transactional anonymity in privacy principles – Australia and elsewhere –

Graham Greenleaf
UNSW Faculty of Law

OII AnonEvent, London 8-12-11

Anonymity in privacy principles

1. De-identification required once purposes of collection complete
   - Conflicts with data retention requirements?
2. Is anonymisation a secondary use?
3. Anonymisation could breach the data quality (or security) principle
4. **Anonymity at collection?**

Is this required in EU law?

- Directive A6(1)(c) requires data collected be 'not excessive' in relation to purpose of collection.
  - Kuner (2006) sees A6(1)(c) as one basis of 'data minimization' principle that the minimum data should be processed
  - Bygrave (2003) thought that requirements of anonymity could be implied from the general 'data minimization' approach of the Directive
  - Both cite only German law as requiring anonymisation
- Conclusion: As part of EU law, a requirement of anonymous transactions is 'unproven'

Germany goes further

- A3 German Federal Data Protection Act:
  - (1) '.... systems must be oriented toward the goal of collecting, processing, and using no personal data or as few as possible'
  - (2) 'In particular, the possibilities of anonymisation and pseudonymisation are to be used insofar as is possible and the cost and effort stand in a reasonable relationship to the protective purpose which is strived for'
- Strongest European law - in principle?
  - Called 'data avoidance and data frugality' in German law
  - Derived from 1989 decision of Working Group on Telecoms re anonymity; from research by Roßnagel's research group on 'data frugality' (1995); from previous Teleservices Data Protection law 1997

Outside Europe

- Neither the OECD Guidelines nor APEC Framework require minimality in collection or de-identification after use
  - These omissions are two of their main weaknesses
- However 21/28 data privacy laws outside Europe follow Europe in requiring collection be limited to the minimum information necessary for the purpose of collection (Greenleaf 2011)
- But explicit requirements of anonymous transactions are as rare outside Europe as they are within the EU ...

Which laws **don't** require minimum collection?

- The not-so-magnificent seven:
  - Malaysia
  - Kyrgyz Republic
  - Mexico
  - Bahamas
  - Japan
  - Chile
  - Vietnam
  - *A roll-call of the world's weakest data privacy laws*
- Minimality is standard; anonymity not yet

The strange story of NPP8 (*datenschutz* down under)

- Germany passed an Act ...
- Lee Bygrave wrote an article ...
- Simon Davies convened a circus ...
- Nigel Waters & I helped write a Charter ...

... years passed ...

- The government did a U-turn ...
- The Privacy Commissioner plagiarised ...
- Parliament was asleep ...

... And NPP 8 arrived in Oz ...

NPP 8 Anonymity

- NPP8: A person must have the option of not identifying himself or herself when entering transactions with an organisation, wherever this is lawful and practicable.
- No reported complaints or cases (for injunctions) after 10 years

Proposed revision

- Draft Bill before Australian Parliament
  - APP2: 'Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.' (includes government)
- Principle may be strengthened, or destroyed - fate unknown
  - Including pseudonymity as well is good
  - Requires clarity that anonymity must be offered first
  - Dangerous proposed exception wherever an entity is 'authorised' (not required) by law to identify individuals (worse than previous 'wherever lawful and practicable')

When could 'nymity apply?

- Anonymity
  - All public transport systems and tollways
  - All online purchases if some form of digital cash is available and as reliable as credit cards (problems of IP addresses and email address remain, but are lesser)
  - All meatspace transactions where attempts are made to extract ID when cash should suffice
- Pseudonymity
  - Where tracking ex-post-facto abuse is justifiable, but up-front surveillance is not

Please suggest examples, these are just a few

Identity and necessity

- How much ID is 'necessary'?
  - Bygrave (2003): Does 'necessary' mean 'indispensable' or merely 'useful'?
  - Proposes requirement of 'proportionality' between the degree of processing and the justification for it (consistent with ECtHR)
- When is no ID 'necessary'?
  - This is the $64K question: 'Do surveillance-based business models justify collection "necessary" for surveillance, though not for the immediate transaction?'
  - This leads to another question ...

Charging for anonymity?

- Is charging more for anonymity OK?
- In favour:
  - Collection of personal data is part of many business models? ('the surveillance option')
  - If you choose the anonymity option, it is fair to charge you more. But how much more? The answer probably lies in proportionality (at least in Europe).
- Against:
  - If anonymity is a right (like 'reasonable data security') it must not be charged for without specific authority
  - Governments should not use a surveillance business model, so should not charge for anonymity

The Korean approach

- Article 16 of the new Korean Act (2011):
  - (1) The personal information processor shall collect the minimum personal information necessary to attain the purpose in the case applicable to [A 15(1) on collection]. In this case, the burden of proof that the minimum personal information is collected shall be borne by the personal information processor.
  - (2) The personal information processor shall not deny the provision of goods or services to the data subjects on ground that they would not consent to the collection of personal information exceeding minimum requirement.
- This 'no disadvantage' principle gives data subjects of refusing to pay for anonymity or minimality

Conclusions

- 'Minimality' of collection is an established principle world-wide
  - But its meaning and relation to surveillance-based business models is nowhere established
- An explicit anonymity principle has potential to:
  - Make the cost of the 'surveillance option' explicit
  - Promote real 'privacy by design' (cost of retro-fitting)
- The revised Directive and CoE 108 need an anonymity principle
  - So do the OECD Guidelines (a little joke to finish with)

And a postscript …

- The leaked proposals for an EU Regulation (+Directive) on 6/12/12:
  - A83 ('Processing for historical, statistical and scientific purposes'): Research projects must be carried out with fully anonymised data if possible; if not, pseudonymised data should be used (with key kept separately).
  - Considerable dangers that this may substitute for consent (beyond scope here)
  - So anonymity and pseudonymity are proposed to make their first explicit appearances in EU data privacy law. But it is not enough.

References & acknowledgments

- Nicol, Prins & van Dellen *Digital Anonymity and the Law* Asser Press, 2003
  - esp chapters by Grijpink and Prins, and by Walden
- Bygrave *Data Protection Law*, Kluwer, 2003, [3.3] and [18.4.3]
- Kuner *European Data Protection Law* (2nd Ed), Oxford, 2006, [2.08]-[2.12], [2.30]-[2.32]
- Greenleaf 'The Influence of European Data Privacy Standards Outside Europe' (2012) 2:2 *IDPL* (on LSN)

- Matthias Pocs (from Alexander Roßnagel's Project Group 'Constitutionally Compatible Technology') for German information
- Prof Whon-il Park for Korean translation
- Nigel Waters for joint work on APP2