that identifies a person will be retained or shared for additional purposes.

All information sharing and handling within the Aries team complies with EU legislation. Anonymised results will be written up in a report which will be made available within the Aries team and to the EU research office.

Information will be used ethically. Confidentiality will be maintained and individual responses anonymized. Any information provided by a participant who withdraws from the Focus Group or part way through the questionnaire, will be discarded before the results from the Focus Group or questionnaires are analysed.

Contact for further information or in the event of complaint

"reliAble euRopean Identity EcoSystem"

CONSENT FORM

Title of project: ARIES

Name of Researcher:

Please initial and sign the form giving your consent to participating in the project.

1. I confirm I have read and understand the ARIES information sheet dated……..
   I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

2. I have been told what the purpose is of collecting and analysing information resulting from my participation, how information and data obtained will be used, processed, shared, and disposed of before taking part.

3. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason, without prejudice and without my legal rights being affected.

Signed:

Date:

9 APPENDIX 2: Relevant projects

There are many projects that have focused on realising e-IDs that can be used in different contexts to access services online using a single e-ID. Inter-operability has proven elusive. Typically barriers to the adoption of e-ID have included: incompatible legacy systems, citizen access to enrolment; non-transferability across private and public service applications, citizen scepticism as to the reliability, robustness, dependability and security.

Past projects

Past projects have focused on four main areas: security - borders and travel documents; ecommerce; ehealth and active ageing; and smart environments. Developments such as the Electronic Patient Files, the Quantified Self Movement and Big Data analytics raise ethical issues relevant to all.

Among early projects in 2002 was **eJustice**, designed to enable legal practitioners to exchange information online safe in the knowledge that they could depend on the authenticity of the e-credentials of their counterparts in other member states and jurisdictions, thereby removing the delays and complexities arising out of mutual recognition of standards, technical specifications and comparability of roles.

R4eGov succeeded this and attempted to expand this to borders (SIS II and VIS), international student mobility and international exchanges, e-procurement and cross-border public administration concerned with civil documents. It stressed the possibility of federated identity management for inter-operability.

The FIDO and eStork projects have led the development and roll-out of cross-border e-administration.

These projects feed into contemporary efforts to refine eID use in these settings, and also into the development of eID solutions to address core societal challenges such as ageing societies, eHealth, AI and M2M communication.

Fewer projects have focused on ethics in the digital world and how implicit ethical considerations inhibit citizen adoption of e-IDs. Those with work packages on security in practice (such as ELISE and Challenge dealing with the changing landscape of security and liberty) have attempted to address ethical and societal impact largely as a result of public policy practice changes involving the adoption of biometrics for public policy purposes – notably border control.

Others have examined ethical implications of robots, AI, ad-tracking and ehealth implants; and Konfido (H2020) addresses ehealth administrative related issues.

All are linked by implicit concerns with the societal and ethical impact of the adoption of new technologies and apps. However, there has been a tendency to conflate these with privacy and data protection. While the latter are important in terms of compliance with the law, they do not consciously necessarily sufficiently reflect the ethical and societal implications more broadly speaking. Projects focusing on cybersecurity, security and biometrics tend to view these issues through the PET, PIA and 'big brother' surveillance lens.

Nor do many reflect on how ethical and societal implications inhibit the adoption by citizens of eIDs or a single eID for multiple use in diverse settings in the digital market.

While there are numerous projects that have been undertaken or are underway in the private sector, these have been primarily noted as business attempts to sell a particular company's product. Therefore, we chose

to concentrate instead on projects with a more generic goal having the potential to generate interoperable solutions for the EU28.

The following projects, part-funded by the EU, are of special interest to ARIES.

ABC4TRUST – Attribute-based Credentials for Trust. The aim was to focus on privacy-ABCs to gain trust in the digital world. This project looked at the potential of anonymization to build users' trust in eIDs kept in their hands. It examined what essential elements the users chose to reveal about their e-identity for a particular transaction. Commercialization has been facilitated, inter alia, by Eurodocs AB (a user-friendly and secure service to protect the identity, anonymity and privacy of internet users) http://www.eurodocs.net. See too venturebeat.com

FIDES Federated Identity Management System built on STORK, FutureID, Kantara and SDIM, to define a technical blueprint for federated and interoperable identity management platforms, complying with current regulations such as eIDAS, privacy and data protection, and relevant national legislation in order to define guidelines for a privacy-preserving identity infrastructure service provider. (http://www.st.fbk.eu)

IN-PREP (an INtegrated next generation PREParedness programme for improving effective interorganizational response capacity in complex environments of disasters and causes of crises) Seeks to improve response to urgent natural a)nd manmade crises by sharing response planning across borders and agencies in real time, and improved coordination of critical and scarce resources (http://in-prep.eu)

RAMSES supporting law enforcement in the cyber world, an internet forensic platform for tracking the money-flow of financially-motivated malware (http://ramses2020.eu)

SATORI Improving Practical and helpful cooperation between data protection authorities (http://satoriproect.eu)

SEMIRAMIS – Secure management of Information across Multiple Stakeholders . Developed and deployed a flexible efficient solution for secure exchange of administrative documents and personal information between universities, telecommunication operators, soluton providers and public administrations. Project ran 2010-2012. Its results are available as open source under the GNU Lesser General Public Licence (LGPL). Its results were transferred to STORK 2.0

SIENNA – sets out grounds for ethical codes and recommendations to improve legal frameworks and ensure ethat future applications are designed in line with responsible safeguards. (http://trilateralresearch.co.uk)

SPacIOS testing the security of internet services

STORK 2.0 – builds on STORK - a pan-European eID authentication system (Secure Identity Across Borders Linked making access smarter.eu. This is designed to realise eGovernment saving, cut the costs of e-procurement and use cross-border digital services to realise the digital single market (DSM). A common eID management framework to allow citizens to take their eID anywhere in the EU aims to enable citizens to use their own national e-IDs to access public services online, whether using a smart card or a vtrual eID number, in other EU states that use eIDs. STORK 2.0 extends eID interoperability to electronic representation and mandates, with 57 partners from 19 EU and associated states. It pilots the updated eID interoperability platform in eBanking, ehealth, public services for business and eLearning, student mobility and academic qualifications.

TABULA RASA protecting biometric recognition systems against external security attacks

TREDISEC (Trust aware Reliable and Distributed Information security in the cloud) cloud-security and future of digital security and trust leveraging cryptographic protocols and system security mechanisms offering strong data confidentiality, integrity and availability guarantees while permitting efficient storage and data processing across multiple tenants

CACE Cyptography software development toolbox

PEPPOL -- Pan-European Public Procurement OnLine . The focus is digital public procurement across borders. This project focused on e-procurement and developed solutions for e-signatures, e-ordering, e-cataloguing and e-invoicing throughout the contract cycle. It has been updated and ePeppol is of interest to Aries.

IDAaaS Identity Assurance as a Service. The objective of the overall innovation project is to commercialize a trusted online service for identity assurance. This service will be implemented according to European standards for electronic identity, including eIDAS and STORK. The new service will be based on several years of development of secure electronic identity and digital signatures in the Nordic market. The expected outcome will be a simplified and cost effective online service for identity assurance that can be used in regulated industries such as banks and financial institutions (hereafter referred to as banks). The purpose of the service will be to assure that a user is who she claims to be when signing up to a new online service.

PROGRESS 'Promoting global responsible research and social and scientific innovation'. One goal is to promote social desirability by linking existing international networks of responsible research and innovation (RRI) with relevant social actors. progressproject.eu/

ReCred From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control. ReCRED's goal is to promote the user's personal mobile device to the role of a unified authentication and authorization proxy towards the digital world.

CREDENTIAL Secure Cloud Identity Wallet: The focus is on evaluating and applying novel crypto-approaches for IAMs but also on implementing them in an easy-to-use way to motivate secure handling of identity data. In order to also address security, privacy and trust issues related to the used cloud platforms and services the project will investigate assurance and resilience approaches for enhancing underlying cloud services, in eGovernment, eHealth and eBusiness. The goal of CREDENTIAL is to develop, test and showcase innovative cloud based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of strong hardware-based multi-factor authentication with end-to-end encryption representing a significant advantage over current password-based authentication schemes. The use of sophisticated proxy cryptography schemes will enable a secure and privacy preserving information sharing network for cloud-based identity information in which even the identity provider cannot access the data in plain-text and hence protect access to identity data.

PROTECT Pervasive and UseR Focused BiomeTrics BordEr ProjeCT The goal is an enhanced biometric-based person identification system that works robustly across a range of border crossing types and that has strong user-centric features. The system will be deployed in Automated Border Control (ABC) areas supporting border guards to facilitate smooth and non-intrusive rapid crossing by travellers based on deployment of the next generation of biometric identification detection methods.

MEDI@4SEC The emerging role of new social media in enhancing public security. This focuses on enhancing understanding of the opportunities, challenges and ethical consideration of social media use for public security. Making use of the possibilities that social media offer, including smart 'work-arounds' is key, while respecting privacy, legislation, and ethics.

ETICAS www.eu-forum.org/identity-management

EKSISTENZ (Harmonized framework allowing a sustainable and robust identity for European Citizens) Aims to deliver innovative and interoperable tools, procedures, methods and processes to tackle identity theft in the EU. Actions to assist citizens affected by ID theft and to facilitate ID recovery are planned, including the creation of guidelines, advice, assistance, and a thinktank with appropriate bodies like Europol and Interpol; and a European Observatory of Identity theft. www. eksistenz.eu. EKSISTENZ will not address identity management and identity in general, but will focus on identity theft.' Interoperability between the member states is to be piloted using STORK to enable bilateral recognition of primary identities among member states.

