The Economics of Data Privacy: Should we place a dollar value on personal autonomy and dignity?

Blair Stewart

Assistant Commissioner, Office of the Privacy Commissioner, New Zealand

Blair.Stewart@privacy.org.nz

Abstract: Economic interests lie behind the development of many international data privacy standards. Such standards are premised upon promoting the economic value in free flow of information by adequately protecting privacy: a process of reconciling competing interests rather than balancing them. It is difficult to strike a balance since a monetary value can usually be placed on economic costs but not the privacy benefits. Data protection and privacy commissioners are well placed to observe the costs that data privacy regulation can impose and recognise the benefits that compliance can bring. While it is not their task to decide how much society is willing to pay for their privacy, commissioners do have responsibility for the costs they impose through their own actions. Commissioners should strive for cost effective regulation, but must take care to see that privacy is not undervalued merely because a monetary value cannot always be assigned to its observance.

[E]veryone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.

- Posner, "The Right of Privacy", 1978[1]

The economic argument can be taken too far. Certain values, such as human life and liberty, cannot be totally subjugated to the tyranny of cost accounting.
- Australian Law Reform Commission, *Privacy*, 1983[2]

1 Introduction

Economic questions have been central considerations in the development of many international data privacy instruments.[3] The European Union Data Protection Directive[4] is, for instance, part of the grand harmonisation strategy to achieve the economic benefits of a "Europe without frontiers". Similarly, the influential OECD Guidelines[5] explicitly recognise that although countries have a common interest in protecting privacy, there is a real risk that uncoordinated domestic legislation may hinder transborder data flows that can contribute to economic development. In much data privacy discourse there is a constant refrain that interests in privacy are not absolute. Rather, they must be weighed, with complementary and associated interests, against competing public and private interests.

---

1 R A Posner, "The right of Privacy" 12 *Georgia Law Review* 393 (1978)

2 Law Reform Commission, *Privacy*, Report No 22, Australia, 1983, paragraph 77.

3 "Data privacy", used throughout this paper, may be taken as a synonym for "data protection" or "information privacy".

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

5 Recommendation of the Council of the Organisation for Economic Cooperation and Development concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

The importance of the economic questions, and the centrality of the commissioner to the operation of data privacy law, means that commissioners have a duty to be vigilant to seek to ensure that data privacy is achieved in a cost effective manner. It is proper that the International Conference of Privacy and Data Protection Commissioners should continually return to the subject of the economics of data protection through sessions like this.

2 International approaches to the big economic questions

All of the data privacy commissioners represented at the international conference operate under a law that is compatible with the principal international instruments dealing with data protection and privacy.[6] I will briefly (and relatively superficially) characterise the approach of each of these instruments and then briefly mention some work in progress within the Asia Pacific.

Unsurprisingly, the Organisation for *Economic* Cooperative and Development had economic considerations in mind when it issued its 1980 Guidelines. The principal economic consideration, and its general approach, is neatly summed up in the brief recitals to the Guidelines which recognise:

> *that, although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;*
>
> *that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;*
>
> *that transborder flows of personal data contribute to economic and social development;*
>
> *that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows*.

The OECD, "determined to advance the free flow of information between member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations amongst member countries", recommended that member countries:

- take into account in their domestic legislation the privacy principles set out in the Guidelines; and
- endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data.

The OECD, having recognised the common interest in protecting privacy, identified a problem of diverging national data privacy legislation law and sought to facilitate the harmonisation of national legislation. The OECD only became involved in privacy issues because of the economic imperatives to have a compatible framework amongst member countries whereby privacy was effectively protected without unnecessarily interfering with, what would today be called, electronic commerce. Having embarked upon the task for economic reasons, the OECD produced a rational, effective and well expressed privacy framework document. Its analysis was ahead of its time in, for example, explicitly rejecting distinctions based upon "automated and non-automated data".[7] The OECD Guidelines do not subordinate privacy to economic considerations.

---

[6] Accreditation principles adopted by the 23rd International Conference of Data Protection Commissioners held in Paris, 24 - 26 September 2001, principle 3. The principal international instruments are the OECD Guidelines (1980), Council of Europe Convention No 108 (1981), UN Guidelines (1990) and the EU Directive (1995).

[7] OECD Guidelines, Explanatory Memorandum, paragraphs 34-38.

