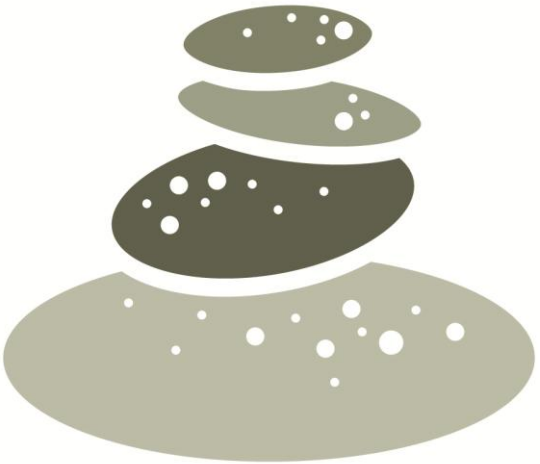

Vrije
Universiteit
Brussel

INTERDISCIPLINARY
STUDIES OF LAW
[METAJURIDICA]
VRIJE UNIVERSITEIT BRUSSEL



LSTS

LAW, SCIENCE, TECHNOLOGY & SOCIETY STUDIES

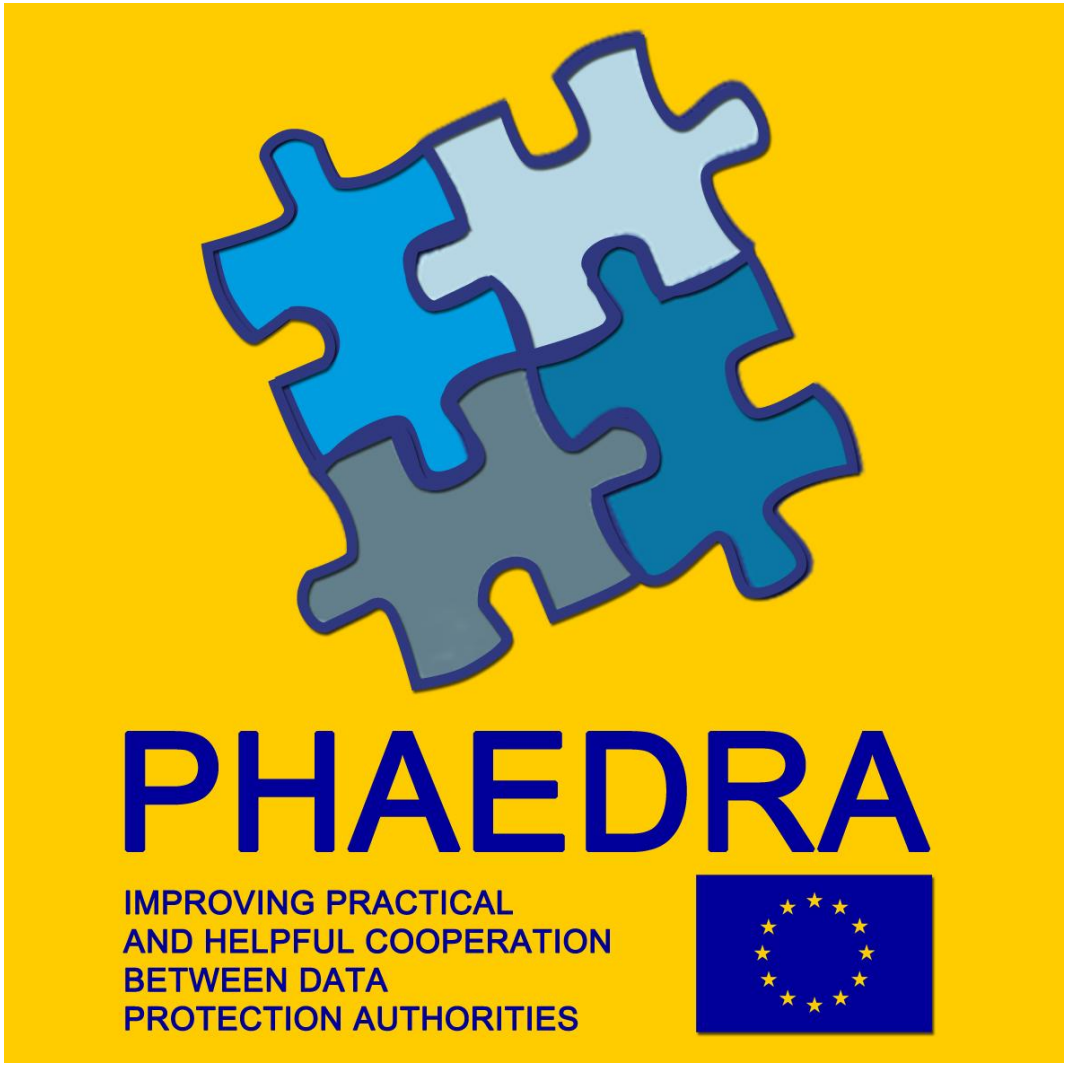
VRIJE UNIVERSITEIT BRUSSEL

BELGIUM


PRIVACY
BROTHER
NETWORKS
PROTECTION
EUROPEAN
BIG
DATA
SURVEILLANCE
TECHNOLOGIES
SCIENCE
BIOTECHNOLOGY
TARGETING
DUBSTEP
LES
SCANNERS
AUTHORITIES
CARE
HEALTH
ITALIE
PRIVACYCAMP
ASSESSMENT
RIGHTS
PARLIAMENT
DISCRIMINATION
BROTHER
ETHICS
MUSIC
MOBILE
NETWORKS
PHAEDRA
PRESCIENT
AUTRES
PUBLIC
HIRSI
COPYRIGHT
EMSOC
ECTHR
PIAF
BORDERS
STUDIES
JUSTICE
INTELECTUAL
IMPACT
FACEBOOK
EUROSUR
MHEALTH
PROFILING
PNR
LOCATION
PROTECTION
READING
SOCIAL
MEDIA
AWARDS
PROPERTY
EMERGING
EU
SIAM
SURVEILLANCE
TECHNOLOGIES
PHILOSOPHY
SURVEILLANCE
INNOCENCE
PARTY
DATA
USE
LISS
LAW
PRÜM
SLOW
BODY
SCIENCE
SOCIAL
CONTEXTUAL
PIAS
EU
POLICE
EUROPEAN
SMART
BEHAVIOURAL
PROPERTY
EHEALTH
ART
AWARDS
CPDP
EMERGING
BORDERS
ACTA
PRIVATE
UNION
FUNDAMENTAL
SECURITY
FRONTEX
INTELLECTUAL
PRESUMPTION
JAMAA
FOUCAULT
DAY
PRIVACY
SPHERE
DISCRIMINATION
BIOTECHNOLOGY
SCANNERS
AUTHORITIES

PIAF

PRIVACY IMPACT ASSESSMENT FRAMEWORK


PHAEDRA
IMPROVING PRACTICAL
AND HELPFUL COOPERATION
BETWEEN DATA
PROTECTION AUTHORITIES

7th INTERNATIONAL CONFERENCE

22 23 24 JANUARY 2014 • BRUSSELS BELGIUM

COMPUTERS, PRIVACY & DATA PROTECTION

REFORMING DATA PROTECTION: THE GLOBAL PERSPECTIVE