E-Forum is a not-for-profit association on eGovernment in Europe. It focuses on the future needs of smart governance and smart cities in Europe, and on *Identity Management and EU-China Smart City development.* E-Forum is currently engaged with. **EKSISTENZ** . E-Forum is now heading the dissemination of **EKSISTENZ.**

SMART CITIES and PORVOO: The Porvoo Group (established April 2002 during the international conference held in conjunction with Public Identity Project of the Smart Card Charter operating under the eEurope 2002 programme. It is an international network whose primary goal is to promote a trans-national, interoperable electronic identity based on PKI (Public Key Infrastructure) technology, smart cards and chip ID cards in order to help ensure secure public and private sector e-transactions in Europe. The group promotes the introduction of interoperable certificates and technical specifications, the mutual, cross-border acceptance of identification and authentication mechanisms, as well as cross-border, online access to administrative services.

PRIPARE Preparing Industry to Privacy -by-design by supporting its application in research part of eu-forum.org publishing privacy guidelines for smart cities and communities. PRIPARE publish privacy guidelines for smart cities and communities

European Observatory on Identity Theft and eCrime (EOITEC) on European identity protection initiatives. It will inform the citizen on methods, procedures and possibilities to recover his/her identity after theft, serve as a policy adviser to EU MSs and advance a common position on European identity protection. Repository of knowledge for EKSISTENZ and sister projects along with initiatives such as the Porvoo Group; Already, re-titling of the Observatory to EOITEC in order to cover eCrime.

EIP-SCC's Citizen-Centric Approach to Data (Privacy-by-Design) The EIP-SCC has launched a Citizen-Centric Approach to Data (Privacy-by-Design). It focuses on Privacy-by-design and default; Privacy settings ;Data protection impact assessments; And interaction with existing network and community.

EEMA The European association for eIdentity and Security http://www.eema.org is the Leading, Not For Profit, Independent European Think Tank networking on Identification, Authentication, Privacy, Risk Management, Cybersecurity, the Internet of Things, Artificial Intelligence and Mobile Applications.

The European Trust Foundation (ETF) is an independent body, created and coordinated by the EEMA, and aims to strengthen digital trust throughout Europe. It works across the public and private sectors within and outside the EU. 'http://Europeantrustassociation.eu/

Futurium project on digital futures 2050, hyperconnected humans, neuro morphic computing and cross border and cross sectoral collaboration

FutureID - Shaping the Future of Electronic Identity . www.futureid.eu This project identified technical and other barriers to eID adoption, focusing on federated identity management and eID authentication with PETs and PEDs.

SSEDIC - Scoping the Single European Digital Identity Community www.ssedic2020.eu

SSEDIC.2020 follows on from the EU funded thematic network SSEDIC "Scoping the Single European Digital Identity Community". From 2010 to 2013 SSEDIC conducted an intensive 3-year consultation together with over 200 European and international digital identity management experts and many stakeholder organizations. In 2013 SSEDIC identified four key areas central for the future development of digital identity (mobile identity, attribute usage, authentication, liability. SSEDIC.2020 is an active platform for all the stakeholders of digital identity to work together and collaborate towards creating a Single Digital Identity Community as a foundational infrastructure for trusted online services and a single digital market in Europe and beyond.

The Open Identity Exchange (2017) www.oixuk.org (a non-profit, technology agnostic, collaborative cross sector membership organization with the purpose of accelerating the adoption of digital identity services based on open standards).

Trust In Digital Life rustindigitallife.eu The Trust in Digital Life (TDL) community was formed by leading industry partners and knowledge institutes that hold trust and trustworthy services to be an essential ingredient of the digital economy. The TDL community is committed to enabling a trustworthy ecosystem that protects the rights of citizens while creating new business opportunities. TDL will form the bridge between citizens entitled to the best possible services and an industry that develops devise, applications and services that protect them from Internet threats and provides them at an affordable price.

di.me -- Integrated digital.me Userware

PETWeb II -- Privacy-respecting Identity Management for e-Norge

TDL -- Trust in Digital Life

A4Cloud -- Accountability for the Cloud [1] [2]

GINI-SA -- Global Identity Network of Individuals - Support Action

epSOS -- European Patients Smart Open Services

SEMIRAMIS --Secure Management of Information Across Multiple Stakeholders

TClouds -- Trustworthy Clouds. Privacy and Resilience for Internet-scale Critical Infrastructure

Vendorcom a multi stakeholder membership organization connecting parties in the European payments industry. Launched in 2003, it claims to be the most trusted, independent forum for suppliers and users. www.vendorcom.com

European Internet Service Providers (EuroISPA) www.euroispa.org (ISP assocs from member states); has MoUs with like-minded members' organisations across the world, including CAIP (Canadian Assoc of IP providers), IIA (Australian Internet Industry Assoc), INHOPE (Assoc of Internet Hotline providers in Europe, and US ISPA (US Internet Service Provider Assoc). It engages with the European Parliament on cybersecurity issues (like terrorism directive).European Telecommunications Network Operators Assoc (ETNO)

10 Bibliographical references

The bibliographical references are sub-divided thematically

10.1 *Background documents / Project knowledge repository*

Bates, M (2016) Kids and the Connected Home: Privacy in the age of connected dolls, talking dinosaurs, and battling robots, Future of Privacy Forum, 1 December 2016**.**

Bezes, C (2016) 'comparing online and in-store risks in multi-channel shopping', International Journal of Retail & Distribution Management (44:3) 284-300.Capurro, R & J.D.Holgate (2011) Messages and Messengers: Angeletics as an Approach to the Phenomenology of Communication, Fink

Capurro, R (2011) 'Never enter your real data', International Review of Information Ethics, 16 (12) 74-78.

Capurro, R (2017) Ethical Issues of Humanoid-Human Interaction, in G.Hermann and U.Leonards (eds).In P Vadakkepta and J-H Kim(eds), Handboook of Humanoids. New York, Spring,2017.

Capurro, R (2003) 'Angeletics: A message theory', in Ramsay.H.H & L.Ramsay (Eds)Hierarchies of Communication, Karlsruhe, Verlag ZKM, pp 58-71.

Capurro, R (1990). Towards an Information Ecology. In: I. Wormell, Ed.: Information and Quality, London: Taylor Graham 1990, pp. 122-139.

Capurro, R (2006). Towards an Ontological Foundation of Information Ethics. In: Ethics and Information Technology, Vol. 8, 4, pp.175-186.

Capurro, Rafael (2002). Perspectivas de una Cultura Digital en Latinoamérica. In: DataGramaZero (April 2002).

Capurro, Rafael (1999). Beiträge zu einer digitalen Ontologie.

Capurro, Rafael (1995). *Leben im Informationszeitalter.* Berlin: Akademie Verlag.

Grumbrecht, Hans-Ulrich, K. Ludwig Pfeiffer (eds.): Materialität der Kommunikation, Frankfurt 1988 with a contribution by Lyotard, 'Ob man ohne Körper denken kann'.

Haarkötter, H and Weil, F (Guest Editors): Ethics for the Internet of Things. In: International Review of Information Ethics (IRIE), Vol. 22, Feb. 2015. http://www.i-r-i-e.net/current_issue.htm

Hauge, M.V, D.K.Rossmo & S.C.le Comber,'Tagging Banksy:using geographic profiling to investigate a modern art mystery,' Journal of Spatial Science, access online 3 March 2016.

Krebs, S., (2006) ' On the Anticipation of Ethical Conflicts Between Humans and Robots in Japanese Mangas'. In: International Review of Information Ethics, Vol. 6, 2006, 63-68.

Lodge,J & D Nagel (2016) 'Magicians and Guerillas: transforming time and space' *in Information Cultures in the Digital Age: A Festschrift in Honor of Rafael Capurro*, (eds) M.Kelly and J Bielby, NY Springer (2016)

Olsen. S,(2015) Nearly Undetectable Tracking Device Raises Concern, CNET (02.01.2002) http://www.cnet.com/news/nearlu-undetectable-tracking-device-raises-concern; A.Turner How Ads follow

you from Phone to Desktop to Tablet, MIT.Tech.Rev 01.07.2015, http://www.technologyreview.com/news/538731/how-ads-follow-you-from-phone-to-desktop-to-tablet/.

Rizza,C & L.Draetta (2015) The 'silence of the chips' concept: towards an ethics (by design) for IoT, International review of Information Ethics, 22.

Roessler, B. (2005). The value of privacy. Cambridge: Polity Press.

Sabo, J (2016) This new privacy methodology makes data protection more science than art, Privacy Tech, IAPP, 9 December 2016.

Sax, M. (2016) Big data: Finders keepers, loser's weepers? Ethics and Information Technology, March 2016, Volume 18,1, pp 25–31.

Skeggs, B (2017) Wake up, algorithms are trawling your phone while you sleep… LSE Business review, 21/09/2017

van der Sloot, B. (2015). Privacy as personality right: Why the ECtHR's focus on ulterior interests might prove indispensable in the age of 'Big Data'. Utrecht Journal of International and European Law, 31, 25–50.

10.2 *Privacy, PbD, PETS*

Acces.Now Victory! EU court rules that indiscriminate data retention is not permissible, accessnow.org/victory-eu-court…not-permissible/ 21 Decmber 2016.

Australian Bureau of Statistics (2011) Australian Health Survey – Privacy Impact Assessment at http://oaic.gov.uk

Australian Attorney General's Department (2012) Privacy Impact Assessment – Extension of Document Verification Service to Private Sector Organisations available at http://oaic.gov.uk

Bock, K (2016) Data Protection Certification: Decorative or Effective Instrument? Audit and Seals as a Way to Enforce Privacy, Wright, D and P de Hert in *Enforcing Privacy, Regulatory, Legal and Technological Approaches*, New York:Springer,pp 335-56.

Cabinet Office (2008), Cross Government actions:Mandatory Minimum Measures, http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

Cavoukian, A., (2011) Commissioner for Privacy and Data Protection, http://www.privacybydesign.ca, Privacy by Design:the 7 Foundational Principles, Information and Privacy Commissioner, Ontario.

