

Notional and actual financial penalties for privacy breaches: Asia-Pacific and European comparisons

GRAHAM GREENLEAF AM
UNSW AUSTRALIA

4TH ASIAN PRIVACY SCHOLARS NETWORK
(APSN) CONFERENCE,
MEIJI UNIVERSITY, TOKYO, 10-11 JULY 2014

Money talks?

- 'Responsive regulation' requires 'speak softly and carry a big stick' – and use it very visibly when justified.
- Privacy laws have a bad reputation for not being enforced.
- Enforcement takes many forms; most are difficult to measure.
- Direct financial penalties are one of the simpler ways to measure *some* consequences of privacy breaches.
 - This includes fines for criminal offences, administrative fines, compensation orders, and mediated settlements.
 - *If* appropriately publicised, such penalties also send signals to all relevant parties about the costs of privacy breaches.
- They also send simple signals to the 'privacy market'
- What do we know that goes beyond anecdotes?
 - In particular, are Asian laws different from elsewhere in this respect?
 - This paper is a **first attempt** to assemble some data ...

This paper will consider ...

- 4 types of financial payments
 - Existence of powers
 - Evidence of payments
- EU data from:
 - EU Fundamental Rights Agency (FRA) report, 2013
 - Bird & Bird (law firm) case studies for 2013
 - Aurelie Pols article, 2014, based on DPA Annual Reports
 - Databases of Irish and UK DPA cases in WorldLI's International Privacy Law Library.
- Asia-Pacific data from:
 - Analysis of legislation, annual reports, websites etc gathered for book.
 - Australian data added
- Future work needed:
 - Additional regional data from USA, NZ, Canada & Mexico
 - Including data from WorldLI's International Privacy Law Library.

FRA analysis of fines (in €) by DPAs

- Fines are 'the most common course of action' taken by EU DPAs, with 19/28 States having ability to fine.
- FRA figures show fines can be over €300,000, but only cover 9 countries and with less data on frequency.

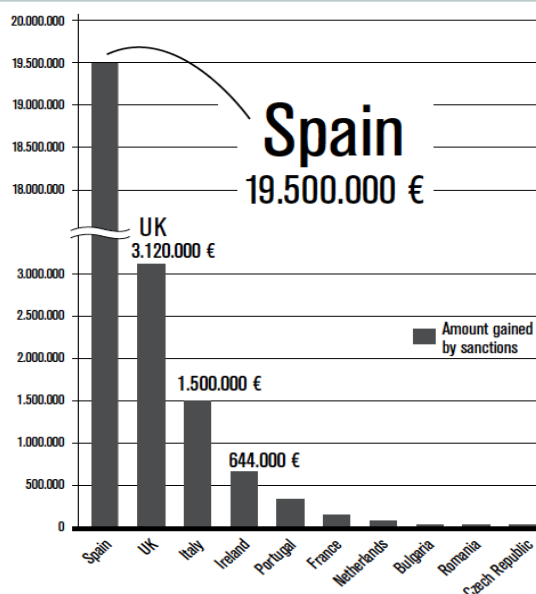
Country	Max fine	Fines 2009-11
Spain	600,000	1715
UK	500,000	9
Slovakia	332,000	45
France	300,000	
Greece	150,000	
Poland	48,000	
Hungary	35,000	
Slovenia	12,519	
Romania	12,000	148

Adding FRA analysis of fines (in €) by Courts

- FRA data on Court fines, and its source files, shows
 - FRA data is incomplete and inconsistently interpreted
- Can reasonably conclude:
 - All EU countries have either DPA or court fines, possibly both
 - Maximum amounts vary greatly, from €600K+ down to €12K.
 - Actual fines are erratically provided by FRA, but Pols has data on actuals in 2013.

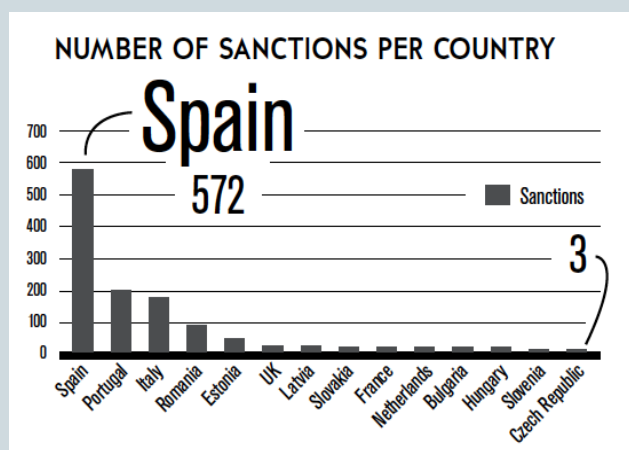
Country	DPA max	No. 09-11	Court max
Spain	600,000	1715	N/A
UK	500,000	9	No limit
Slovakia	332,000	45	None
France	300,000		300,000
Greece	150,000		30,000
Poland	48,000		
Hungary	35,000		40,000
Slovenia	12,519		
Romania	12,000	148	
Croatia			5,325
Czech Rep.			8,500
Netherlands			19,000
Malta			23,923
Portugal			30,000
Ireland	N/A	28	250,000
Latvia			50,000
Belgium	None		100,000
Luxembourg	125,000		125,000
Austria	100,000	N/A	None

