Submission to balance of competence review of information rights

Caspar Bowden is an independent advocate for information privacy rights, and public understanding of privacy research in computer science. He is a specialist in EU Data Protection, European and US surveillance law, PET research, identity management, and information ethics. He is author of 2013 EU Parliament inquiry briefing[1] on the US FISA law, and co-authored the 2012 Note on privacy and Cloud computing[2] (which anticipated the infringements to EU data sovereignty disclosed by Edward Snowden). For nine years he was Chief Privacy Adviser for Microsoft for forty countries, and previously co-founded and was first director of the Foundation for Information Policy Research (www.fipr.org). He was an expert adviser for UK Parliamentary legislation, author of the RIP Act Information Centre (**www.fipr.org/rip/**), and co-organized six public conferences on encryption, data retention, and interception policy. He has previous careers in financial engineering and risk management, and software engineering (systems, 3D games, applied cryptography), including work with Goldman Sachs, Microsoft Consulting Services, Acorn, Research Machines, and IBM. He founded the Award for Outstanding Research in Privacy Enhancing Technologies, is a fellow of the British Computer Society, and a member of the advisory bodies of several civil society associations.

1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

Recital 26 or the EU Directive 95/46 defines the concept of anonymous data, as (likely reasonably) not re-identifiable by the Controller "or by any other person". The UK never gave effect to this recital in the DPA 1998. It is widely believed in Brussels, that the UK exacted as a price to allow the Directive to proceed (in secret Trialogue in 1995), the dilution of a corresponding Article in the original draft into a Recital (which are not mandatory to transpose).

The subsequent legislative history has been both confusing and contradictory both at UK level (Durant, DoH vs IC 1430), and at EU level (WP29 Opinion 136). The effect has been that for nearly 20 years the UK has followed a policy of "we will call pseudonymous data 'anonymous' if we want to". This is inconsistent with the ordinary meaning of the word anonymity, and courts have struggled to develop a coherent meaning for the central concept of personal data without ever isolating the original problem – that the "variable geometry" outcome of Rec.26, by not obligating a coherent interpretation of anonymity on Member States, was a booby-trap in the key term of art, which sabotaged the consistent application of the Directive to the Internet.

There is now a manifest contradiction between the 2012 ICO Code of Practice on Anonymisation, which in four places declares pseudonymisation is a valid form of anonymisation, and the new (WP29 Opinion 216 on Anonymisation) which four times stresses it is not. The latter is the correct position in computer science, the former is essentially founded on an oxymoron.

The UK public has been disadvantaged in several ways:

---

1 *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights*, 16-09-2013, Caspar Bowden, intr. Didier Bigo http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

2 *Fighting Cyber Crime and Protecting Privacy in the Cloud*, 15-10-2012, Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, Amandine Scherrer http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf

a) the treatment of pseudonymous data as anonymous has deprived individuals of their rights to access/delete/correct such personal data, not merely under the DPA but via the evasive limitations on the scope of personal data in the US/EU Safe Harbour Agreement, under which the ICO disowns any enforcement duties.

b) the UK (and IE) have engaged in a large-scale regulatory arbitrage versus the rest of the EU states which gave effect to Recital 26 in law and policy. Superficially, this may appear to have benefited the UK, but it has prevented the UK (and the rest of EU internal market) from developing internationally competitive Internet industries. The effect of scientifically incompatible definitions of anonymity, as a core concept underlying 28 national transpositions, has been regulatory paralysis and legal uncertainty since 1995. In direct consequence, business models based on effective privacy technology and/or subscriptions have been subjected to unfair competition from “free” US services which could exploit data in ways unlawful under the Directive (and regulatory action to curb this has been extraordinarily slow).

c) A counter-factual history of UK Internet policy might have seen the development of global scale software industries, with strong EU market share, leveraging the UK's traditional strengths and pioneering expertise in computer science. Instead the UK Internet economy comprises service industries, built on US commercial platforms, which harvest the major share of value - ironically (but not coincidentally) through the deregulated processing of pseudonymous click-stream data in online advertising.