The next major international instrument was the Council of Europe Convention No 108 (1981).[8] The economic imperative is less marked in this Convention. It presents itself unapologetically as a human rights treaty. Its object and purpose is simply stated:

> *The purpose of this Convention is to secure in the territory of each party for each individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection').*[9]

The preamble does briefly state that it recognises that it "is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples".

The UN Guidelines (1990) add little to the general picture. They are clearly derivative of earlier work. Like the OECD Guidelines, they do not require data export controls and, although acknowledging that they can be legitimate, state that they should not be imposed unduly and only in so far as the protection as privacy demands.[10] It is perhaps unfortunate that the UN has not been more influential since, almost 15 years later, there is a large number of countries that have taken no action to provide legal protection to personal data in the way anticipated by international instruments. (Interestingly, these Guidelines have not been influential – or even been explicitly considered – in the development of APEC guidance although all Asia Pacific countries are of course members of the UN.)

The EU Directive (1995) is clearly motivated by economic considerations, particularly the need to harmonise data privacy laws within the Union. However, the Directive also stresses the importance of fundamental human rights. The economic impact of the EU Directive has been far greater than any other instrument given its legal effect within the EU and its approach towards third countries. The Directive's general approach is not unlike the other instruments and can be conveniently summarised from Article 1:

> 1. *In accordance with this Directive, member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*
>
> 2. *Member states shall neither restrict nor prohibit the free flow of personal data between member states for reasons connected with the protection afforded under paragraph 1.*

One of the fundamental economic objectives of the Directive was to enhance the free flow of data *within* the EU by removing barriers caused by internal borders. It is sometimes easy for commentators outside the EU to forget that fact when the principal effect for third countries is to highlight the barriers at what might be called the "outer border".

There is a certain consistency amongst these principal instruments. Each seeks to establish consistent rules to protect the recognised right to privacy in order to pre-empt incompatible national rules that would damage the economic benefits of a free flow of information.

The UN Guidelines, for whatever reason, have not been influential. Convention No 108 and the EU Directive only operate within Europe.[11] The OECD Guidelines covers only member countries. Accordingly, for many non-OECD countries there is no applicable instrument. Although occasionally mooted, an international treaty has not yet eventuated to fill the void. Accordingly, some international organisations have looked at developing data privacy instruments at the regional level, such as the Asia Pacific Economic Cooperation (APEC).[12] Economic considerations are central to APEC's interest and its work on data privacy is being handled out of its Electronic Commerce Steering Group. Its major driver is the wish to promote consumer trust in e-commerce. It is conceivable that the outcome of the APEC work will differ from other instruments mentioned since it does not explicitly acknowledge human rights within its frame of reference.

---

8 The Convention was updated by protocol in 2001 to encapsulate manual data – thereby aligning itself to the position the OECD reached 20 years before.

9 Council of Europe Convention No 108, Article 1.

10 United Nations Guidelines Concerning Computerised Personal Data Files, 1990, principle 9.

11 The Council of Europe Convention can be acceded to by non-member countries but none have chosen to do so.

12 In addition to the work of APEC, the Asia Pacific Telecommunity (APT) has, for example, also done preliminary work on an instrument for the Asia Pacific region.

To illustrate that the formulation of an appropriate balance to be struck between privacy and other economic interests is still open to debate, it may be noted that the draft APEC Privacy Framework proposes the following principle, not found in other international instruments:

> ***Preventing harm***
> *Recognising the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.*[13]

3 Costs imposed by Data Privacy Commissioners

The data privacy commissioner model vests in a statutory officer a large degree of autonomy and independence. A commissioner will have a range of functions in areas such as compliance, supervision, investigation, redress, guidance and public education. The data protection authorities accredited to this conference are, by virtue of their broad functions and depth of experience, the premier experts on the principles and practice of data protection and privacy in their jurisdiction. They each have a clear mandate to promote and protect data protection across a wide sphere of activity and all the necessary legal powers to carry out the task. Data privacy commissioners have a unique role, and a heavy responsibility, in respect of ensuring that an appropriate balance is struck between costs and benefits when implementing data privacy law.

Of course, to a certain extent, data privacy commissioners, simply "play the cards that they have been dealt". If, say, the law requires that data controllers be licensed, then this is the function that must be performed notwithstanding any economic impact. Commissioners do not control the fundamental balances that a national data privacy law strikes on economic questions, nor the unavoidable compliance costs involved in meeting its requirements.

