Lessons for Japan from the Upcoming EU Data Protection Reforms : Beyond the Gold Standard?

Lilian Edwards

Professor of E-Governance, Strathclyde Law School

Japan, November 2012

Lilian.edwards@strath.ac.uk

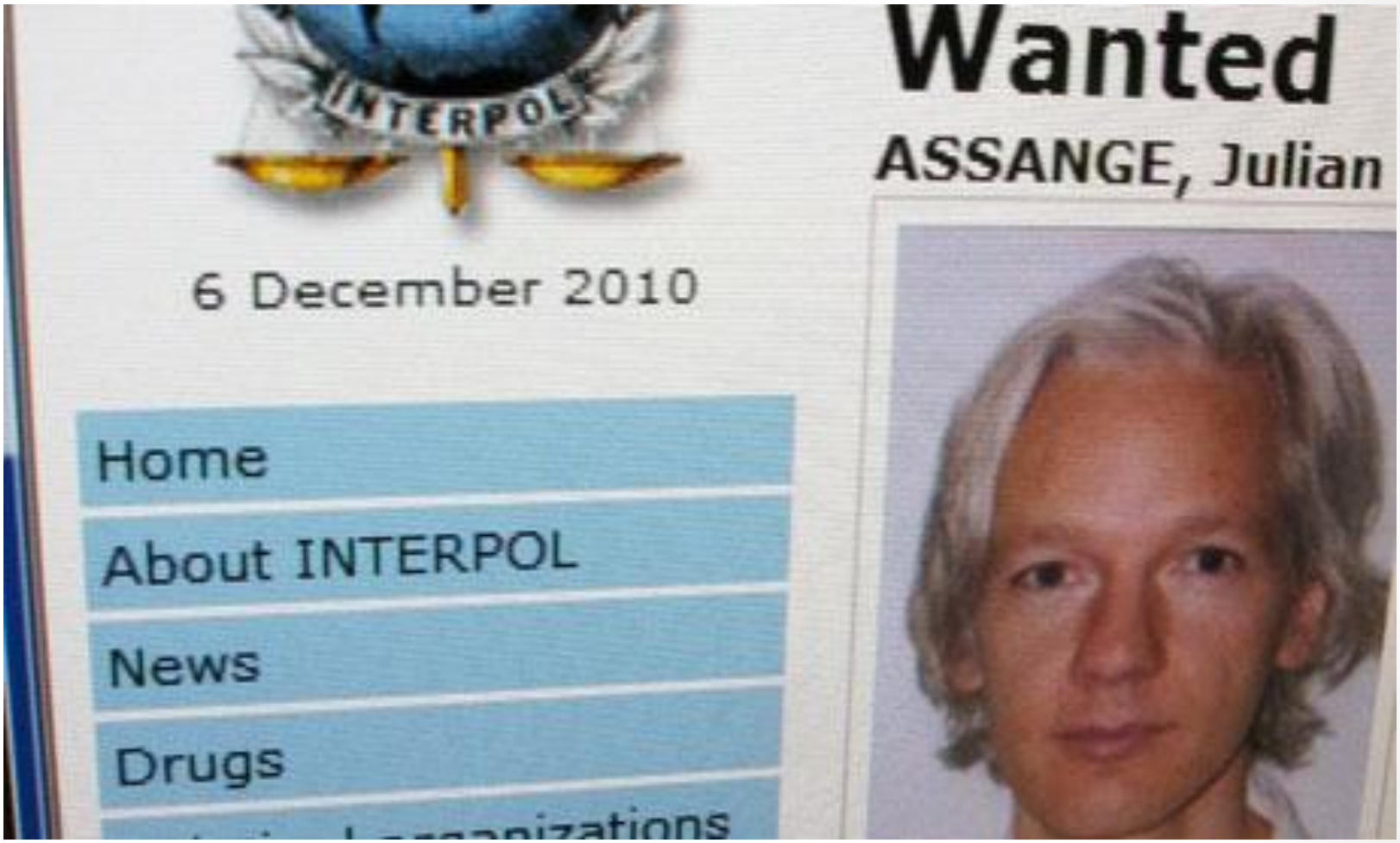
Pangloss blog: http://blogscript.blogspot.com

Twitter: @lilianedwards

When did privacy and personal data become headlines?