d) the UK long-standing policy of *de minimis* privacy protection, and Recital.26 in particular, has also impoverished the human rights of the UK public through macro-economic effects on market structures. Centralised identity systems and web services have become *de facto*, in the private and public sector, as opposed to "user-centric" models such as those engineered in the PRIME and PrimeLife EU research projects. Because of the fictitious notion that Data Protection legislation must be "technology-neutral", the ICO has been able to equivocate that no technical architecture is categorically preferable to “organisational” methods of protecting privacy, which are illusory and ineffectual on an Internet scale. Yet Privacy Enhancing Technology intrinsically protects privacy better than ordinary systems – it is the raison d'etre of an entire field of computer science developed since the Directive, using cryptographically sophisticated privacy-risk minimization (and these methods are to be distinguished from true anonymisation). Because of the original sin of omission of Recital 26, none of this work has been appreciated or taken up in the UK.

2. What evidence is there that the EU’s competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals’ data protection rights and the pursuit of economic growth?

The question is mis-posed as a "balance" between individual rights and economic growth, but this framing does not admit that the nullification of data protection rights caused by the Recital 26 situation has warped the entire European Internet information economy and architecture, by permitting the “regulatory arbitrage” referred to above. In direct consequence, over two decades the UK and the EU have become strategically dependent on the US for Cloud software services and infrastructure, advertising data flows, and much of e-commerce. Moreover, the highest external risks of privacy harm in pseudonymous data arise from traffic analysis of flows, which may be encrypted, yet re-identifiable. UK and EU information security policy, so far as the general public is concerned, has been built on

foundations of sand, which left foreign intelligences agencies out of the threat model. The disruption to the internal market caused by loophole of Recital 26 has rippled through cyber-security, and post-Snowden has left a chilling effect on free expression rights.

The economic opportunity cost becomes apparent when one considers that Airbus now has a 50% global market share with Boeing. Cloud computing is already an industry of comparable global strategic significance, yet the EU has almost no technological capacity in depth, and the EU's “Cloud strategy” amounts to a marketing campaign for US Cloud services. The laxity of UK data protection and concomitant distortion of the EU internal market, not only inflicted privacy harms to its own citizens and those of the EU, but was a central factor in a European lack of competitiveness to develop major scale Internet industries, either from entrepreneurial start-ups or innovations by telco companies. Lacking clear Data Protection design requirements, the internal market was badly fragmented. The cost of not integrating European resources and policies has been the forfeiture of the major economic rewards and strategic control of the entire sector.

It is therefore essential that the EU proceeds with a Regulation not a Directive, and that changes the UK is promoting in Council to exempt pseudonymised data are rejected, both for the benefit of UK citizens and a cohesive future as a Member State.

Strong economic performance is possible in highly authoritarian societies, but UK policy has failed to recognize that the long-term cause of its surveillance society, is the marginalization of privacy rights pursued since the Lindop report of 1978, as part of the permanent policy of the civil service, because respect for privacy was presumed to be incompatible with administrative and economic benefits.

Re-shaping UK policy around genuinely privacy-protective user-centric designs is fundamental to restoring a sense of autonomy to private life and authentic free expression to public life. A succession of data leak scandals even before Snowden has led to a correct public understanding that their data is not safe under the chronically weak UK data protection regime.

Posing the policy "balance" as between individual rights and economic exploitation of data is a abdication of long-term policy planning to adopt privacy technology which could protect rights and sustain a flourishing economy. There is now a 20-old literature of the computer science and economics of privacy, of which the UK policy apparatus still seems oblivious. When the author made an FOI request for what the Information Rights department of MoJ knew about the computer science of privacy a few years ago, the answer was absolutely nothing. Policy-making in information privacy in MoJ has been based on a vacuum of scientific knowledge.