WWW.CPDPCONFERENCES.ORG

part 1
new tools to protect: pia case-study

PIAF

A Privacy Impact Assessment Framework for data protection and privacy rights

Deliverable D1

Editors:
David Wright, Trilateral Research & Consulting
Kush Wadhwa, Trilateral Research & Consulting
Paul De Hert, VUB-LSTS
Dariusz Kloza, VUB-LSTS

Prepared for the European Commission
Directorate General Justice

JLS/2009-2010/DAP/AG

21 September 2011

PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK

PIAF

A Privacy Impact Assessment Framework
for data protection and privacy rights

Deliverable D2

Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union

Editors:
Gus Hosein, Privacy International
Simon Davies, Privacy International

A projected co-funded by the European Commission's Special Programme
"Fundamental Rights and Citizenship," 2007-2013.
JLS/2009-2010/DAP/AG

PIAF
PRIVACY IMPACT
ASSESSMENT FRAMEWORK

Introduction of PIA policy

- High-level support for PIA
- Compulsory nature
- A firm legal basis
- Conflicts of interest
- Multi-organization and trans-border dimension
- Leadership of the data protection authorities
- Complementary with prior checking

PIA policy: the core elements

- An on-going process
- Scalability
- All privacy types
- Accountability
- Transparency
  - Publication of the PIA report
  - Central registry
  - Sensitive information
- Stakeholders' involvement
- Risk management
- Audit and review