As an aside, data privacy commissioners are not entirely passive in respect of the law under which they operate: For instance:

- They may have the opportunity to advise on revisions of data privacy law.[14] This was the experience of many European commissioners whose laws were re-enacted to comply with the EU Directive.

- Some commissioners have statutory functions to review their law. For example, the New Zealand Privacy Commissioner is required to do so every five years and recommend amendments.[15] Even without an explicit function, commissioners may offer recommendations for improvement.[16] Some commissioners individually, or collectively, made submissions on the European Commission's first review of the operation of the EU Directive.

- Commissioners also engage in rule setting of their own, for example by statutory codes of practice.

Many data privacy laws "build in" reference to competing interests into the operative provisions. A typical example, found in the New Zealand law, permits disclosure of personal information is where an agency believes, on reasonable grounds:

---

[13] APEC has not yet adopted its privacy framework and the text quoted is simply a version released during 2004 for public consultation.

[14] In New Zealand's case the first Privacy Commissioner, appointed in 1992 under a small paving law known as the Privacy Commissioner Act 199, actually had the task of advising Parliament on the enactment of the full data privacy law, the Privacy Act 1993.

[15] Privacy Act 1993 (NZ), s.26. When the New Zealand Privacy Commissioner last undertook such a review, an18-page discussion paper "Compliance and Administration Costs" (September 1997) was released. More than 2000 copies were distributed seeking submissions. The paper and submissions received are available on request.

[16] I must note the UK Information Commissioner's "Make Data Protection Simpler" campaign. An invitation to business and others to provide suggestions appears on the Commissioner's website. The campaign aims to simplify the law and compliance requirements.

> *that the disclosure of the information is necessary to facilitate the sale or other disposition of a business as a going concern.*[17]

This enables, for example, "due diligence" disclosures to be made during the process of a sale of business. It has worked successfully and has meant that the Privacy Act has not imposed any costly barrier to reasonable business practice in that context.

Some data privacy laws, in addition to mentioning economic factors in particular provisions, give an overall direction to a commissioner to bear in mind economic impacts when exercising powers. For example, the New Zealand law provides:

> ***Commissioner to have regard to certain matters***
> *In the performance of his or her functions, and the exercise of his or her powers, under this Act, the Commissioner shall:*
> *(a) have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and*
> *(b) take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and*
> *(c) consider any developing general international guidelines relevant to the better protection of individual privacy; and*
> *(d) have due regard to the information privacy principles and the public register privacy principles.*[18]

The activities of a regulator (such a data privacy commissioner) always have the potential to have an impact on economic activity and economic outcome. While much of the economic impact may be inherent in the law itself, there may nonetheless be an additional impact, either way, through the performance of the regulator. The regulator's impacts may be direct or indirect, positive or negative, and intentional or unintentional. Assessing these impacts is by no means straightforward. However, a commissioner may help avoid the unintended consequences of its decisions by paying attention to the practical impact of its decision. Decisions that do not take into account the way a particular sector or constituency works, and whether it is going to be able to implement the decisions within the constraints under which it operates, likely to have adverse economic consequences without necessarily achieving the goal sought.[19]

An exceptionally thoughtful and reflective piece by the former Australian Privacy Commissioner develops these points and ought to be required reading for all those interested in the subject.[20] That paper suggests that measures of a good regulator when evaluating economic impact could be:

- the regulator has a positive impact on the economy
- if the regulator has a negative impact on the economy this is an intended consequence and is outweighed by either positive indirect economic outcomes, or positive social outcomes
- the regulator has a process for assessing and evaluating economic impacts
- economic impacts are fairly distributed across the economic sectors
- economic efficiency costs, caused by organisations or individuals having to meet bureaucratic requirements are minimised

---

[17] Privacy Act 1993 (NZ), s.6, information privacy principle 11(g).

[18] Privacy Act 1993 (NZ), s.14. A similar provision is found in Australian law: Privacy Act 1988 (Cth), s.29.

[19] An example is the requirement that before the New Zealand Privacy Commissioner may issue a code of practice she must not only arrange public notification but *also* do "everything reasonably possible on her part to advise all persons who will be affected by the proposed code, or representatives of those persons, of the proposed terms of the code, and of the reasons for it" and give such persons or their representatives "a reasonable opportunity to consider the proposed code and make submissions on it". See Privacy Act 1993 (NZ), s.48.