Chadwick, R., & Shickle, R. C. M. L. D. (Ed.) (2014). *The Right to Know and the Right not to Know: Genetic Privacy and Responsibility*. (2 ed.) (Bioethics and Law). Cambridge: CUP.

Chadwick, R. (2012). *Encyclopedia of Applied Ethics*. (2 ed.) Oxford: Elsevier.

Commission Nationale de l'Informatique et des Libertes (2016) CNIL publicly serves formal notice to Microsoft corporation to comply with the French Data Protection Act within three months, www.cnil.fr, 20 July.

Connolly, C and P.van Dijk (2016) Enforcement and Reform of the EU-US Safe Harbor Agreement, in Enforcement and Reform of the EU-US Safe Harbor Agreement in D Wright & P de Hert, *in Enforcing Privacy, Regulatory, Legal and Technological Approaches*, New York:Springer, 261-83

Daskal, J (2016) Law Enforcement access to data across borders: the Evolving Security and Human Rights Issues, Future of Privacy Forum Privacy Papers for Policymakers series.

Department of Homeland Security, Privacy Office (2010) privacy Impact Assessments – The Privacy Office Official Guidance available at http://oaic.gov.uk

Edelman B.G (2015) 'Does Google Leverage Market Power through Tying and Bundling?' *Journal of Digital Context.*

Englehardt, S (2016) Online tracking: A 1-million-site Measurement and Analysis, Future of Privacy Forum Privacy Papers for Policymakers series. Papers.ssrn.com

Etzioni, A. (1999). The limits of privacy. New York: Basic Books.European Court of Justice. (2015). Maximillian Schrems v data protection commissioner, joined party: Digital rights Ireland Ltd, In Case C-362/14.

European Data Protection Supervisor (2015) Opinion: Towards a new Digital Ethics and Big Data

European Data Protection Supervisor (2016) opinion 8/2016 : Coherent enforcement of Fundamental Rights in the age of Big Data, 23 September 2016, www.secure.edps.europa.eu

Eurobarometer Special, Number 431. Data Protection, June 2015.

Dordrecht: Springer, 2009. (www.springer.com)

Gutwirth, S., Y. Poullet, and P. De Hert, eds. Data Protection in a Profiled World. Dordrecht: Springer, 2010.

Gutwirth, S., Y. Poullet, P. De Hert and R. Leenes eds. Computers, Privacy and Data Protection: an Element of Choice. Dordrecht: Springer, 2011.

Gutwirth, S., R. Leenes, P. De Hert and Y. Poullet, European Data Protection: In Good Health? Dordrecht: Springer, 2012.

Gutwirth, S., R. Leenes, P. De Hert and Y. Poullet, European Data Protection:Coming of Age, Dordrecht: Springer, 2012.

Hall, K (2016) Shared services centres supposed to save £128m saved £0…and cost £4m, The Register 20 May 2016 http://www.theregister/2016/05/20/shared_services_centres_supposed_to_save_£128m_saved_£0/

Immigration New Zealand (2012) Privacy Impact Assessment: Collection and Handling of Biometrics at the Ministry of Business, Innovation and Employment.

Information Commissioner's Office (UK) Privacy by Design, www.ico.org.uk

Information Commissioner's Office (UK) (2009) PIA Handbook. www.ico.org.uk.

Internet Gesellschaft Co:llaboratory (2012) *Menschenrechte und Internet : Zugang, Freiheit und Kontrolle*, Berlin, Creative Commons BY 3.0 DE.

Kassner, M (2016) Privacy advocates rejoice: A new way to anonymise data might actually work, TechRepublic, 29 November 2016.

Kelly, M & J.Bielby (2016) (eds) Information Cultures in the Digital Age, Wiesbaden, Springer VS.

Krebs, S., (2006) On the Anticipation of Ethical Conflicts Between Humans and Robots in Japanese Mangas. In: International Review of Information Ethics, Vol. 6, 2006, 63-68.

Kroll, J.A, Huey, J, E.W.Felten, J.R. Reidenber, D.G.Robinson and H.Yu (2016), Accountable Algorithms, Future of Privacy Forum.

Martin, K & H. Nissenbaum (2016) Privacy of Public Data, Future of Privacy Forum.

Office of the Australian Information Commissioner (2014) Guide to Undertaking Privacy Impact Assessments, http://oaic.gov.au

Office of the Australian Information Commissioner (2017) Privacy Impact Assessment eLearning, http://oaic.gov.au

Office of the New Zealand Privacy Commissioner (2007) Privacy Impact Assessment Handbook available at oaic.gov.uk.

Prisco, G (2016) 'Department of Homeland Security awards Blockchain Technical Development Grants for Identity Management and Privacy Protection', Bitcoin Magazine, BTC Media, accessed 12.06.2016.

Roessler, B. (2005). The value of privacy. Cambridge: Polity Press.

Sabo, J (2016) This new privacy methodology makes data protection more science than art, Privacy Tech, IAPP, 9 December 2016.

Watson, H., R.l L. Finn and D. Barnard-Wills, 'A gap in the market: the conceptualization of surveillance, security, privacy and trust in public opinion surveys', *Surveillance and Society*, 15(2), 2017, pp. 269-285.

Wright, D & K.Wadhwa (2012) A step-by-Step Guide to Privacy Impact Assessment, PIAF, Poland available at http://oaic.gov.au

Wright, D & P.de Hert , Eds., (2012) Privacy Impact Assessment, Dordrecht:Springer.

10.3 *Airports and borders*

Brouwer, E. (2007). The use of biometrics in EU databases and identity documents. In J. Lodge, *Are you who you say you are? the EU and Biometric Borders* (pp. 1-151). The Netherlands: Wolf Legal Publishers (WLP).

Brunton, F., and H.Nissenbaum (2015) Obfuscation. A User's Guide for Privacy and Protest, The MIT Press.

Buchmann, J., (ed) (2012) Internet Privacy Eine multidisziplinäre Bestandsaufnahme/ A multidisciplinary analysis, Berlin, Acatech, September.

Center for Democracy and Technology, Note to the Federal Trade Commission Washington, on Cross-device tracking, Nov 2015. Cdt.org/files/2015/11/10.16.15-CDT-Cross-Device.

Civil Service World (2016) Planned watchdog merger to give public the chance to directly complain about departments, 6 December 2016 www.civilserviceworld.com.

Claburn, T (2016) Real Deal: Hackers steal steelmaker trade secrets, The Register, 8 December 2016 http://www.theregister.co.uk/2016/12/08/hackers_steal_steelmaker_secrets/

Cross, K (2016) This is the new reality for cyber security: Accept that hackers will get in, MarketWatch 10 December 2016. www.marketwatch.com accessed 11 December 2016.

Hern, A., (2014)'Hacker fakes German minister's fingerprints using photos of her hands', The Guardian, 30 December 2014.

Hoikkala, H and N.Magnusson (2016) Fingerprint Chief considers Acquisitions to Speed Expansion, Bloomberg, 15 September.

Home Office (2016), Decisions Taken : JHA (title V) opt-in and Schengen opt-out decisions, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/51525/2016-optin-webpage-update.pdf accessed 25/01/2017.

House of Lords (2016), European Union Committee, Brexit: future UK-EU security and police cooperation, 7th Report of Session 2016-17, HL Paper77, London.

Immigration New Zealand (2012) Privacy Impact Assessment: Collection and Handling of Biometrics at the Ministry of Business, Innovation and Employment.

Kassner, M (2016) Privacy advocates rejoice:A new way to anonymise data might actually work, TechRepublic, 29 November 2016.

Lampathaki, F et al (2013) National interoperability frameworkds : the Way forward in Information Resources Management Associations (eds) IT Policy and Ethics : Concept, Methodologies, Tools and Applications, IGI Global.

Lanzing, M. (2016) The transparent self, Ethics and Information Technology, March 2016, Volume 18, Issue 1, pp 9–16.

Lee, J (2015) Mcdonald's testing biometrics technology on POS system, www.biometricupdate.com 2 December.

Lee, J (2016) Documents reveal that cyberattack on biometric data could jeopardise security at Canadian borders, www.biometricupdate.com 15 September 2016.

Lee, J (2016a) Military biometrics market to grow more than 7% through 2020, www.biometricupdate.com 14 December.

Leenes R., Van Brakel, R., Gutwirth, S. and P. De Hert (2017)Computers, Privacy and Data Protection: Invisibilities & Infrastructures. Dordrecht: Springer.

Liberatore, A. (2007). Challenging Liberty, In J. Lodge, *Are you who you say you are? the EU and Biometric Borders* (pp. 1-151). The Netherlands: Wolf Legal Publishers (WLP).

Lodge, J., (2012b) 'Airports: A Mirror for Future biometrics?' Planet Biometrics. http://ww.planet-biometrics.com/creo_files/upload/article-files/airports_-_a mirror_for_future_biometrics.pdf.

Lodge., J (2013a) 'Who or What Is in Control of My Digital Identities and Can They Be Trusted?' EurActiv,6 December, available at: http://www.euractiv.com/infosociety/control-digital-identities-trust-analysis-532174.

Lodge. J., (2012a) 'Biometrics? Well-understood and a Panacea to Verifying and Authenticating Identity? Or Something That Is Vastly Overrated?' *Pentest* (October).

Lodge. J., (2013b) 'Nameless and Faceless: The Role of Biometrics in Realising Quantum (In)securityand (Un)accountability'. In: P. Campisi (ed.), *Security and Privacy in Biometrics*. New York, Springer, pp. 311–38.

Lodge, J. (2010), *Quantum Surveillance and 'Shared Secrets': A Biometric Step Too Far?* Brussels: CEPS, available at: http://aei.pitt.edu/15108/1/Lodge_on_Quantum_Surveillance_e-version12.pdf

Lodge, J. (2012c) 'The promise of ethical secrecy: can curiosity overcome automated group-think?' International Review of Information Ethics, 17(7),32-36.