PIA practice: introduction

- Internal management of PIA
  - Internal architecture
  - Privacy awareness
  - Professional independence of an assessor
- Preliminary issues
  - Threshold analysis
  - Determination of the scale and scope of PIA
  - Roles and responsibilities

PIA practice: the process

1. Early start
2. Project description
   - General description of the project
   - Information flows and other privacy implications
3. Stakeholders' consultation
   - Identification
   - Information
   - Consultation
   - Consideration
4. Risks management & legal compliance check
   - Risk assessment
   - Risk mitigation
5. Recommendations and report
6. Decision & implementation of recommendations
7. Audit & review
8. PIA is a living instrument

part 2
environmental democracy

privacy is the new green
robin wilton

fundamental rights
deliberative democracy
corporate responsibility
informed decision-making
…

a consultation is a way to gather fresh input
on the perceptions of the severity of each risk
and on possible measures to mitigate these risks

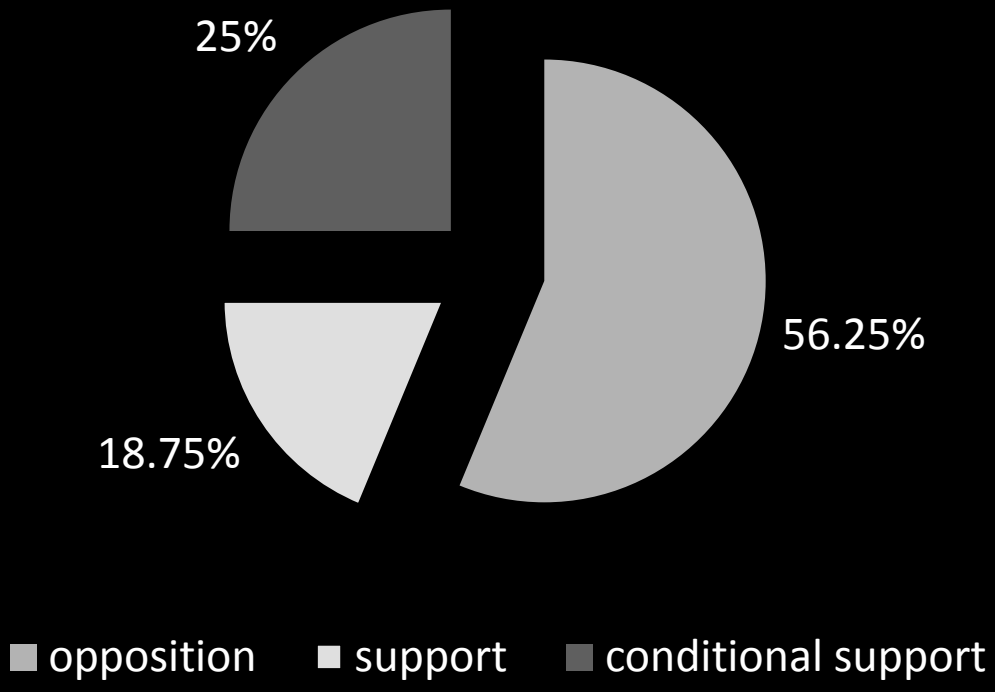
wright & de hert

Features The PIA guide…	Australia	Victoria	Canada	Ontario	Alberta	Ireland	NZ	UK ICO	US OMB	US DHS
reviewed here, was published in	May 2010	Apr 2009	Aug 2002	Dec 2010	Jan 2009	Dec 2010	Oct 2002-2007	June 2009	Sept 2003	June 2010
says PIA is a process	✓	✓	✓	✓		✓	✓	✓	✓	✓
contains a set of questions to uncover privacy risks (usually in relation to privacy principles)	✓	✓	✓	✓		✓	✓	✓		✓
targets companies as well as government	✓	✓			✓	✓	✓	✓		
addresses all types of privacy (informational, bodily, territorial, locational, communications)	✓	✓		✓						
regards PIA as a form of risk management	✓		✓	✓		✓		✓	✓	✓
identifies privacy risks	✓	✓	✓	✓		✓	✓	✓		
identifies possible strategies for mitigating those risks		✓					✓			
identifies benefits of undertaking a PIA	✓	✓	✓			✓	✓	✓		
supports consultation with external stakeholders	✓	✓				✓		✓		
encourages publication of the PIA report	✓	✓	summary		summary		✓	✓	✓	✓
provides a privacy threshold assessment to determine whether a PIA is necessary	✓	✓	✓			✓		✓	✓	✓
provides a suggested structure for the PIA report	✓	✓	✓		✓		✓	✓	✓	✓
defines "project" as including legislation and/or policy		✓								
says PIAs should be reviewed, updated, ongoing throughout the life a project	✓	✓			s✓	✓	✓	✓	✓	✓
explicitly says a PIA is more than a compliance check	✓	✓	✓	✓				✓		
The PIA policy provides for third-party, independent review or audit of the completed PIA document.			✓		✓		✓		✓	✓
PIA is mandated by law, government policy or must accompany budget submissions.			✓	✓	✓	✓		✓	✓	✓
PIA reports have to be signed off by senior management (to foster accountability).		✓	✓	✓	✓	✓			✓	✓