[20] Malcolm Crompton, " 'Light touch' or 'soft touch': Reflections of a regulator implementing a new privacy regime", 2004.

- decisions the regulator makes are practical, workable and able to be implemented by the constituency
- regulator sought to harness market forces rather than oppose them, either by finding explicit pricing models that provide incentives to appropriate behaviour, or by helping businesses and others to see the business case behind complying with the regulation or even going beyond that.

The Australian Commissioner attempted to assess his own activities against these measures, not an entirely straightforward task. [21]

Data privacy commissioners typically have a function of promoting compliance with the law. Within a commissioner's budget there will always be pressure between competing claims for resource. Does an audit programme or a publicity campaign deliver the results desired? Should money be spent on researching new technological impacts or in investigating complaints? How much time should be spent lobbying politicians and how much in speaking to community groups? Commissioners are generally empowered to do a range of functions while resourced to actively perform somewhat fewer. Commissioners have a discretion as to which aspects they particularly target for compliance work. The attitude taken in respect of non-compliance will also send economic signals. A punitive message might have a different effect to one which places an emphasis upon promoting compliance. Weak or non-existent enforcement action may equally send a message which could promote non-compliance. There is certainly room for more comparative study as to different means of achieving compliance in ways that are cost effective both for commissioners and regulated organisations.[22]

4 Challenges: Difficulties in measuring costs, benefits and risks

It is now a quarter of a century since key data privacy instruments were adopted by the OECD (1980) and Council of Europe (1981). These were followed by the UN Guidelines (1990) and the EU Directive (1995). Most of these instruments have had reviews of a sort. The OECD Guidelines were reaffirmed by a 1998 Ministerial declaration,[23] the Council of Europe Convention received an updating protocol in 2001,[24] and the European Commission has been reviewing the Directive's transposition. Nonetheless, there are people who wonder whether the various national laws, and the international instruments, really achieve their objectives of protecting privacy and whether achieving the supposed benefits is worth the cost.

It would seem a reasonable proposition to seek to measure the benefits brought by data privacy laws, and the costs in complying with those laws, to see whether there is a net benefit.

There is much to be said for studying the usefulness of Cost Benefit Analysis (CBA) in data privacy regulation. Colin Bennett and Charles Raab discussed some issues surrounding the use of CBA and also the related attempts to quantify "privacy risk" in their recent book. They note, for example:

> *[P]rivacy and data protection discourse uses the language of 'risk' as if the concept were unproblematic, and as if all risks were alike. Yet even if we were able to estimate different degrees and kinds of risks inherent in transactions involving personal information, to say simply that 'data matching poses a threat to privacy', or that 'people's privacy is at risk if databases are inaccurate' – whatever the truth in that – does not get us closer to a more nuanced understanding of what is more serious and what is less serious, or what is perceived to be the case, and why, on which to found regulatory policies and practices. If this has been a problem at the organisational and national levels, it is perforce true at the global level. However, ... we cannot easily separate objective and subjective dimensions of the concept of risk, or describe clearly the relationship between the two. No easy distinction can be drawn between 'real risks' and 'mistaken perceptions', nor can it be supposed that science can determine the former and explode the fallacies of the latter. This may be particularly so in fields such as information processes, in which human perception and agencies shape the situation in which personal data are collected or transmitted, and in which regulatory policy must be geared to people's perceptions and fears as much as – or more*

---

[21] Ibid.

[22] Bennett and Raab (2003) is a recent comparative study of particular interest.

[23] OECD, "Declaration on the Protection of Privacy on Global Networks", 1998.

[24] Council of Europe, Additional Protocol to the Convention of the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, 2001 (CETS No 181).

> *than – to any 'objective' calculation of risk, even if the latter were conceptually and empirically possible.*[25]

Certainly monetary figures can be put upon some of the costs of complying with a data privacy law but it is much more difficult to quantify the benefits in monetary terms. Usually the characterisation of benefits, if it is attempted at all, is done merely by a narrative list. Accordingly, where this kind of CBA is attempted one will frequently have a monetary figure for costs, easily understood by decisionmakers (even if that figure is arrived at by fairly dubious means) set against a narrative for benefits given in rather vague terms such as "greater accuracy" or even in unconvincing terms like "some individuals do not like being numbered" or "some people fear having their data kept in a centralised database".