Lodge,J.,(2007). A Challenge for Privacy or Public Policy – Certified Identity and Uncertainties. *Regio Minorities, Politics, Society English Edition*, pp. 193- 206.

Lodge, J., (2006) *Trends in Biometrics,* European Parliament, Policy Department Citizens' Rights and Constitutional Affairs. Brussels, September 2006.

Maguire, M. (2009, April). The birth of biometric security. *Anthropology Today*, pp. 9-14.

Mordini, E., & Petrini, C. (2007). Ethical and Social Implementations of Biometric identification technology. *Ann. Ist Super Sanita* , **43**:5-11

Mordini, E., & Massari S. (2008). Body, Biometrics and Identity. *Bioethics,* **22**(9): 488- 498.

Manning,J., ,J.C.Hulbert, J.Williams, L.Piloto, L.Sahatyan, K.A. Norman., 'A neural signature of contextually mediated intentional forgetting', Psychonomic Bulletin and Review, 5 May 2016, Open Access.

Maupin, J (2017) Blockchains and the G20: Building an Inclusive, Transparent and Accountable Digital Economy, CIGI Policy Brief No.101.

Mayhew (2016) Vision-Box introducing new biometric passenger platform at connect:ID, biometricupdate.com, 11.3.16

Nagenborg, M R.Capurro, J. Weber, C.Pingel (2008) Ethical Regulations on Robotics in Europe, AI & Society, 22:349-366.

Nakada, M., & R.Capurro (eds) (2013) 'An intercultural dialogue on roboethics'. In The Quest for Information ethics and roboethics in East and West (13-22) Research Report on trends in information ethics and roboethics in Japan and the West. http://www.capurro.de/intercultural-roboethics.html

Nissenbaum, N., (2010) Privacy in Context. Technology, Policy, and the Integrity of Social Life, Stanford: Stanford University Press.

Nlets, the international Justice and Public Safety Network (2011), Privacy Impact Assessment Report for the Utlisation of facial Recognition Technologies to Identify Subjects in the Field, http://oaic.gov.auOECD (2017) Trust and Public Policy. How Better Governance can help rebuild Public Trust. Paris.

Othman A and A. Ross (2014) Privacy of Facial Soft Biometrics: Suppressing Gender but Retaining Identity, Proceedings of the ECCV Workshop on Soft Biometrics, Zurich, September 2014. Cse.msu.edu/rossarun/pubs/OthmanRossGenderPRivacy_ECCVW2014.

Out-law.com (2017) First EU Privacy Shield annual review to take place in September, 04/04/2017.

Reichert, C (2017) Draft Identity Framework revealed, http://www.zdnet.com/article/government-reveals-draft-digital-identity-framework.

Richter,P & Kaminski A (2016) Before you even know…Big Data und die Erkennbarkeit des Selbsts, International review of Information Ethics, 24.

van der Sloot, B. (2015). Privacy as personality right: Why the ECtHR's focus on ulterior interests might prove indispensable in the age of 'Big Data'. Utrecht Journal of International and European Law, 31, 25–50.

Solove, D. (2013) Nothing to Hide: the false trade-off between privacy and security. New Haven, CT: Yale University Press.

Solove, D. J(2008). Understanding privacy. Cambridge: Harvard University Press.

Statewatch (2017) NOTE from: Hungarian delegation to: Working Party on Information Exchange and Data Protection (DAPIX): **Information Managment Strategy - Action 3 - Passenger Name Records Data Exchange Pilot (PNRDEP) - Final report** (10879/17, LIMITE, 28 September 2017, pdf): http://www.statewatch.org/news/2017/oct/pnr-pilot-project.htm.

Statewatch (2017) EU-wide biometric databases, 'soft targets', cybersecurity and data protection: Commission's fourth report on building the 'Security Union', Briefing by C. Jones, Feb. 2017.

Stokes, P. (2015) Deletion as second death: the moral status of digital remains,Ethics and Information Technology December 2015, Volume 17, Issue 4, pp 237–248

Terwangne, C de (2013) The Right to be Forgotten and the informational Autonomy in the Digital Environment, EU Joint Research Centre, Report EUR 26434 EN.

The Scottish Government (2013) Government and Young People (Scotland) Bill, Privacy Impact Assessment Report.

Thomson, J. J. (1975). The right to privacy. Philosophy & Public Affairs, 4(4), 295–314.

UK Border Agency, Report of a Privacy Impact Assessment conducted by the UK Border agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference (Australia, Canada, New Zealand and the USA) www.gov.uk accessed 3 November 2017.

Venkatesh, V and H.Bala (2008) Technology Acceptance model 3 and a research agenda on interventions, Decision Sciences, 39 (2).

Weimann, T., & D.Nagel (2011) IPv6 und Datenschutz – Personalisiertes Surfen mit Gefahren fur die Privatsphare. Legal Tribune Online. http://www.lto.de/recht/hintergruende/h/ipv6-und-datenschutz-personalisertes-surfen-mit gefahren-fuer-die-privatsphere/

Your Europe (16 Aug 2016), Travel Documents for EU nationals http://europa.eu/youreurope/citizens/travel/entry-exit/eu-citizen/index_en.htm

10.4 *eCommerce*

ALDE Mareitje Schaake, Algorithmic Accountability and transparency in the digital economy 7/11/2016, mareitjeschaake.eu (roundtable with Microsoft, Cantab, French digital council, NYU, EUCommission, Data and Security)

Barlow, John Perry (1996). HYPERLINK "http://homes.eff.org/~barlow/Declaration-Final.html"A Declaration of the Independence of Cyberspace.

Business Insider (2016) The Mobile Payments Report, http://www.businessinsider.com/the-mobile-payments-report-market-forecasts-consumer-trends-and-the-barriers-and-benefits-that-will-influence-adoption-2016-5

Bonham, G., Seifert, J. and Thorson, S. (2001), "The transformational potential of e-government: the role of political leadership", paper presented at 4th Pan European International Relations Conference, University of Kent.

Burn, J. and Robins, G. (2003), "Moving towards e-government: a case study of organisational change processes", Logistics Information Management, Vol. 16 No. 1, pp. 25-35.

Canadian Commissioner for Privacy and Data Protection www.cpdp.vic.gov.au

CPC(2014) NetworkSWEEPomwww.ec.europa.eu/consumers/strategy../policy/consumer_policy_report2014_en.pdf.

Deli-Gray, Z, M-P. Pinto., C.McLaughlin & R. Szilas (2016) Perception of young children of the ideal shopping experience, International Journal of Retail & Distribution (2016) (44) 996-1012.

Digital Evidence and Electronic Signature Law Review http://journals.sas.ac.uk/deeslr/ (also available in the LexisNexis and HeinOnline electronic databases).

Dillon, J. and Pelgrin, W. (2002), E-Government/Commerce in New York State, Office of Technology, New York, NY.

eCommerce Europe (2015), Ecommerce Europe Priority Paper: Policy and market solutions to stimulate cross border e-commerce in Europe.(www.ecommerce-europe.eu) (Futurium).

Electronic Signatures in Law (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, university of London, 2016) http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

Euractiv.com Two Thirds of Europeans are digitally illiterate, 10 June 2016.

EurActiv.com Europe's Tech Industry could get a boost from visa overhaul, 8 June 2016.

EurActiv.com EU eSkills campaigns reduce gap in the labour market, 18 October 2016.

European Commission (2015) Consumer attitudes towards cross-border trade and consumer protection (Sept)

http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2031

European Commission (2016) How Digital is Your Country?New Figures show action needed to unlock Europe's potential. Press release. Europa.eu/rapid/press-release/IP-16-384_en.htm.

European Commission, Joint Research Centre (2007) Overcoming Barriers in the EU Digital Identity Sector, Institute for Prospective Technological Studies, Seville.

European Commission (2016) Employment, Social Affairs & Inclusion, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A New Skills Agenda for Europe : Working Together to strengthen human capital, employability and competitiveness,* COM (2016) 381 final. Brussels, 10.6.2016 .

European Commission (2015) Retailers' attitudes towards cross-border trade and consumer protection, Brussels.

European Commission (2015) Consumer Conditions Scoreboard :Consumers at home in the Single Market. http://ec.europa.eu/consumers/consumer_evidence/consumer_scoreboards/11_edition/docs/ccs2015scoreboard_en.pdf

The European Policy Centre (EPC) The Economic Impact of a European Digital Single Market www.epc.eu/dsm/2/study_by_copenhagen.pdf

Fletcher, K. and Wright, G. (1995), "Organisational, strategic and technical barriers to successful implementation of database marketing", International Journal of Information Management, Vol. 15 No. 2, pp. 115-26.

Forbes (2016) 'Ecommerce 2020: Sites, Consumer Expectations Evolving Fast,' Oracle Voice, 14 July. www.forbes.com

Gefen, D. and Pavlou, P. et al. (2002), "Egovernment adoption", paper presented at Americas Conference on Information Systems, Tampa, FL.

Goles, T., Lee, S.J., Rao, S.V. and Warren, J. (2009), "Trust violations in electronic commerce: customer concerns and reactions", Journal of Computer Information Systems, Vol. 49 No. 1, pp. 1-9.

Golla., A (2016) 'Germany criminalises trading "stolen" data via the Internet, Privacy Laws and Business International Report, April 2016:16-17.