3. What evidence is there that the EU’s competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

Social network data is of an intermediate character between public and confidential personal data. However the appropriate integration of social network data into the DP framework has been performed in strong work from WP29 and ENISA.

The principal failing of the Directive in addressing new technology and the scale of flows is

that it is locked into various false conceptual models of privacy risk, as if in a parallel but fallacious "fantasy computer science" universe. For example, it is obvious and true that privacy risk increases monotonically every time data is copied to a new machine, especially if in another organization, and especially to another jurisdiction. Moreover one must distinguish risk (as something quantifiable) from uncertainty about consequences which cannot be estimated by members of the public when they use interconnected transnational systems. Yet data protection law says that if the right legal boxes are ticked, then disclosures and transfers can be made again and again, without regard to cumulative risk. This technical solecism has now reached a pitch of absurd refinement in the notion of adding "sub-processors" recursively into a Cloud Computing service contract, allowing the risk from indefinite complexification of data-flows to be ignored. There are some similarities with neglect if spiralling macro-risk before the financial collapse of 2008.

This para-scientific legal engineering may be neat, but it has no relation to the reality of architectures which can protect against attacks long understood in computer science, and validated by Edward Snowden. The legal models for "commercial" transborder data-flow are irreparable precisely because their function was to magic away concerns over mass-surveillance (from the time of the ECHELON affair 1999-2001). Practically speaking, the mechanisms of BCRs, model contracts and Safe Harbour should be shut down strategically (with a view to EU negotiating advantage), and replaced with a quality-controlled and unified European Privacy Seal, enhanced from the proposal in the LIBE draft of the GDPR. Not all services will be able to obtain a seal, if they cannot isolate themselves technically and legally from known risky jurisdictions. The transition may engender a measure of market disruption.

The other major incoherence created at a conceptual level in European data protection is failure to distinguish between the operations of storage and computing, both subsumed in the term data "processing". This unification might seem attractive and without controversy, but was made long before the availability of strong and standardized cryptography. The risks of remotely storing data, properly encrypted under the user's control, compared to transferring "plain-text" data to another party (even if encrypted en route), is simply incommensurable - yet they are not distinguished by the conceptual framework of DP. However, it must not be assumed that even data encrypted under apparent control of the user is risk-free - Edward Snowden has demonstrated that transmitting supposedly encrypted data is much riskier than not exposing the data at all.

To pile on the absurdity, there appears to be systematic confusion amongst policy-makers that Cloud computing (as opposed to mere remote storage of data) can be protected by encryption. This is simply untrue. Commercial models of Cloud computing depend on working with decrypted data, thus exclusive custody to the key is forfeit implicitly. Most services have “key recovery” architectures to decrypt user data trivially, and for those that do not, keys and/or plaintext are easily recovered from the remote computer's memory by forensic means.

To deal with post-Snowden risks, the EU should:

a) criminalize acquiescence of EU Controllers/Processors to direct (secret) demands from foreign entities
b) criminalize planting of back-doors or collaboration in weakening privacy or security by manufacturers
c) insist on a selection process for DP Commissioner (DPC) which gives a short-list of at least 6 to a national Parliament for final decision, and prohibit appointment by the

Executive.

d) require DPCs and their DPA staff to have contemporary technical competence
e) establish a central EU prosecution unit for major cases of transnational DP enforcement, with sufficient legal and technical staff, accepting referrals from national DPAs or the DP Board.
f) the DP Board should establish a computer science committee, including civil society members, to be consulted on privacy technology innovation and standardisation
g) eliminate references to pseudonymisation and pseudonymous data in the GDPR, and follow the analysis of WP216.