Notwithstanding the difficulties, commissioners should consider these supposedly "objective" measures of costs and benefits if only because other decisionmakers expect them to be used. With luck and skill it might well be that better methodologies will be developed to quantify privacy risk and benefits. If this remains elusive (as I expect it may) commissioners still need to better understand the methodology so as to knowledgably challenge (or contribute to) the CBA attempts of others.

Of course, even if only the cost side of the equation can be accurately identified this will usefully inform commissioners. It may also be helpful to know the measurable non-privacy benefits of invasive practices. CBA is, for example, an established part of the evaluation of proposed data matching programmes in New Zealand.[26] The assumption is that the invasive practice of data matching may well be justified in the public interest if there is a significant and quantifiable benefit, but if this cannot be established the data matching should not proceed.

Attempts at systematically assessing projects that may have a significant impact on privacy are also being promoted by way of privacy impact assessment. The New Zealand Privacy Commissioner has, for instance, published a handbook to encourage organisations to more systematically assess their own projects and, in particular, to try to mitigate privacy risks at the time of design of new systems.[27] Privacy impact assessment is also widely required in Canada and the USA.[28]

5 Warning: Don't over-balance the scales

No doubt everyone rightly expects commissioners to strive for cost effective regulation which does not impose unnecessary burdens. However, it may be worth expressing some caution about "tipping the scales" in favour of business interests and against those of individuals. If a country's legislature has enacted a law which already strikes a balance, there may be a danger that a commissioner in zealously striving to, say, diminish compliance costs, may reset the balance to one that differs from that intended.

The former Australia Privacy Commissioner nicely characterised the possibility of the regulator tilting the balance too far by wondering, in the title of a speech, whether the Australian law represented a 'light touch' or a 'soft touch'.[29] He posed the question as follows:

> *The office's approach to regulating privacy has caused some controversy. For example, has the office been in the pocket of the big end of town or has it failed to act sufficiently strongly against organisations that breach provisions of the Act? Or has the office in fact taken too tough a stance, as has been claimed elsewhere?*[30]

Data privacy laws are premised upon the need to modify the information handling practices of organisations towards certain norms. It must inevitably impose a cost on some organisations. Whether the cost is worth it is ultimately one

---

[25] Bennett and Raab (2003), 227.
[26] Privacy Act 1993 (NZ), s.98.
[27] Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook*, Auckland, March 2002.
[28] Privacy impact assessment is, for example, a statutory requirement in the health sector in the province of Alberta and is government policy at federal level and in Ontario. In the USA, privacy impact assessment is required under the E-Government Act 2002.
[29] Crompton (2004).
[30] Ibid, 1.

for society and, in particular, the legislature, rather than the regulator. Care must be taken to avoid "regulatory capture" whereby commissioners come to identify more with the interests of the people that are supposed to be regulating than with the interests of the people they are supposed to protect.

6 Conclusions

In conclusion:

The international instruments on data privacy were premised upon reconciling the need to protect the fundamental human right to privacy and the need to avoid unwarranted barriers to transborder data flows.

The international approach is implemented in national data privacy laws. These laws impose economic costs but they also strike a series of balances between privacy and competing public interests and vest discretion in regulators.

Data privacy commissioners are the key institution established by data privacy laws. Commissioners can play a special role in respect of recognising and responding to the economic issues involved.

Commissioners should seek to be flexible and innovative in seeking to making data privacy laws work in a cost effective manner. Where appropriate they should actively engage in law reform to improve ineffective data privacy laws or laws that are unduly burdensome. They should be mindful of the power and usefulness of Cost Benefit Analysis while recognising its shortcomings.

However, commissioners should avoid "regulatory capture" by failing to enforce privacy rights that the legislature has enacted through undue deference to concerns about business compliance cost.

Bibliography

1. Australian Law Reform Commission, *Privacy*, Report No 22, 1983

2. Bennett & Raab, The Governance of Privacy: Policy Instruments in Global Perspective, 2003

3. Crompton, Federal Privacy Commissioner of Australia, "'Light Touch' or 'Soft Touch' – Reflections of a Regulator Implementing a New Privacy Regime", speech delivered at National Institute of Governments – Canberra and Committee for Economic Development of Australia – Melbourne, March 2004

4. Office of the Privacy Commissioner, *Privacy Impact Assessment Handbook*, New Zealand, March 2002