C4, May 2010

Scotland!
22 May
2011


INTERPOL
Wanted
ASSANGE, Julian
6 December 2010
Home
About INTERPOL
News
Drugs

Drivers & conflicts for EC DP reform..

- **Economic**
- "..That's why I say that data is the new oil for the digital age. How many other ways could stimulate a market worth 70 billion euros a year, without spending big budgets? Not many, I'd say." *N Kroes, March 2012*

- **Trust**
- "Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities… Building trust in the online environment is key to economic development. Personal data protection therefore plays a central role in the Digital Agenda for Europe.." *Draft DPR introduction, Jan 2012*

- **Security and policing**: profiling agendas

Users, trust online and personal data

Attitudes towards data protection

- **60%** of Europeans who use the internet **(40% of all EU citizens) shop or sell things** online and use social networking sites.
- People disclose personal data, including **biographical information** (almost 90%), **social information** (almost 50%) and **sensitive information** (almost 10%) on sites (notably social networks)
- **70%** said they were concerned about how companies **use this data** and they think that they have **only partial**, if any, control of their own data.
- **74%** want to give their **specific consent** before their data is collected and processed on the Internet.

Reform of the DPD? Nov 2010 consultation -> Jan 2012 draft General DP Regulation

- Main issues
  - *Integrate* rules on DP police & LEAs sector with existing rules for "civilian" data controllers? (in eventual draft, separate general Regulation and policing Directive))
  - Address *globalisation* better – personal data flows *out of* EU
  - Clarify rules on *jurisdiction, applicable law* and DP (issue for non-EU data controllers, esp multinationals, Google etc
  - Improve *harmonisation within* EU (binding interpretation by Art 29 WP?)
  - *Strengthen data subject's rights* : enhancing control over PD eg, online subject access, explicit consent, "right to forget"
  - *Cut costs, red tap*e for data controllers – multinationals only to be regulated by 1 EC DPA - 2.3 bn Euros savings for EU industry - quid pro quo?
  - -> Make DCs more *accountable*, eg, must have a CPO; audit trails of processing; "privacy by design" (?)

Issues – 1 - User rights & the Right to Forget

- Right to forget – new art 17, recitals 45-46
- Aim – to provide control over data disclosed on SNSs? To control private & public profiling?
- Right to "*obtain from the DC the erasure of [their] personal data*" but also to have no further "*dissemination*" of it - especially re data exposed when a child
- Would a host have to go track down everywhere on the web the data was held or linked to and delete it? Responsibilities of search engines? See new art 17(2)
  - Balance with freedom of expression? With proof?
  - Balance with "historical, statistical and scientific research"? (cf Wikipedia on criminal convictions)

The Oxford philosophy student, 2007

“Foggy thinking about the right to oblivion”

- Peter Fleischer, Google, March 9 2011
- “More and more, *privacy is being used to justify censorship*. In a sense, privacy depends on keeping some things private, in other words, hidden, restricted, or deleted. And in a world where ever more content is coming online, and where ever more content is find-able and share-able, it's also natural that the privacy counter-movement is gathering strength. *Privacy is the new black in censorship fashions*. It used to be that people would invoke libel or defamation to justify censorship about things that hurt their reputations. But invoking libel or defamation requires that the speech not be true. *Privacy is far more elastic, because privacy claims can be made on speech that is true*.”
- Do we want the “PR” society? Cf UK super injunctions..
- If aim to restrict profiling - main concern may be mundane profile data – not big historical journalism?

More new user rights..