Total DPA fines in 2013 in €, by country



Aurelie Pols, Privacy Laws & Business International Report, 04/14

Total instances of fines in 2013, by country



Aurelie Pols, Privacy Laws & Business International Report, 04/14

Average EU DPA fines in € per country, in 2013

Country	Total fines	No. of fines	Average fine
Ireland	644,000	2	322,000
UK	3,120,000	10	320,000
Spain	19,500,000	572	34,091
Portugal	300,000	200	15,000
France	120,000	10	12,000
Italy	1,500,000	180	8,333
Netherlands	70,000	10	7,000
Czech Rep.	9,000	3	3,000
Bulgaria	20,000	10	2,000
Romania	12,000	90	133

Approximations derived from Pols' tables, PLBIR, 04/14

Data is incomplete and inconsistent, but ...

- Actual fines also vary wildly between EU countries
- Positive aspects of EU fines practice:
 - Some EU fines are significant (except for largest companies).
 - Maximum fines are increasing by legislation.
 - Statutory maximum fines can be applied multiple times (eg total fine of €1million in Greece against Google)
 - Significant DPA fines are becoming more frequent (eg UK).
- Eg Bird & Bird case studies for 2013
 - Czech Republic – Ttl €69,400 for 4 cases (av €17,350) (Bird & Bird) – not €3,000 as Pols says.
 - Italy – Ttl over €1 million (Bird & Bird)

Fleabites and business risks

- Nevertheless, Pols is probably right to conclude:

‘When Google decided to bundle the privacy policies of all their products into one, their lawyers probably knew that they would face an outcry in Europe. They probably went through a rapid risk analysis, summing up the [maximum fines from 12 EU countries she considered]. Counting loosely, adding legal expenses, the amount **doesn’t add up to more than 3 million euros**. In the light of Big Data promises and seen from Google’s perspective, wouldn’t you also recommend they intertwine the data collected through their services?’

 - Aurelie Pols, *Privacy Laws & Business International Report*, 04/14
- Will there be € 1 Billion fines to cause Google etc to think again? ...

EU proposals for new Regulation

- One scale of fines will apply in all EU countries
 - There will be a Regulation, despite UK wishes for a Directive
- The formula is not yet finalised but will probably be:
 - Fines up to 2% of annual global turnover (EU Commission - or 5% says EU Parliament), or €100 million (whichever is greater).
 - Businesses with a compliance certificate from a DPA would be immune from such fines except where breach intentional or sufficiently negligent.
 - Will apply to businesses outside EU making profits in EU
 - ✦ already so – see ‘establishment’ rule in Google Spanish case

Fines in Asia-Pacific jurisdictions

Jurisdiction	Admin Max US\$	Admin actual	Court Max US\$	Court Actual
Australia	None	N/A	\$1,590,000	N/A
China (PRC)	\$82,500	Not known	None	N/A
Hong Kong SAR	None	N/A	\$13,000	\$900
Japan	None	N/A	\$3,000	None
India	None	N/A	\$8,000	None
Korea	\$50,000	Not known	\$100,000	N/A
Macau SAR	\$10,000	Not known	None	
Malaysia	None	N/A	\$100,000	N/A
Philippines	None	N/A	\$45,500	N/A
Taiwan	\$15,000	Not known	\$33,000	\$3,000
Singapore	\$790,000	N/A	\$80,000	N/A
Vietnam	None	N/A	None	N/A

N/A (not applicable) = either because no power, or because the Act is not in force.

- Every jurisdiction (except Vietnam) gives a DPA, Ministry or Court power to fine.
- Australia, Singapore, Korea and Malaysia have US\$100K+ fines in some case.
- Fines are known to occur (except in Japan) but amounts are often not known.
- There will be pressure to raise these fine levels when the EU Regulation proceeds.

Compensation & mediation payments – EU

- Directive A 23 requires compensatory damages to be available
- In most EU Member States 'judicial authorities can award damages' (FRA).
 - Whether this covers non-pecuniary damage varies. Austria sets a maximum €20,000 for non-pecuniary damages.
 - FRA notes actual awards of 'ranging from €300 to €800 in Finland, up to €600 in Sweden, and from €1,200 to €12,000 in Poland'. (No detailed survey otherwise available.)
- EU DPAs cannot usually award compensation.
 - If complaints are settled by DPA mediation, compensation may result but statistics are hard to find. Possibly significant.