Hall, K (2016) UK.gov oughta get its data-sharing house in order before Digital Economy Plans, The Register, 19 September 2016 http://www.theregister.co.uk/2016/09/19/ukgov_digital_economy_shambles/

Hall, K (2016) Shared Services centres flop: Only one UK.gov department uses them, The Register 8 December 2016

http://www.theregister/2016/12/08/shared_servcies_centres_a_flop_only_one_department_is_using_one/

Hern, A (2016) 'Airline passenger details easy prey for hackers, say researchers,' The Guardian 28 December. (https://www.theguardian.com/technology/2016/dec/28/airline-passenger-details-online-bookings-easy-prey-hackers-say-researchers?utm_source=esp&utm_medium=Email&utm_campaign=GU+Today+main+NEW+H+categories&utm_term=206159&subid=10924169&CMP=EMCNEWEML6619I2)

Heeks, R. (Ed.) (1999), Reinventing Government in the Information Age: International Practice in IT-Enabled Public Sector Reform, Routledge, London

Heeks, R. (2001), Understanding E-Governance for Development, Institute for Development Policy and Management, Manchester.

Ho, A.T-K. (2002), "Reinventing local governments and the e-government initiative", Public Administration Review, Vol. 62 No. 4, pp. 434-44.

Holsapple, C.W. and Sena, M.P. (2005) 'ERP plans and decision-support benefits', Decision Support Systems, Vol. 38, No. 4, pp.575–590.

Hota, M., M.Derbais (2016) A real child in a virtual world ; exploring whether children's participation in MMORPGs transforms them into virtual retail shoppers, International Journal of Retail & Distribution (2016) (44) special issue 11 on *Kids and Retailing :Future Trends.*

Ipsos MORI (2017) 60years of 'Europe' – a success story? Accessed via linkis.com 27/02/2017.

Ipsos MORI (2016) Tech Tracker Quarterly Release Q4 2016: trends in Internet Usage, tech Ownership and the Connected Home, Ipsos Connect, November.

Joshi, J. and Ghafoor, A. et al. (2001), "Digital government security infrastructure design challenges", IEEE Computer, Vol. 34 No. 1, pp. 66-72.

Kaapu, T., &. T. Tiainen (2009) Consumers' Views on Privacy in e-Commerce, Scandinavian Journal of Information Systems, 21(1), 3-22. At www.iris.cs.aau.dk.

Lambrinoudakis, C. and Gritzalis, S. et al. (2003), "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy", Computer Communications, Vol. 26 No. 16, pp. 1873-83.

Layne, K. and Lee, J. (2001), "Developing fully functional e-government: a four stage model", Government Information Quarterly, Vol. 18 No. 2, pp. 122-36.

Lee, Y.J., A.J.Dubinsky (2017) 'Consumers' desire to interact with a salesperson during e-shopping: development of a scale,' International Journal of Retail and Distribution (45:1)20-39.

Lenk, K. and Traunmuller, R. (2000), "A framework for electronic government", paper presented at 11th International Workshop on Database and Expert Systems Applications, IEEE Computer Society, London.

Leonard, Lori N. K. and Jones, Kiku (2014) "Consumer-to-Consumer Ecommerce: Acceptance and Intended Behavior," Communications of the IIMA: Vol. 14 Iss. 1, Article 1.

Li, F. and Steveson, R. (2002), "Implementing e-government strategy in Scotland: current situation and emerging issues", paper presented at 2nd European Conference on E-Government, St Catherine's College, Oxford.

McClure, D. (2000), "Electronic government: federal initiatives are evolving rapidly but they face significant challenges", Accounting and Information Management Division, available at: www.gao.gov/new.items/a200179t.pdf

McKnight, D., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. Information Systems Research, 13(3), 334-359.

Moon, M.J. (2002), "The evolution of e-government among municipalities: rhetoric or reality", Public Administration Review, Vol. 62 No. 4, pp. 424-33.

NECCC (2000), E-Government Strategic Planning, National Electronic Commerce Coordinating Council, Las Vegas, NV.

NG eCommerce,Meeting Millennial Demand: eCommerce Innovation in 2016 (www.Gdsummits.com) St Andrews, Scotland 7-9 November 2016.

Official Journal of the European Union (2014) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC , L257/73, Brussels, 28.8.2014.

Opinium (2016) Research of 7000 European and Middle Eastern individuals. https://f5.com/about_us/news/press-releases/european-and-middle-eastern-consumers-deeply-conflicted-over-privacy-and-security-priorities-19968 (accessed 24.10.16)

Palvia, P., Means, D.B. and Jackson, W.M. (1994), "Determinants of computing in very small businesses", Information & Management, Vol. 27 No. 3, pp. 161-74.

Pan, Y & G. Zinkhan (2006) 'Exploring the Impact of online privacy disclosures on consumer trust.' Journal of Retailing (82:4) 331-338.

Pavlou, Paul A., Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model (2003). International Journal of Electronic Commerce (2003), 59, (4), 69-103.. Available at SSRN: https://ssrn.com/abstract=2742286

Reidenberg, J & T. Breaux (2016) Ambiguity in Privacy Policies and the Impact of regulation, Future of Privacy Forum Privacy Paper for Policymakers series.

Robins, G. (2001), "E-government, information warfare and risk management: an Australian case study", paper presented at 2nd Australian Information Warfare Security Conference, Perth.

Secureauth (2016) Get the User Convenient Authentication RSA Can't Deliver, www.secureauth.com/sites/default/files/sa_solutionbrief_rsa.pdf

Solove, D & D, Citron (2016) Risk and Anxiety: A theory of Data Breach Harms, Future of Privacy Forum. (14 December 2016) available at SSRN: https://ssrn.com/abstract=2885638.

Strunsky, S (2017) After Equifax Menendez bill would guard against hacks, njadvancemedia.com accessed 20/09/2017.
www.njcom/hudson/index.ssf/2017/09/after_equifax_menendez_bill_would_guard_against_ha.htm

Tasheva, I (2017) European Cybersecurity Policy: Trends and Prospects, European Policy Centre, 8 June 2017.

Taylor, E. (2016) 'Mobile payment technologies in retail: a review of potential benefits and risks', International Journal of Retail & Distribution Management (44:2) 159-177.

Themistocleous, M. and Irani, Z. (2002), "Novel taxonomy for application integration", Benchmarking: An International Journal, Vol. 9 No. 2, pp. 154-65.

Udo., G.J. (2001) 'Privacy and security concerns as major barriers for e-commerce: a survey study,' Information Management & computer Security (9:4)165-174.

Unesco (2016) Human Right and encryption, ed. Schulz.W & J van Hoboken.

Urueña López, Alberto & Pascual-Miguel, Félix & Iglesias-Pradas, Santiago. (2012). Value, quality, purchasing habits and repurchase intention in B2C: Differences between frequent and occasional purchaser. Direccion y Organizacion. 47. 70-80.

Van der Sloot, B. (2015). Privacy as personality right: Why the ECtHR's focus on ulterior interests might prove indispensable in the age of 'Big Data'. Utrecht Journal of International and European Law, 31, 25–50.

Verhagen,T., Meents, S & Y-H., Tan (2006) 'Perceived risk and trust associated with purchasing at electronic marketplaces', European Journal of Information Systems (15) 542-555.

Wallner, S (2017) 'Datarino: 'to make sure data is valuable, collect everything', www.magazine.startus.cc (4/7/2017)

Wessels, B, R. Finn, K. Wadhwa and T. Sveinsdottir (2017), *Mobilising Data in a Knowledge Society*, Amsterdam University Press, Amsterdam.

Yrcan, B (2016) 'How Blockchain fits into the future of Digitial Identity', Americanbanker.com 18/08/2016

Electronic Signatures in Law (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, university of London, 2016) http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures

Zakareya Ebrahim, Zahir Irani, (2005) "E-government adoption: architecture and barriers", Business Process Management Journal, Vol. 11 Issue: 5, pp.589-611.

Zeichner, L.M. (2001), "Developing an overarching legal framework for critical service delivery in America's cities: three recommendations for enhancing security and reliability", Government Information Quarterly, Vol. 18 No. 4, pp. 279-91.

10.5 *Relevant EU legislation and guidance*

Article 29 Working Party (2016), Working Document 01/2016 on the justification of interfaces with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), adopted 13 April 2016.

Buchmann. J (ed) (2012) Internet Privacy: Eine multidisciplinaere Bestandaufnahme, Acatech Studie, Berlin, Springer

Bundesministerium fuer VErkehr und digitale Infrastruktur (2017) Ethik-Kommission, Automatisiertes und Vernetztes Fahren, Bericht Juni 2017, accessed www.bmvi.de/SharedDocs/DE/Publikationen/G/ and available at www.bmvi.de/bericht-ethikkommission

Council of Europe (2017) Convention on Human Rights and Biomedicine, Oviedo Convention (http://coe.int)

European Commission (2017) Principles and Guidance on eID interoperability for online platforms-finalisation and way ahead (November) https:// digital-single-market/en/news/principles-and-guidance-eid-interopability-online-platforms-finalisation-and-way-ahead)

DIRECTIVE (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ

L194/1 of 9 July 2016. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Commission (2015) Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market Text with EEA relevance, OJ L53 of 25 February 2015.

European Commission (2015) Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 235, 9 September 2015.

European Commission (2015) Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic market, OJ L 235, 9 September 2015.

European Commission (2015) Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L 289, 5 November 2015.

European Commission (2017) Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council framework Decision 2001/413/JHA, COM (2017)489.

European Commission (2016) Security Union: Commission Presents Action Plan to strengthen the European response to tackle travel document fraud, Press Release, Brussels, 8 December 2016.

European Commission (2016) Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System, Brussels, 6 April 2016.

European Commission (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM (2015) 185 final, Strasbourg, 28.4.2015

European Commission (2016) State pf the Union 2016: Commission Targets Stronger external Borders, Press Release, Strasbourg 14 September.

European Commission (2016) Communication: eGovernment Action Plan 2016-2020. Accelerating the Digital Transformation of Government, COM (2016)179 final. 19 April.

European Commission (2016) DG Connect Public Consultation on the eprivacy Directive Review.

European Commission (2016) Communication from the Commission to the European Parliament and the Council, Stronger and Smarter Information Systems for Borders and Security, COM (2016) 205 final, Brussels, 6.4.2016.