- Right to *access your data electronically* if it is held electronically – ie "online subject access"
- Right to *data portability,* - "*in an electronic format which is commonly used*" ? - > competition in SNS market?
- *Right to object* not just to use of data for direct marketing but to decision solely based on automated *profiling* inc. by "location, health, personal preferences, reliability or behaviour". Note this right does NOT apply to police/LEA profiling.
- *Consent* as grounds for lawful processing must always be explicit (??)
- *Privacy policies* to be more transparent

Issue 2: The Cloud and globalised data flows

Issues – 2; the Cloud and globalised data flows

- EU discourse since 1995 DPD has been that where EU personal data flows outside EU, it should receive "adequate" protection
- And that non EU businesses in EU should respect EU DP law
- Problematic – US safe harbor etc - exacerbated by the Cloud and fact that is mainly US centred
- Not just B2B services as with out-sourcing – but B2C (eg Google Docs, Gmail, Facebook)
- Issues:
  - When/how can personal data be *exported* from EU ?
  - When is EU law applied to data controllers doing business i*n* EU?
  - What should *division* of responsibility for personal data between data processors and data controllers
  - Which category is a *cloud provider in*? Issue since SWIFT case – Art 29 WP Opinion 10/2006

Reform?

- **Data exports**:
- "Adequacy" process clearly not working, largely replaced by standard contractual clauses
- Binding Corporate Rules – a kind of charter for entire multinational company – to become easier. Non US safe harbors?
- Nothing much done about land grabs of data in cloud for national security purposes eg US Patriot Act
- **Applicable law**:
- Current art 4 binds cos with "establishment" in EU or if none, using "equipment" in EU – v widely defined by A29 WP eg cookies.
- New proposal would replace latter with test based on whether goods & services *offered to* EU data subjects or if they are "*monitored*".
- Interpn? For both, enforcement**? Recital 21.**
- **Defining data controllers and processors**: Attempts to redistribute more responsibility to data processor from data controller, including that a processor who processes data *beyond* the controller's instructions is to be considered as a *joint controller*
- Industry fearful of need to renegotiate all delegation contracts with cloud providers.

Issues – 3 - enforcement

- Continual problems of resourcing DP Authorities independent of state and industry
- Lack of technical knowledge, political will ("business friendliness"), extraterritoriality of key DCs.
- Are bigger fines the whole answer?
- Big headline figures – harmonised penalties of *up to €1 million or up to 2% of the global annual turnover* of a company.
- But *not* disqualification as director, or jail.
  - Cf UK - – now max £500,000 fine, jail sentences still not implemented. In 2011, 7 cos fined – average £77K.
- Will EC DPAs have the resources to *go after* these big enforcement actions?
- Will multinationals arrange to have a "compliant" DPA as their sole regulator – UK/Ireland – race to the bottom cf "corporation tax" opportunity? New Art 51 – "main establishment".

Security breach notification

- *Mandatory security breach notification* proposed (new arts 30-32).
- Already introduced for telcos/ISPs in PEC Dir art 17(1)
- Aim is naming and shaming; also notice to public enables them to get remedies, take protective steps
- Details are controversial: what triggers (no "serious breach" threshold? ; how long to fix before notifying (24 hours?!) ; who to notify? – police/DPA/data subjects affected? DPREg prioritises DPA.
  - No notification if data was encrypted (?)
  - Not to "public as a whole"
- Breach ennui? US experience not that helpful; Jp?
- What can victims do even if notified? Depends on other EU initiatives re collective court action..

Will these reforms produce better data privacy? The cookies experience.

- "This is where the real problem seemed to come for me. All the businesses want to know how to comply with regulations – but they don't seem to understand the real point. These kinds of regulations aren't really supposed to be about ticking boxes, or finding the right words to describe your activities in order to comply with the technical details of the relevant laws. [A lawyer] gave a very revealing and detailed picture of how he had to navigate some of his multi-national clients through the complexities of the different international regulations concerning data protection – but he seemed not to want to offer one particular piece of advice. He didn't seem to want to tell his clients that they might well have to change what they do – or perhaps even decide not to do it.

The purpose of the very existence of these regulations are to make businesses (and governments) *change what they do*, or at least how they do it."

Paul Bernal's blog, March 8 2012. (paulbernal.wordpress.com)