Compensation & mediation – Asia-Pacific

- Most Asian data privacy laws include a right to seek compensation through court actions
 - Hong Kong, Macau, Singapore, South Korea, Taiwan, China, Vietnam and possibly India.
 - The Civil Code in some civil law jurisdictions (Macau, Taiwan, South Korea) may create equivalent rights for breach of Act. Vietnam's e-commerce and consumer laws do similarly.
 - The Philippines' Act only provides for compensation actions when an offence has occurred (Civil Code actions also possible).
 - No common law jurisdictions have a tort of invasion of privacy.
- Only Japan and Malaysia have no statutory rights to seek compensation from a court for breaches.

Compensation & mediation – Asia-Pacific (2)

- **In Asia-Pacific DPAs cannot award compensation**
 - Australia is the exception – DPA can award compensation, but has only done so a half-dozen times in 25 years.
 - Korea's PIDMC (Mediation Committees) arbitrate small complaints against businesses, and settled 76% (242 in 2009-12) for compensation, usually US\$1-10K. Others settle before arbitration.
- **Most DPAs mediate compensation settlements**
 - DPAs do so, even if they have not explicit powers to do so
 - Ministries do not do so, so “no DPA = no compensation”.
 - Statistics on settlements are difficult to find.
 - Australia's DPA's practice (5% of complaints) can be inferred:
 - ✦ 2008/9: A\$290K in 75 settlements, averaging \$4,407
 - ✦ 2011/12: A\$120K in 56 settlements, averaging \$2,134

Conclusions

- Financial payments (fines and compensation) are commonplace in data privacy laws in both EU and Asia-Pacific
- Penalties are too low to deter major privacy-invading practices in Asia-Pacific, but may become sufficient in EU
- Compensation is an accepted right in almost all Asia-Pacific laws, an Asian standard as well as in the EU
- Laws require serious criminal penalties to be of international standard, both in EU and Asia-Pacific

Further work

- Find more systematic studies from Europe & USA
 - See if systematic Latin American studies exist
- Use the *International Privacy Law Library* to find more systematic data on actual penalties imposed by some DPAs (eg USA, UK, NZ)
 - <http://www.worldlii.org/int/special/privacy/>
 - Constructing effective searches can be complex
- Use this data to construct a benchmark for what is currently 'normal' for both notional & actual penalties
 - Shed light on the question 'are privacy laws actually enforced?'
 - Enable a more accurate debate about *real* 'international standards', because international agreements don't assist
 - Use this data to assist submissions etc when laws are being reformed (eg Japan)


[\[Home\]](#) [\[Databases\]](#) [\[Search\]](#) [\[WorldLII\]](#) [\[Feedback\]](#) [\[Help\]](#)

[\[Advanced Search\]](#) [\[Search Help\]](#) [\[Results Interface Help\]](#)

WorldLII Databases - Documents found: 338 for (compensation not (" worker compensation" or " employee compensation"))

[Collapse Listing](#)

1. Federal Privacy Commissioner of Australia Case Notes: 81 documents	Da: Clic
2. Federal Privacy Commissioner of Australia Complaint Determinations: 7 documents	
3. New South Wales Privacy Commissioner Cases: 5 documents	
4. Office of the Victorian Privacy Commissioner Case Notes: 10 documents	
5. Australian Privacy Case Summaries: 28 documents	
6. Office of the Privacy Commissioner for Personal Data Administrative Appeals Board Decisions: 4 documents	
7. Office of the Privacy Commissioner for Personal Data Complaint Case Notes: 9 documents	
8. European Commission Article 29 Working Party Opinions and Recommendations: 44 documents	
9. Irish Data Protection Commission Case Studies: 1 document	
10. Irish Information Commissioner's Decisions: 19 documents	
11. Korean Personal Information Dispute Mediation Committee Cases: 18 documents	
12. Macau Office for Personal Data Protection Case Notes: 7 documents	
13. New Zealand Privacy Commissioner Case Notes: 36 documents	
14. Information Commissioner's Office: 36 documents	
15. United Kingdom Information Tribunal including the National Security Appeals Panel: 33 documents	

'By database' display of search of DPA cases concerning compensation

References

- Fundamental Rights Agency *Access to data protection remedies in EU Member States*, 2013
- Fundamental Rights Agency *Ad hoc information reports on access to data protection remedies* 2013
- Bird & Bird *International data protection enforcement bulletin*, October 2013 and April 2014
- Aurelie Pols 'Spain is responsible for 80% of European Data Protection Fines (2014) 128 *Privacy Laws & Business International Report*, pgs 22-24.
- Graham Greenleaf *Asian Data Privacy Laws* (OUP, forthcoming October 2014), Chapter 18.
- World Legal Information Institute *International Privacy Law Library* <http://www.worldlii.org/int/special/privacy/>