European Commission (2017) EU Citizenship Report 2017, Strengthening Citizens' Rights in a Union of Democratic Change. Brussels, January 2017.

European Commission, Communication from the Commission to the European Parliament and the Council, Action plan to strengthen the European response to travel document fraud. COM (2016) 790 final, Brussels, 8.12.2016.

European Commission (2017) Schengen Borders Code: Systematic Checks of EU Citizens crossing external Schengen borders mandatory as of today, 07/04/2017 Press release.

European Commission (2016) Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal L 119, 54 May 2016, pp1-88.

European Council (2017) Implementing the Bratislava Roadmap, October www.consilium.europa.eu/nedia/2159/bratislava-implementing-the-bratislava-roadmap

European Council (2017) PRADO Public Register of Authentic Travel and Identity Documents Online, http://www.consilium.europa.eu/prado/en/prado-start-page.html

European Council (2017) E-signature ceremony: first EU legislation signed electronically, http://www.consilium.europa.eu/en/policies/digital-single-market/

EDPS Opinion on the processing of health data at the European Securities and Markets Authority (ESMA) (case 2013-0927) https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/ReferenceLibrary/16-11-16_Health_data_workplace_EN.pdf

European Data Protection Supervisor (2017) Statement on the concept of interoperability in the field of Migration, Asylum and Security; at edps.europa.eu/sites/publication/17-05-08_statement_on_interoperability_ed.pdf.

European Data Protection Supervisor (2017a) A New Chapter for EU data protection: managing accountability and compliance in the Reform Era. Speech to the European Parliament's Data Protection Day, 28 June 2017.

European Data Protection Supervisor (2017b) DPOs preparing for implementation of accountability in daily work of EU institutions and bodies (edps.europa.eu)

European Data Protection Supervisor (2017c) The State of the Data Protection Union (edps.europa.eu)

European Parliament (2017) e-Privacy: MEPS look at new rules to safeguard your personal details online (18.04.2017) Press release. Video of hearing (11 April 2017) http://www.europarl.europa.eu/news/en/news-room/2017045IPR70233

European Parliament, European Parliamentary Research Services, (2016) Golden Eye: Who Rules tomorrow's Europe? The European Youth Event. www.europarl.europa.eu/RegData/etudes/ATAG/

PE581.976/2016/581976/EPRS_ATA (2016) 581976_EN.pdf

European Parliament (2017) Committee on Civil Liberties, Justice and Home Affairs, Draft Report – Conditions of entry and residence of third-country nationals for the purposes of highly skilled employment – PE 595.499v02-00.

European Parliament (2017) Committee on Civil Liberties, Justice and Home Affairs, Draft Report on Establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013, for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) –PE597.620v01-00.

European Parliament (2017) LIBE Report, Committee on Civil Liberties, Justice and Home Affairs, Draft report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)) 09.06. 2017. Amended as doc. A-0324/2017 20.10.2017

Article 29 Working Party on the protection of personal data ec.europa.eu/justice/data-protection/article-29/index_en.htm

Privacy Commission (Belgium) on Article 29 Working Party https://www.privacycommission.be/en/art-29-wp

Charter of fundamental rights of the European Union (2000/C364/01). http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

European Commission (2016) Commission Implementing Decision of XXX pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf, accessed 16.03.13

European Community (1995) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

European Commission (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM92015) 185 final, Strasbourg, 28.4.2015 http://www.eur-lex.europa.eu

European Commission Communication from the Commission to the European Parliament, the European Council and the Council, Second Progress report towards an effective and genuine Security Union, COM (732) 16.11.16

European Commission, Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final, Brussels 29.2.16.

European Commission (2014) Digital Agenda for Europe – Trust Services and eID.

European Commission (2007), Report on Identity theft/fraud – Fraud Prevention Expert Group.

European Court of Justice, Case C-362/13, Maximillian Schrems v Data Protection Commissioners ('Schrems') EU:C:2015.

http://www.theregister.co.uk/2016/03/01/safe_harbour_20_oks_six_bulk_collection_excuses/

European Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C (2000)2441) (Text with EEA relevance.) Official Journal L 215, P. 0007–0047 25/08/2000

European Commission Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM (2016) 883 final, 2016/0409 (COD), Brussels 21.12.2016.

European Commission (2013) proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union COM/2013/095 final -2013/0057 (COD).

European Data Protection Supervisor, Ethics Advisory Group (2016) report of the first Workshop with experts from the data protection community, Brussels, 31 May.

European Data Protection Supervisor (2015) Towards a new digital ethics: Data, Dignity and Technology, Opinion of 11 September 2015.

European Data Protection Supervisor (2015a) Strategy 2015-2019: Leading by Example, Brussels.

European Group on Ethics in Science and New Technologies (EGE) (2012) Ethics of Information and communication technologies, Opinion No 26 – 22 February, available at http://ec.europa.eu/ege/index.cfm

European Parliament (2015) Committee on Civil Liberties, Justice and Home Affairs, Working Document on the Entry/Exit system (EES) to register entry and exit data of third country nationals crossing the EU Member States' external borders, PE544.477v01-00, Jan 2015.

European Parliament (2017) Smart Borders: Entry- Exit system, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/586614/EPRS_BRI(2016)586614_EN.pdf

European Parliament (2016) DG for Internal Policies, Citizens' Rights and Constitutional Affairs, The Legal and Political Context for Setting up a European Identity Document, Study for the AFCO Committee.

European Parliament (2016) Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters. Procedure file 2016/0409 (COD).

European Parliament Research Service, the cost of Non-Schengen: Civil Liberties, Justice and Home Affairs, (W.van Ballegooij for the European Parliament think tank) (2016)

Holgate, J (2016) Rafael's School of Athens from the Perspective of Angeletics, 223-246

IDABC, (2005) Towards Interoperable eIDs for European Citizens.

IDABC (2005) The Porvoo Group: promoting eID interoperability

Kelly, M & J.Bielby (eds) (2016) Information Cultures in the Digital Age: A Festshrift in Honor of Rafael Capurro, Wiesbaden, Springer

Lodge,J & D.Nagel (2016) Magicians and Guerillas : Transforming Time and Space 359-372

Lodge, J (2016) 'Fortress Europe': Borders and the power of information in the European Union, in J.M.Magone(ed) Routledge Handbook of European Politics, London,132-152

Regulation (EU) No 254/2014 of the European Parliament and of the Council of 14 March 2014 on a multiannual consumer programme for the years 2014-20 and repealing Decision No 1926/2006/EC, OJ L 84/42 28.2.2014. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0254&from=EN

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May JHA, on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA, 2009/968/JHA, OJ L 135/53, 24.5.2016

Rossnagel, A (2011) Das Gebot der Datenvermeidung und sparsamkeit as Alsatz wirksamen tecknikbasierten Persoenlichkeitsschutzes? In M. ifert & W. Hoffmann-Riem (eds) Innovation, Recht und oeffentliche Kommunikationen (Sonderdruck) Innovation und Recht IV, Berlin

Office of the Information Commissioner (2016) General Data Protection Regulation https://ico.org.uk/for-organisations/**data-protection**-reform/...25/10/2016 · This overview highlights the key themes of the **General Data Protection Regulation** (GDPR) to help organisations understand the new legal framework in the EU

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA , OJ L 119/91 4/05/2016accessible at http://data.europa.eu/eli/dir/2016/680/oj

European Parliament, DG for Internal Policies, (2016) potential and Challenges of eParticipation in the European Union, Study for the AFCO Committee, Brussels.

European Parliament(2012) Digital Single Market REPORT on completing the Digital Single Market - A7-2012-0341 …www.europarl.**europa.eu**/sides/getDoc.do?type=REPORT&reference=A7... (2012/2030(INI)) The **European** Parliament, having regard to the Commission communication of 3 October 2012 to the **European** Digital single market for Europe - Consilium www.consilium.europa.eu/en/policies/digital-single-market-strategy

European Commission (2016) Communication eGovernment Action Plan 2016-2020, Accelerating the Digital Transformation of Government, COM (2016) 179 final., 19/04/2016.

European Commission (2016) Digital Futures. Final Report. A journey into 2050 Visions and Policy Challenges report, 2015.

http://ec.europa.eu/achives/futurium/digital-agenda/sites/futurium/files/DF_final_report.pdf

European Commission (2015) Communication from the Commission to the European Parliament, Council, European Economic and Social Committee and Committee of the Regions, *A Digital Single Market Strategy for Europe*, COM (2015) 192 final.

European Commission (2016) Proposal for a Regulation of the European Parliament and of the Council on cooperation between national authorities responsible for the enforcement of consumer protection laws COM(2016) 283 final,2016/0148(COD) 25 May 2016.

European Commission Report to the European Parliament and the Council on the application of Regulation (EC) 2006/2004, COM(2009) 336 final, 7 July 2009.

http://ec.europa.eu/consumers/enforcement/docs/Commission_report_en.pdf.

European Parliament (2017) Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on International trade, Towards a digital trade strategy (2017/2065(INI)) Rapporteur: AngelikaMlinar,01-09-2017.

http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-609.526&format=PDF&language=EN&secondRef=01

European Parliament (2017) Report on the proposal for a regulation of the European Parliament and of the Council amending regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities (COM (2016/0589 -C*-0378/2016-2016/0287(COD), A8-0181/2017 and debated OJ 12/09/2017-44.

European Data Protection Supervisor Opinion 7/2015 Meeting the Challenge of Big Data.

European Parliament Think Tank (2017) WIFI4EU Promotion of Internet Connectivity in local communities, 05/09/2017.

European Commission Representation in the United Kingdom (2017) Better privacy on Facebook, fewer nuisance calls and less barriers to cross-border services, Press Release, London, 10/01/2017.

IDABC (2005) Towards Interoperable eIDs for European Citizens.