4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

The advantage of the Regulation is that this would be a real Data Protection and privacy law, rather than the simulacrum of the Data Protection Act 1998 which is designed to give *de minimis* protection. The Regulation curtails many unfair or unwise limitations on data subjects rights, particularly:

- by providing an express right to data portability, since frequent access can be beneficial to user security, eliminating ambiguities about the interpretation of "permanent form"
- since the Regulation has direct effect, an end to the UK's "pseudonymity arbitrage" (i.e. the omission of transposition of Recital 26) which endangers the privacy of UK citizens (and EU citizens whose data flows to or via the UK)

Although for the above reasons a Regulation is in every way preferable to another Directive (which would be prone to the same crippling divergences), on the other hand the Regulation is extremely bureaucratic and could be simplified if the concepts were clarified across disparate sections. The structural complexification of Regulation arises from special-case derogations invented to placate different policy constituencies, which have now grow into a thicket of disparate mechanisms for compliance, with very little *prima facie* prospect of success.

Some of the chief deficiencies of the Regulation (across Council and LIBE drafts) remain:

a) model contracts & BCRs are never litigated (reputation damage and legal uncertainty outweigh gains), leading to an opaque market in data processor reliability
b) Codes of Practice are allowed as a compliance vehicle, including for Third Country country transfers, equating “self-certification” with independent assessment for “adherence”
c) for a critique of Safe Harbour, I refer to my recent evidence to the House of Lords enhanced scrutiny committee.
d) BCRs-for-processors, concocted for Cloud computing, were manufactured with FISA-shaped loopholes built in, despite clear warnings given to WP29 prior to Snowden
e) "legitimate interests" remains entirely vague, with the potential to generate a microcosm of administrative jurisprudence mirroring wider controversies in DP.
f) various uncertain formulae for exceptions such as "important public interest" lack any explanation of the type of circumstances for which they are intended
g) the implausible "consistency" machinery of the DP Board, still without legal personality to make binding rulings at EU level

h) many Commission delegated powers to specify technical matters like Data Protection By Design, without transparency or conspicuous expertise to be able to do so

However, judging from the footnotes in Council positions, the MoJ s invariably in favour of weakening privacy protection across the board, and so presumably will take opposing positions on most of the above issues. Indeed it appears the UK has led the Council in a direction of a “risk-based approach” entirely based on the spurious and obsolete notion that pseudonymized data is intrinsically “less risky” for privacy. If the EU unwisely follows this approach, the net effect will be a vast increase in total privacy risk, as huge new tranches of pseudonymous data will be exported from the EU, outside of effective regulatory control and trivially easy to re-identify. The UK's “care.data” fiasco could not have happened in many other EU countries, because the proposition that pseudonymised health data is “anonymous” would have been legally laughable.

5. What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

I make regular use of the Access to Documents procedure, which is satisfactory, but in some respects over-bureaucratic. For example I am pursuing a complaint that they require (without good reason) a postal address even if the documents are to be delivered by email, ostensibly so that a registered delivery receipt of acknowledgement of every decision can be obtained. This seems both disproportionate and excessive data collection, and profligate compared to the theoretically low cost of purely electronic fulfilment.

It is beneficial that the EDPS has jurisdiction over maladministration connected with the intersection of Data Protection with Access to Documents.

6. How would UK citizens’ ability to access official information benefit from more or less EU action?

The Freedom of Information Act's exemptions are far too broad, especially in respect of those for :

- "free and frank advice, or would prejudice the effective conduct of public affairs"
- international relations
- national security (although “national security” *per se* is carved out from TFEU, there is substantial intersection with EU affairs on Snowden matters)

Other countries manage with substantially less broad exemptions. Further EU harmonization of national FOI laws, and standardisation of online request and fulfilment, would be beneficial provided this levelled up government transparency, not levelled down.

A general problem is that departments “game” the cost limits. In other words if there is a query they do not want to answer, and they know perfectly well what the point of the request is, they will start by looking in the “wrong place” or otherwise unintelligently in an attempt to exhaust the cost limit (usually by means of a bogus estimate of time rather than actually claiming to do the work). I have seen this done in obvious bad faith, repeatedly, by the Home Office, the FCO and by the ICO itself, but of course it would be extremely difficult to prove, and even if it were proved, departments do not seem to fear any sanction for such obstreperousness. FOI seems to complied with only with the reluctance of comfortable burghers of a fortified town adjusting to life under a long term siege.