Canadian PIAs seldom involve public consultation, opinion polling or other means of gauging the privacy values of the Canadian public. They tend to focus on legal compliance rather that doing the right thing and asking larger questions.

the final PIA reports often fail to acknowledge …
give it limited berth …
details on such consultations are lacking …
the stakeholders are not adequately identified …
piaf deliverable d1

most dpas oppose mandatory external stakeholder engagement



piaf deliverable d2
wright & wadhwa

… such an obligation makes sense especially
for products and services that will necessarily affect
a specific category of people in everyday life:
employees, hospital patients, public transport users, etc. …

cnil

4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

com(2012) 11 final

access to environmental information
public participation in decision-making
access to justice

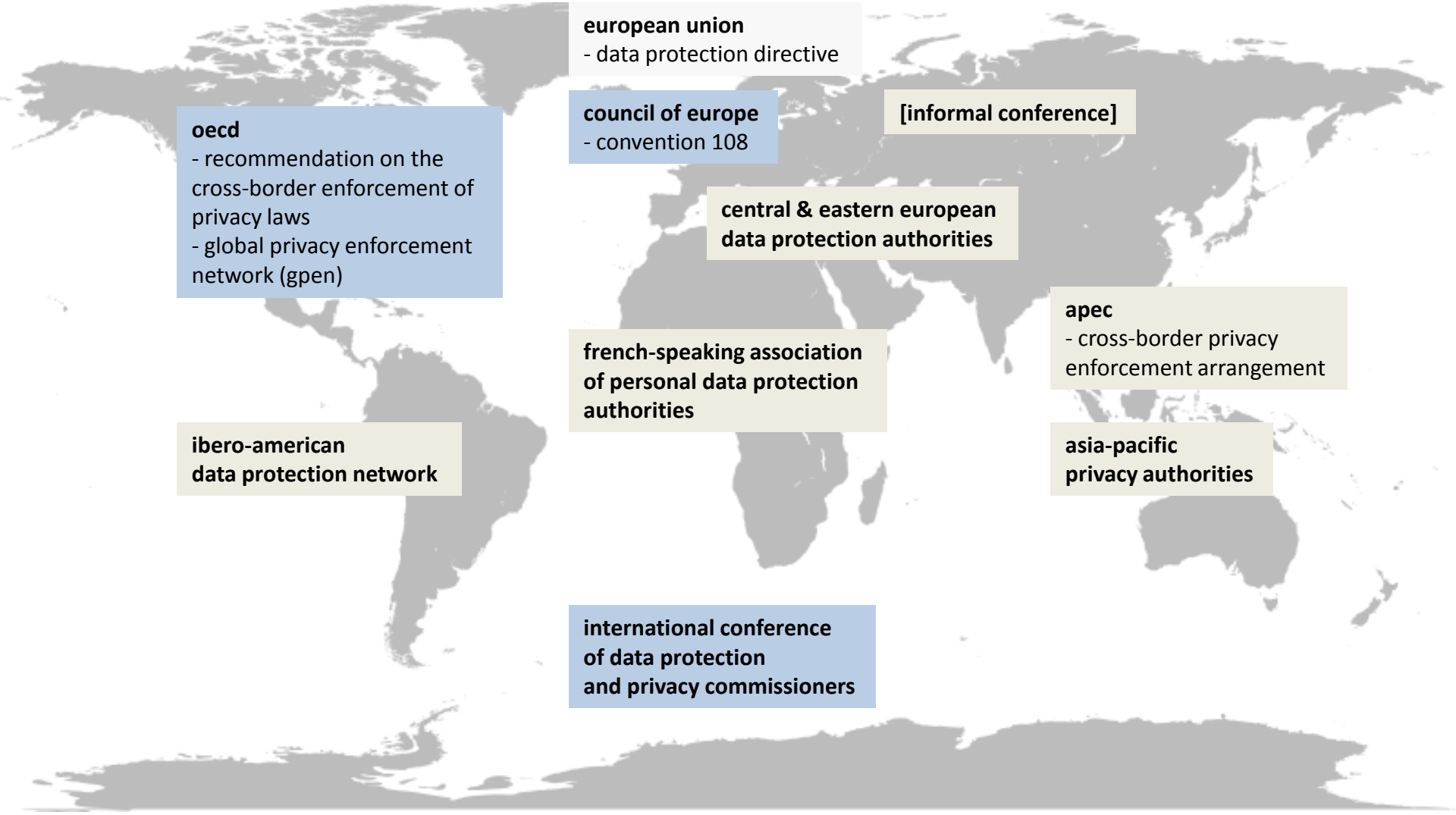
aarhus convention 1998

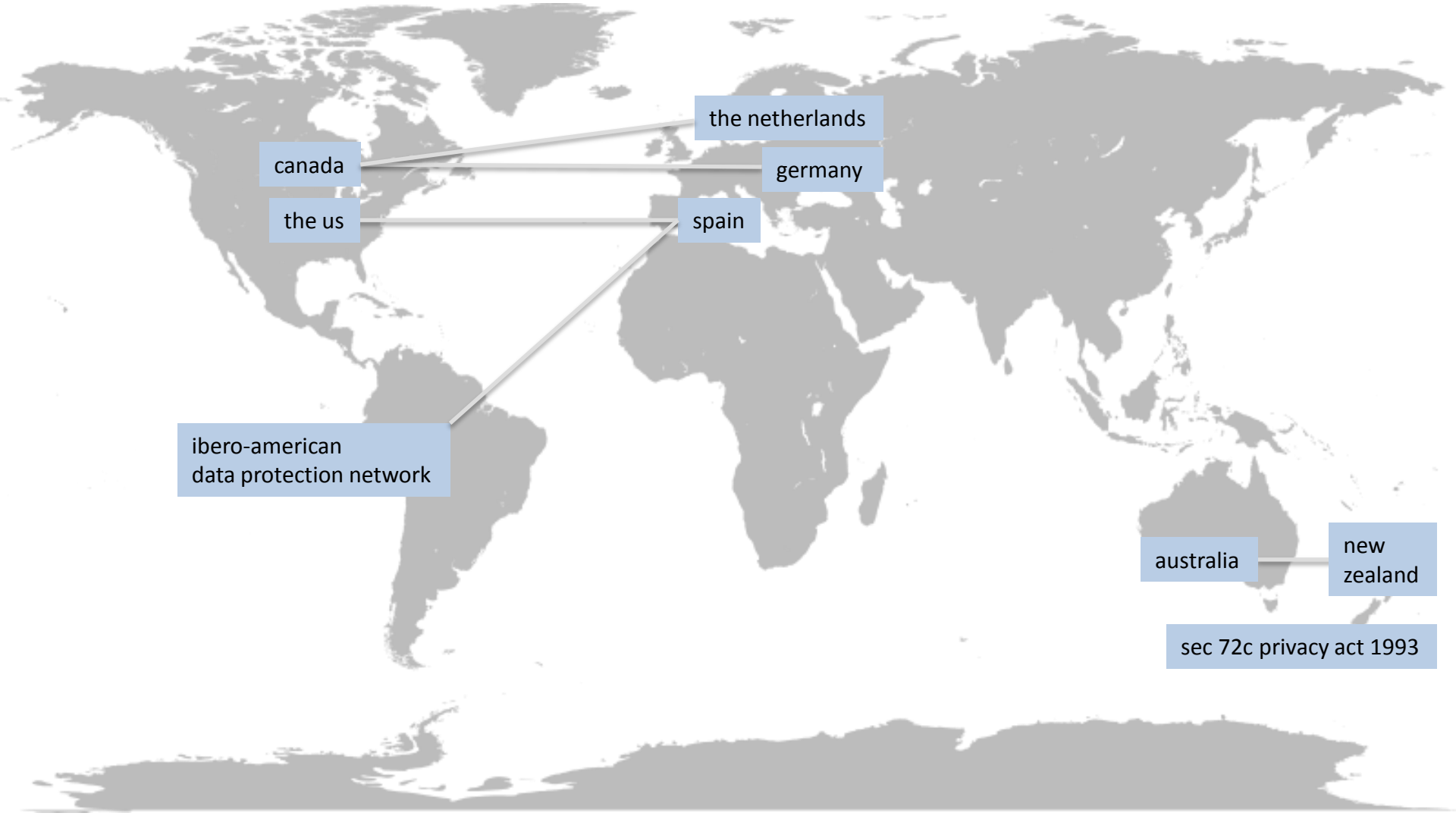
… the importance of public access to … to information
… the views of individuals were taken into account …
… individuals must … be able to appeal to the courts
echr: taskin et al v turkey