European Parliament, Legal Affairs Committee (2016) Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))31 May 2016. (PR\1095387EN.doc 15/22 PE582.443v01-00 EN)

European Parliament (2014) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS regulation), http//eid.as

European Commission (2017) Summary report on the public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA) (23.06.2017) https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-european-union-agency-network-and *Special issue of Competition Law and Economics*, vol 11/2, June.

10.6 *eCrime*

Commission of the European Communities (2004) Proposal for a Council Regulation on standards for security features and biometrics in EU citizens' passports. COM (2004) 116 final. Brussels,18February 2004.

Commission of the European Communities (2005) Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, COM (2005) 600 final, Brussels 24.11.2005.

Council of the EU **Proposal for a Regulation on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 - Revised draft** (LIMITE doc no: 11884-17, pdf): 140 Footnotes with Member State positions.

Council of the EU **Proposal for a Regulation on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 - Revised draft** (LIMITE doc no: 11884-17, pdf.

Council Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) **Regulation... to supplement and support the European criminal records information system (ECRIS-TCN system) and amending Regulation (EU) No. 1077/2011 - Questions on prior convictions and on access by certain agencies** (LIMITE doc no: 12033-27, pdf): available via www.statewatch.org

ENISA (2017) Cyber Security resilience of Smart Cars: Good practices and recommendations, Brussels, https://www.enisa.europa.eu/media/news-items/news-wires/RSS

European Commission, DG for Migration and Home Affairs (2017) High Level Expert Group on Information Systems and Interoperability, Final Report (2017) Ares(2017)2412067 - 11/05/2017

http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1

European Parliament (2017) Draft Report of the Committee on civil Liberties, Justice and Home Affairs, LIBE, Proposal for a Council implementing Decision on the launch of automated data exchange with regard to vehicle registration data in Denmark, PE 597.478v01-00, 3 February.

European Parliament (2017) Draft Report of the Committee on civil Liberties, Justice and Home Affairs, LIBE, Establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation(EU)No 604/2013, for identifying an illegally staying third country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) PE 597.62002-00, 3 February.

European Parliament (2017) Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices Report for the LIBE Committee 06-04-2017, http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2017)583137

European Parliament (2017) LIBE Committee on Civil Liberties, Justice and Home Affairs, **Progress towards the interoperability of EU information systems: extracts from the exchange of views with Dimitris AVRAMOPOULOS, Member of the EC in charge of Migration, Home Affairs and Citizenship and Krum GARKOV, Director of eu-LISA, accessed 21/09/2017 http://audiovisual.europarl.europa.eu/Assetdetail.aspx?id=06d1448c-d843-47c1-a2a9-a7e4010a8029.**

European Parliament and the Council (2008) Regulation (EC) No 767/2008 of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short – stay visas (VIS Regulation), Official Journal of the European Union, L218, Brussels, 13.8.2008.

Official Journal of the European Union (2009) Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, L 142, Brussels, 6.6.2009.

Article 29 Working Party, Statement on the Consequences of the Schrems Judgment of 3 February 2016, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

Article 29 Working Party, Working Document 01/2016 on the justification of interfaces with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), adopted 13 April 2016.

Australian Privacy Foundation (2016) http://www.innovationaus.com/2016/09/Privacy-lobby-digs-trenches-sets-guns

Office for National Statistics (2017) Crime in England and Wales : year ending Sept 2016, London.

US VISIT Smart Border Alliance RFID Feasibility Study Final Report, http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf

National Office for Statistics (2014) Monitoring e-commerce 2014.nao.org.uk.

National Audit Office (2016) Protecting Information Across Government, London, 2016 accessed 12 Dec 2016 http://www.nao.gsi.gov.uk

National Audit Office (2015) e-borders and successor programmes, London 2016 accessed 4 Dec 2016

National Audit Office (2014) Identity Assurance Programme, Briefing Paper, London 2014 accessed 11 Dec 2016 http://www.nao.gsi

Official Journal of the European Union (2014) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC , L257/73, Brussels, 28.8.2014.

Statewatch.org (2017) Newsletter/

Sussex and Surrey Police Drone PIA (UK) Privacy Impact assessmenthttps://wwww.sussex.police.uk/media/5583/drones-privacy-impact… guide.

10.7 *Industry statements*

ETNO (2016) joint Industry Statement: Empowering trust and Innovation by repealing the e-Privacy Directive (5 July 2016) https://www.etno.eu/news/etno/2016/878

eCommerce Europe (2015), Ecommerce Europe Priority Paper: Policy and market solutions to stimulate cross border e-commerce in Europe. (www.ecommerce-europe.eu) (Futurium)

European Parliament (2013) All-Party Group for European Reform, Inquiry into the EU Single Market in services (www. Archive.openeurope.org.uk).

FIDO Alliance (2015) Response to NIST RFI on the framework for Improving Critical Infrastructure Cybersecurity, February 2015 www.csrc.nist.gov accessed 11 December 2016.

GSMA (2016) The Mobile Economy: Europe 2015. http://gsma.com/mobileeconomy/europe.

Hewlett Packard Enterprise (2017) Keep key identification documents always close at hand**:** Slovakia prototypes mobile electronic identification (MeID) solution. White Paper.http://www.securitydocumentworld.com/creo_files/upload/article-files/4AAX-XXXXENW-Mobile-Identity-Documents.pdf

HID (2015) Protecting Against Criminal Use of Stolen Biometric Data. https://www.hidglobal.com/sites/default/files/resource_files/hid-biometrics-stolen-biometric-data-wp-en.pdf

Magazine.startus.cc (2017) Disrupting the Retail Industry :A Breakdown on startup driven innovation (accessed 5/7/2017).

Mercator Advisory Group (2017) Biometrics: A Market forecast for Consumer Adoption.

Security Document World (2017) http://www.securitydocumentworld.com/article-details/i/13222/

ANNEX 1: The European agenda on security COM(2015) 185

Excerpt from:
European Commission (2015) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28.4.2015 pp6-7.

Legal implementation of EU instruments at national level is not enough. The tools of the EU security framework will only take full effect when national law enforcement agencies feel confident in existing instruments and share information readily. The proposal for a new legal basis for **Europol**, (note 15 states COM(2013) 173 final of 27.3.2013. Part of the proposal was replaced by the proposal for a Regulation establishing a European Union agency for law enforcement training Cepol (COM (2014) 465 final of 16.7.2014).

Currently before the co-legislators, seeks to enhance Europol's analytical capabilities, trigger operational action on the part of Member States, and reinforce the agency's data protection regime. Member States should use Europol as their channel of first choice for law enforcement information sharing across the EU. Europol's Secure Information Exchange Network Application (SIENA) allows Member States to exchange information in a swift, secure and user-friendly way with each other, with Europol, or with third parties that have a cooperation agreement with Europol. The active use of information exchange instruments also needs the right interface between the EU's tools and national law enforcement systems, such as **Single Points of Contact**. Member States must put the right structures in place at national level to integrate and coordinate the work of the relevant authorities. Tracking the movements of offenders is key to disrupting terrorist and criminal networks.

It is now urgent that the co-legislators finalize their work on the establishment of an **EU Passenger Name Record (PNR)** system for airline passengers that is fully compatible with the Charter of Fundamental Rights while providing a strong and effective tool at EU level. Analysis of PNR information provided at the time of booking and check-in helps to identify high risk travelers previously unknown to law enforcement authorities. PNR data has proven necessary to identify high risk travelers in the context of combatting terrorism, drugs trafficking, trafficking in human beings, child sexual exploitation and other serious crimes. Once adopted, the PNR Directive will ensure better cooperation between national systems and reduce security gaps between Member States. Common risk indicators for the processing of PNR data will help to prevent criminals escaping detection by travelling through another Member State. Europol and Frontex can again play a key role in developing and distributing such risk indicators on the basis of information received from Member States.

The EU has concluded **PNR agreements** with the United States, Canada and Australia.

Such cooperation has real added value in identifying and apprehending foreign terrorist fighters, drug traffickers or travelling sex offenders. The Union’s future approach to the exchange of PNR data with non-EU countries will take into account the need to apply consistent standards and specific fundamental rights protections. Once the European Court of Justice has issued its opinion on the draft PNR Agreement with Canada, and based on the Court's conclusions, the Commission will finalize its work on legally sound and sustainable solutions to exchange PNR data with other third countries, including by considering a model agreement on PNR setting out the requirements third countries have to meet to receive PNR data from the EU.

Common rules on **data protection** will enable law enforcement and judicial authorities to cooperate more effectively with each other, as well as building confidence and ensuring legal certainty. Agreement by the

end of 2015 on the Data Protection reform as a whole is key, and particularly on the proposal for a Data Protection Directive for police and criminal justice authorities. In addition, the European Union is negotiating with the United States government an international framework agreement ("Data Protection Umbrella Agreement") in order to ensure a high level of protection of personal data transferred between the EU and the US for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

Communications data can also contribute effectively to the prevention and prosecution of terrorism and organized crime. Following the judgment of the European Court of Justice on the Data Retention Directive, the Commission will continue monitoring legislative developments at national level.

Fighting criminal organizations active in several EU countries also requires information exchange and cooperation between judicial authorities. 26 Member States are using the **European Criminal Records Information System** (ECRIS), which allows for information exchange on previous convictions for EU nationals. However, it does not work effectively for non-EU nationals convicted in the EU. The Commission will accelerate the work already under way to improve ECRIS for non-EU nationals and is ready to contribute to its effective implementation.

