



# **Privacy Impact Assessments:**

## ***Experiences from industry***

Toby Stevens, Director  
Enterprise Privacy Group





# Introduction

---

- Privacy Impact Assessments are a relatively new concept for most UK private companies
  - public authorities at least have greater experience of the concept through the likes of Equality Impact Assessments
- The ICO has just updated the PIA process, and there are numerous other processes available
- My focus will be on the usage context for PIAs
  - motivations and uses for the PIA process
  - barriers, obstacles, pitfalls, opportunities
  - exploiting the deliverables



# About the Enterprise Privacy Group

---

- A consultancy and think-tank developing best practice in the management of personal information
- Specialists in facilitating and resolving complex and contentious privacy issues
  - DfT: National Road Pricing conferences
  - HM Treasury: Public-Private Forum on ID Assurance
  - IPS: ID Cards Stakeholder Engagement
- Authored the Information Commissioner's Privacy by Design report
- *The views I give today are my own and do not necessarily reflect those of my clients or EPG member organisations*



## Our PIA experience

---

- Our commercial experience includes four PIAs of particular note
  - for Aegate: privacy implications of using RFID technologies to authenticate prescription pharmaceuticals at point of sale
  - for DfT: privacy implications of national time-distance-place road pricing policy
  - ongoing: privacy implications of population-scale biometric enrolment and verification
  - ongoing: privacy implications of real-time monitoring of domestic energy usage



## Motivations - why conduct a PIA?

---

- The primary use of a PIA should be “to understand the privacy implications of...”
- Motivations for requesting a PIA may include
  - *compliance*: because we have to
  - *solution*: because we’re not sure what the best way is to do what we wish to do
  - *risk management*: because we’re worried that people won’t like what we’re doing
  - *publicity*: because this might help to promote what we’re doing
  - *aspiration*: because we want to do this right
- Very few organisations want to deliver *privacy*



## Motivations - why conduct a PIA?

---

- The triggers for the PIAs we conducted included
  - *protests*: concerns that the project would create significant public protests (as they did in one case)
  - *accreditation*: demonstrating compliance with the Data Handling review so that the delivered system would be fit for accreditation
  - *sales*: removing privacy concerns as a possible barrier to selling the system
  - *risk control*: spotting potential problems before it was too late to fix them



# Barriers, obstacles, traps, pitfalls

---

- The PIA has to happen as early as possible in the programme (ideally as part of the business case)
  - there will be many unanswered questions
  - often difficult to engage with external stakeholders because of commercial confidentiality
- Be ready for at least three iterations of the review: screening process, small-scale, full-scale
  - possibly interim releases as project develops
  - redacted release to shield commercial issues



# Barriers, obstacles, traps, pitfalls

- Internal stakeholders may resist the process
  - projects often see it as a burden
  - PR managers are often very wary of stakeholder engagement or publication
  - security officers may consider this to be their bailiwick, or covered in existing risk management
- External stakeholders will often be reluctant to engage
  - the ICO does not have resources to validate PIAs
  - civil society groups are in the same recession as the rest of us, and are desperately under-resourced



# Barriers, obstacles, traps, pitfalls

---

- Public engagement is never simple, but can be made easier if you are open and honest
  - assume that anything you discuss with external stakeholders may be turned against you
  - don't attempt to request NDAs, Chatham House rule will normally suffice
  - don't bother with external engagement if there is no opportunity to actually change the deliverables



# Exploiting the deliverables

---

- Remember that the PIA document is a living project management tool - it *must* be reviewed and revised
- For high-profile projects, a workshop can be extremely effective, but *must* have full support from the organisation and delivery partners
- The PIA is about data subjects' personal information - so why *shouldn't* it be published?
  - don't publicise the existence of the PIA process if you're not prepared to share the output
- The best-intentioned PIA can still backfire if the project flies in the face of stakeholder wishes



# Tips and tricks

---

- If you don't know the organisation, buddy up with the longest-serving member of the audit team
  - likely to be able to open any door you wish
- Be completely flexible in approach. There is no point in using a prescribed PIA method if it doesn't fit t
- Put disproportionate effort into identifying stakeholders, and seek out their views
- You will almost certainly encounter important issues that aren't strictly privacy-related - don't ignore them
- Never submit a report that isn't a DRAFT until it has been formally accepted by the project owner!
  - give them a chance to fix the problems



## Budget and duration

---

- Clearly the PIA effort will depend upon the scale, complexity and sensitivity of the project in question
- Once you are familiar with the nature and detail of the project, typical durations might be
  - Screening Process: 0.5 days
  - Small-Scale PIA: 5 days
  - Full-Scale PIA: 5 days (depending upon number of stakeholders)



## Finally - when to walk away...

- Sometimes the PIA is simply too high-risk and you do not want to be involved if
  - the motivation is to paper over the cracks or try to persuade stakeholders that a bad project is in fact privacy-friendly
  - you are not able to examine every aspect of the project or report all findings
  - key stakeholders are out of scope or refuse to participate
  - there is a risk that your name will be used to convince stakeholders of the project's credibility
- *Otherwise... get stuck in and good luck!*

# Enterprise Privacy Group

[www.privacygroup.org](http://www.privacygroup.org)

01420 561856