7. How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?

There is a particular problem regarding FOI (or subject access requests) sent to and about the supervisory body (the ICO) itself. In the author's experience of several such requests (notably on the policy history of Recital 26), the process was a travesty of impartiality, with the ICO sometimes gaming the cost limits in manifestly evasive responses. As part of any EU harmonization, a provision should be made for an independent appeal of decisions the ICO makes about itself, with an investigatory capacity. This measure might not be necessary if the ICO were dissolved and a new supervisory body with an entirely new culture was formed, which in the author's view is otherwise long overdue. Cconsider the unresolved controversy surrounding a former IC's alleged suppression of prosecuting phone-hacking where the evidence led in the Levison inquiry – to Fleet Street (“they are too big for us”).

More generally regarding other information rights, the UK has pursued "intellectual-property-maximalist" positions, at least within the EU, only recently legalizing time-shifting and parody [although even the latter has been inexplicably subject to delay at the time of writing].

Special measures are needed to prevent patent abuse when fundamental techniques are effectively taken off the market (and away from disruptive competitors), because an invention has social utility but little commercial utility. A good example are "Privacy Enhancing Technologies" of various kinds, which although extensively researched and developed in EU projects (like PRIME and PrimeLife) have no prospect of deployments unless they are recognized by regulators as paradigmatic examples of “Data Protection by Design” in the new Regulation. The two main companies holding patents are IBM and Microsoft, and the larger business Big Data interests of both companies are against widespread deployment of PETs to the benefit of users' privacy. Neither company has made a serious commercial effort to deploy advanced PETs in the past 10 years.

8. Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

No, *pace* patents, which are not dealt with fully in this response, however the proposed EU Unitary patent can only be appealed within the new system created (rather than to an independent body), and seems increasingly prepared to grant software patents just a the US is finally reforming and beginning to reverse their perverse effects.

Unless the phrase "indirectly to expand the competence of the EU" could be related to the situation already alluded to above, namely that the UK has effectively operated a definition of personal data excluding "indirectly identifiable" data (e.g. via a pseudonym) from the scope of what it recognizes as "personal data". In which case, it would not be correct to say this an expansion of competence, but an elimination of the UK's evasion of competence, long overdue to rectify a great detriment to UK and EU citizens' data protection rights.

9. What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?

The rights to privacy and Data Protection are incorporated as separate rights into the EU Charter, but derive from the UK accession to ECHR and CoE Convention 108. It is well-known that the UK does not really have an "opt-out" from the Charter, in so far as such rights as are already well-established by CJEU and ECtHR jurisprudence.

Moreover the effects can be inhibitory as well as prescriptive, for example the decision of CJEU to declare the Data Retention Directive invalid, because of a specific deprecation of indiscriminate (blanket) retention (paras.58/59), also implies it would be unlawful to replace the DRD with a national blanket retention law, because the national exemption dating from the 2002 e-Privacy Directive Art.15 extensively (and properly) cross-references a requirement for such national derogations to be compatible with human rights.

Actual UK practice and law had already diverged to the far extreme of lip-service towards the principles of data protection, and would do so further without these EU jurisprudential interventions. Without the cover of EU Data Protection, the UK would likely become recognized as a privacy pariah, and the Commission might well not grant a finding of adequacy (or EEA sufficiency) to the DPA regime, if the UK left the EU.

10. What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?

See the attached report prepared for the European Parliament (Oct 2013)

11. Is there any other evidence in the field of EU Information Rights that is relevant to this review?

Yes, much other evidence, on request or for oral hearing. This response is not fully referenced because the marginal effort to do so is unlikely to be worthwhile in terms of incremental policy impact, but references on any point will be provided on request.

Caspar Bowden

June 30th 2014