The real-time availability of existing data across Member States is an area for future work on information exchange. In response to a request made by the Council (fn17), the Commission will assess the necessity and potential added value of a **European Police Record Index System (EPRIS)** to facilitate cross-border access to information held in national police records. In the meantime, the Commission is supporting the launch of a pilot project planned by a group of Member States to establish the mechanisms for automated cross-border searches in national indexes on a 'hit'/'no hit' basis. (fn18)

Finally, the **Maritime Common Information Sharing Environment** (CISE) will enable interoperability of relevant security data in areas such as piracy, terrorism, arms and drugs smuggling, human trafficking, environmental pollution, civil protection and natural disasters between competent authorities within their existing mandates EU action must focus first of all on the **full implementation of rules already in place** – such as the Prüm framework – and **adoption of proposals already on the table** – such as the EU PNR Directive, the Europol Regulation and the Data Protection reform. This will already constitute a major step forward by putting in place a clear, secure, and properly regulated set of tools to give the authorities the information they need – as long as these tools are used to their full potential. **Key instruments** like the Schengen Information System, the Schengen Border Code and ECRIS should also be kept under review and any gaps in coverage filled.

ANNEX 2: ENISA

ENISA focuses on the implementation of aspects of ”by design” and “by default” paradigms and modelling of data protection and privacy requirements, such as:

- Machine readable representations and automatic evaluation of policies
- Enabling transparency: technological and organizational challenges
- Technical solutions for the enforcement and the implications of the subject’s right, e.g. right to erasure, access and correction
- Aspects of privacy impact and risk assessment
- Technical solutions for data portability
- Sustainable business models for privacy friendly online services
- Information and consent in online environments: practical solutions and implementations
- Privacy education, reliability and usability of PETs
- Trust services for the protection of personal data - privacy aware trust services (i.e. electronic certificates, signatures, etc.)
- Security measures for the protection of personal data
- Economics of privacy and personal data
- Legal, technical and organizational aspects of privacy and law enforcement

ANNEX 3: A proposal for a Directive COM(2017)0489

Combating fraud and counterfeiting of electronic payments; a proposal for a Directive COM(2017)0489

EUROPEAN COMMISSION Brussels, 13.9.2017 SWD(2017) 299 final COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JH.

Source: https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-489_en

Executive Summary Sheet; Summary of impact assessment SWD(2017) 298 final
Impact assessment of a proposal for a Directive combating fraud and counterfeiting of non-cash means of payment
A. Need for action
What is the problem and why is it a problem at EU level?
Three problems were identified as drivers of non-cash payment fraud: 1. Some crimes cannot be **effectively investigated and prosecuted** under the current legal framework. 2. Some crimes cannot be **effectively investigated and prosecuted** due to **operational obstacles**. 3. Criminals take advantage of gaps in **prevention** to commit fraud. Non-cash payment fraud is **a threat to security** (is a source of income for organized crime and therefore an enabler for other criminal activities such as terrorism, drug trafficking and trafficking in human beings). In addition, it is **an obstacle to the digital single market** (reduces consumers' trust and causes direct economic losses).
What should be achieved?
Two general objectives: • **Enhance security,** by reducing the attractiveness (i.e. reduce gains, increase risk) for organized crime groups of non-cash payment frauds as a source of income. • **Support the digital single market,** by increasing the trust of consumers and businesses in the payment processes as well as by reducing the direct losses caused by non-cash payment fraud. Three specific objectives: • Ensure that a clear, robust and **technology neutral** policy/legal framework is in place. • Eliminate **operational obstacles** that hamper investigation and prosecution. • Enhance **prevention.**
What is the value added of action at the EU level (subsidiarity)?
Non-cash payment fraud has a very important **cross-border** dimension. Therefore, Member States cannot effectively combat it alone or in an uncoordinated manner with other countries. EU action also facilitates cooperation with non-EU countries given that the international dimension of non-cash payment fraud frequently goes beyond EU borders.
B. Solutions
What are the various options to achieve the objectives? Is there a preferred option or not? If not, why?

Option A: improve implementation of EU legislation and facilitate self-regulation for public-private cooperation. **Option B:** introduce a new legislative framework and facilitate self-regulation for public-private cooperation. **Option C:** same as option B but with provisions on encouraging reporting for public-private cooperation instead of self-regulation, and new provisions on raising awareness. **Option D:** same as option C but with additional jurisdiction provisions complementing EIO and injunction rules. **Option C is the preferred option,** both qualitatively and in terms of costs and benefits.
What are different stakeholders' views? Who supports which option?
In general, stakeholders expressed doubts about the relevance, effectiveness and added value of the current legal framework (Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment). In particular, stakeholders agreed that the definitions included in the Framework Decision are not up-to-date (in particular, experts from judicial authorities pointed out the case of virtual currencies; this was also widely supported by views expressed by individuals and stakeholders during the open public consultation) and that new offences, not included in the legislation, should be considered (experts from law enforcement and judicial authorities indicated in particular the sale, acquisition and making available of stolen credentials; this was also widely supported by contributions received during the open public consultation). Stakeholders indicated the need to improve cooperation between national authorities and between public authorities and the private sector. Stakeholders from financial institutions and other private parties (e.g. merchants) complained about the lack of legal certainty, which hampers their ability to share information, while experts from law enforcement noted that the time to obtain the information does not allow for effectively investigate crime.

ANNEX 4: Report on top EU crimes priorities; illegal migration

Statewatch report on top EU crime priorities (11 October 2017)

Erkki Koort, who chairs an internal security group at the European Council, representing member states, told MEPs on Tuesday (10 October) that fighting "the facilitation of illegal migration" involves more EU states than any other crime; followed by human trafficking, synthetic drugs and then more conventional narcotics like cannabis and cocaine; weapons trafficking and child sexual exploitation were lower priorities. Other major issues include value-added tax fraud.
See: **Migrant smuggling tops EU crime priorities** (EUobserver, link)

The EU policy cycle on serious and organized crime
The EU policy cycle on serious and organized crime was first set up in 2010, having emerged from the Belgian-led 'Project Harmony' aimed at enhancing cross-border police cooperation in the EU. It has become increasingly formalized and better-funded in recent years, with the establishment of an acronym-heavy management system based around Europol and the Council of the EU, in particular the Standing committee on operational cooperation on internal security (COSI). The next policy cycle runs from 2018 to 2021. Priorities include one Operational Action Plan:
"3) To disrupt OCGs who facilitate illegal immigration by providing facilitation services to irregular migrants along the main migratory routes crossing the external border of the EU and within the EU, particularly focusing on those whose methods endanger people's lives, those offering their services online and making use of document fraud as part of their business model.
See: **Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021** (9450/17, 19 May 2017, pdf) and: **Council Conclusions on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021** (7704/17, 28 March 2017, pdf)
For background on the policy cycle and how it is organized see: **EU joint police operations target irregular migrants** by Chris Jones (Statewatch Journal vol 23 no 3/4, February 2014)
Statewatch published the Council report of April 2017, a Restricted document that shows extent of law enforcement cooperation on the issue of "facilitated illegal immigration" (FII) on the implementation of the Operational Action Plan (OAP) for 2016. See: **EU Policy Cycle - Implementation monitoring: Progress Report OAP 2016 - Facilitation of illegal immigration** (6709/17, RESTRICTED, 26 April 2017, pdf)

The report contains details of work undertaken on the following actions:

OA 1.1 Provision of the situational picture of the current trends within the irregular migratory pressure. Europol FP Checkpoint Early Warning Notifications / Frontex risk analysis updates and other strategic intelligence products

OA 2.1 Establishment of a Joint Operational Office (JOO) in Vienna (AT) for the fight against OCGs facilitating illegal immigration into the EU via the south-eastern route and the Balkan route

OA 2.2 TranSEEt (Transiting South East Europe): Investigative action targeting organized crime groups operating on the south East/Western Balkan route

OA 2.3 JOT COMPASS II: Action focusing on OCGs facilitating illegal border crossings towards and through Western European countries of the EU internal borders, and consequently on the illegal immigration predominantly transiting from The Central Mediterranean area into EU

OA 2.4 Integrate money laundering and asset recovery techniques on all operational actions where substantial criminal proceeds are suspected

OA 2.5 Dismantling criminal networks facilitating illegal immigrants from Turkey to Greece in order to get to South East and Central Europe.

OA 2.6 Operational Action PEGASUS focused on tackling the facilitated irregular migration within air border domain.

OA 2.7 Tackling human smuggling in the Western Mediterranean.

OA 3.1 ID FRAUD II (Identity Fraud): To identify and disrupt OCGs using document fraud and specifically ID fraud for the purpose of facilitating illegal immigration.

OA 4.1 Marriages of convenience: Share data with Europol of cases where there is suspicion of marriage of convenience with OC involvement

OA 5.1 Network of liaison officers in Libya

OA 5.1 Turkey Organized Immigration Crime Working Group (TOICWG). Development in capability and capacity of Turkey Organized Immigration Crime Working Group

OA 5.2 Joint Operational Team MARE: JOT, as part of the European Migrant Smuggling Centre (EMSC), to tackle OCGs active organizing ship facilitations in the Mediterranean toward the EU and subsequent secondary movements inside the EU.

OA 5.3 WB 2016: OA focused on Western Balkans Operational Area to be implemented by means by means of selected and fine-tuned Frontex Joint Operations and additionally prepared Joint Action Day.

OA 5.4 Eurosur: Eurosur Fusion Services (EFS) for the sake of detecting, preventing and combating illegal immigration and cross-border crime

OA 5.5 Africa Frontex Intelligence Community (AFIC) development: The AFIC is a platform for joint analyses and common knowledge sharing with respect to border security, irregular trans-border movement of people, trans-border criminality.

OA 6.1 Develop and implement Illegal Immigration related training activities for EU law enforcement specialists in order to exchange good working practices

OA 6.2 Training on advanced skills on detection of falsified documents

OA 6.3 Training for Visa Section Staff of EU MS / SAC embassies and consulates in third countries.

OA 6.4 Intelligence gathering capacity building at the borders.

OA 6.5 Regional Forum: Conference for Chief of Police (if necessary, extended to, or followed by Border Police/Criminal Police high rank officers' meeting) on organized crime and migration issues with reference to the Western Balkans/South East European route and to Western/Central/Eastern Mediterranean route.