Towards a PIA policy: Learning from others

David Wright
Trilateral Research & Consulting
Berlin, 25 November 2011

Current projects

SAPIENT – Surveillance impact assessment [for DG ENTR]

PRESCIENT – Privacy and ethical impact assessment re emerging technologies [for DG Research]

PIAF – A Privacy Impact Assessment Framework for Europe [for DG Justice]

- D1 – reviews PIA policies & methodologies in Australia, Canada, Hong Kong, Ireland, New Zealand, the UK and US
- D2 – survey of EU Member States re introduction of PIA
- D3 – Recommendations re an optimised policy & methodology

Publications

- PIAF Deliverable D1, www.piafproject.eu
- Wright, David, "Should privacy impact assessments be mandatory?", *Communications of the ACM*, Vol. 54, No. 8, August 2011, pp. 121-131.
- Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.
- Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review,* Vol. 28, No. 1, Feb 2012 [forthcoming]

Definition of privacy impact assessment

- A methodology for assessing the impacts on privacy of a project, service, product, policy, programme or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts [Wright & De Hert, 2012]

- A PIA is about identifying risks and finding solutions, not simply producing a report that demonstrates compliance

PIA approaches across countries

PIA features	AU	CA	NZ	UK	US
PIA is mandated by law or must accompany budget submissions.		☑	Varies	☑	☑
PIA guidance is targeted at government departments and agencies only (G) or private sector as well ☑.	☑	G	☑	☑	G
PIA guidance has been prepared by the funding agency (F) or by privacy commissioner (P).	P	F	P	P	F
PIA should be initiated at early stage of project development.	☑	☑	☑	☑	☑
PIA guidance focuses on privacy risks involving personally identifiable data.	☑	☑	☑	☑	☑
Guidance puts emphasis on the process and not just preparation of report.	☑	☑		☑	
PIA guidance explicitly encourages engaging external stakeholders.	☑	Varies	☑	☑	
Guidance has a template for preparation of report.	☑	☑	☑	☑	Varies
Policy provides for 3rd party independent review of completed document.		☑			Varies
Report or summary is to be published on agency's website.		☑	Varies		☑
Guidance says PIA report may need to be revised or updated or a new process undertaken.	☑	☑	☑	☑	☑

Benefits of PIA

- An early warning system, a way to detect privacy problems, build safeguards before, not after, heavy investment – Fix privacy problems now, not later
- Avoids costly or embarrassing privacy mistakes
- Provides evidence that an organisation attempted to prevent privacy risks (reduce liability, negative publicity, damage to reputation)
- Enhances informed decision-making
- A way to gain the public's trust and confidence
- Demonstrates to employees, contractors, customers, citizens that the organisation takes privacy seriously

Features to ensure the effectiveness of PIA

- Who initiates a PIA and who approves it?
- Threshold analysis – Is a PIA necessary?
- Clarify for whom the PIA is prepared
- A PIA should be regarded as a process. It is not simply about preparing a report
- Scale and scope of the PIA – should reflect complexity and significance of privacy risks
- PIA should be started when there is still an opportunity to influence decision-making
- PIA is part of risk management – more than compliance
- Questions to identify risks and solutions
- PIAs are only as good as the processes that support them

Features to ensure the effectiveness of PIA (2)

- Training and raising awareness of employees
- Mandatory PIAs
- Engaging stakeholders
- Recommendations and an action plan
- Publication of the PIA report
- Monitoring implementation of recommendations
- Third-party review and/or audits
- Tying PIAs to budget submissions
- A central registry of PIAs
- Putting accountability for PIAs at highest level

DPIA or PIA: seven types of privacy

- Privacy of personal information
- Privacy of the person (bodily privacy)
- Privacy of personal communications
- Privacy of personal behaviour (Clarke, ICO)
- Privacy of thought and feelings
- Privacy of location
- Privacy of the group and association (Wright, PRESCIENT)

Learning from others

- Europe should take advantage of the experience of Australia, Canada, New Zealand, the US as well as the UK and Ireland
- Europe should take the best elements of existing policies and methodologies to create its own "optimised" policy and methodology
- Europe needs to gain some experience with PIAs before standardising a methodology
- Europe should set a high standard

Thank you.

david.wright@trilateralresearch.com

www.trilateralresearch.com