aarhus system for privacy?

will the public actually take part?
what is covered already?
additional red-tape?

part 3
co-operation of authorities


european union
- data protection directive
council of europe
- convention 108
[informal conference]
oecd
- recommendation on the cross-border enforcement of privacy laws
- global privacy enforcement network (gpen)
central & eastern european data protection authorities
apec
- cross-border privacy enforcement arrangement
french-speaking association of personal data protection authorities
ibero-american data protection network
asia-pacific privacy authorities
international conference of data protection and privacy commissioners


the netherlands
canada
germany
the us
spain
ibero-american
data protection network
australia
new
zealand
sec 72c privacy act 1993

(1) co-operation within the eu
(2) international co-operation

proposal for the general data protection regulation (2012)

(1)

more detailed & specific rules on co-operation
time limits or translation of documents
duty to inform each other
clarity on the extent to which information can be shared

wp29 advice on application art 28(6) of the directive (2011)

(1)

mutual assistance
joint investigation
consistency
european data protection board

arts 55-64 proposed general data protection regulation

(2)

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice.

art 45(1) proposed general data protection regulation

(2)

… the commission shall take appropriate steps to advance the relationship
with third countries or int'l organisations …

art 45(2) proposed general data protection regulation

mutual assistance
investigation or interventions
provide information on law & practice
convention committee

council of europe – proposed modernisation ets 108 (november 2012)

… to organise their co-operation and to perform [their] duties … the supervisory authorities … shall form a conference/network …

art 12bis(8) proposed modernisation ets 108

mechanisms for co-operation within eu
some basis for co-operation with 3rd jurisdictions
some novelties in ets 108
yet certain practicalities still to be dealt with

wp29 & cnil vs. google (2012-)
opc canada & cbp vs. whatsapp (2012-2013)

enforcement co-operation in competition matters

int’l competition network

established october 2001
network of (national or multinational) nca's
specialized exclusively in competition law
informal
voluntary
project-based
consensus-based
virtual yet structured

procedural & substantive convergence
dissemination of expertise & best practices
facilitation of int'l co-operation & mutual understanding
not a forum of co-operation on individual cases

forum for informal contacts
recommendations & best practices
reports
case-handling & enforcement manuals
templates & toolkits

european competition network

based on regulation 1/2003
created may 2004
co-operation in enforcement of unified rules

efficient division of work between authorities
effective & consistent application & enforcement of law
coherent development of eu competition policy

mechanism for case allocation
rules on conflicts between nca's and commission
consultation and assistance mechanism within ecn

info on new cases
assistance in fact-finding measures (inspections, interviews)
consultations on envisaged decisions
information exchange (incl. confidential info)

exchange of confidential information
lack of systematic notification on new cases
differences in timetables & investigation procedures
linguistic concerns
time zone differences
formal co-operation complex & time-consuming
little written guidance on co-operation
limits in resources

dpa's & ca's – comparable needs & similar obstacles:

(1) practice-oriented approach

(2) limits in sharing (confidential) information

(3) enforcement based on mandatory rules

(4) sharing best practice via informal means

…

part 4
big data

part 5
questions

privacy meeting: brussels – bangalore
cis – bengaluru – 14 august 2013

dariusz.kloza@vub.ac.be
gertjan.boulet@vub.ac.be

vub.ac.be/LSTS
piafproject.eu
phaedra-project.eu
www.cpdpconferences.org