Lilian Edwards
Co-Director, AHRB Centre in Intellectual Property and IT Law
Faculty of Law, University of Edinburgh

L.edwards@ed.ac.uk
www.law.ed.ac.uk/ahrb

Poland, September 2004

Reconstructing Consumer Privacy Protection On-Line – A Modest Proposal

AHRB Centre in IP and T stream

"Anonymity, Privacy and Consumers"

www.law.ed.ac.uk/ahrb

Why Do We Want To Protect On-Line Consumer Privacy? Engendering Trust

- UK consumers spent £10bn online in last twelve months (Sept 03 figs), £470 per adult consumer
- Yet 85% think shopping on the High Street still safest (NCC figures for UK, 2000). And even 46% of *experienced* Internet users think the Net is riskiest place to shop.
- E-Commerce even in US is only 1.6% of consumer retail business
- Meanwhile 84% of EC citizens never buy anything over the Internet (only 3% have in Greece, 25% in UK); of these 84%, 25% say they do not trust the Internet.
- Of the 16% of EC consumers who have bought on the Net 48% still report "security concerns" (Eurobarometer, 2004)

How to promote trust in e-commerce?

- Trust in buying on line and protection of privacy *seem* intimately connected (?)
- Eg 25% of consumers report avoiding any sites which collect personal information (Jupiter, Oct 03)
- *Aim* of regulation of consumer privacy on-line should be *to promote confidence and trust in e commerce by consumers.* Approaches: encryption, kitemarking, codes of practice, padlock symbols, awareness campaigns, ADR networks, etc.
- Focus of this paper is on one issue: how to prevent or otherwise deal with *privacy related harms*

Potential privacy harms to consumers from data collection on line?

- *Identity theft harms* eg misuse of credit card info. Up 45% in UK last year (APACS, March 04). Over ½ million complaints re ID theft to FTC in 2003.
- *Disclosure harms* eg Eli Lilly Prozac list, wrongful credit info
- *Invasion harms*: eg spam (now up to 62% all email, Brightmail, Feb 04), pop-up ads, spyware, etc.

Advantages of allowing data collection by on line businesses

- For consumers
  - Personalised service on B2C e commerce sites
  - Giving sites a "memory" eg Amazon shopping cart, combining orders, preference suggestions, wish lists, remembering who you are
  - General *convenience factor* for consumers
- For businesses
  - Gives e-commerce sites a valuable asset ie. database of customer info. Value enhanced on sale, eg, to advertisers, after liquidation; or after data mining.
- For both?
  - Creation of a trusted relationship?? Eg Yahoo! evidence on "permission based marketing"

Solutions 1 – the European/DP model

Strong legal regulation in form of data protection law

Requires

- Registration/notification by data controllers of purposes for which data collected
  - No "primary purpose" restrictions, or checks on whether data collection necessary to core business goal
  - Use of data then restricted to notified purposes
- Consent by data subject to data collection required
  - But significant exceptions eg legitimate business purposes
- Independent enforcement body
- Data security and retention rules
- Data subject rights of access and integrity checking
- Data export rules of "adequacy" – but "safe harbor" for USA, standard contractual terms

DP regulation: problems

- **Historical origins:** DP tailored for mainframe, non-Internet, data warehousing environment, when compliance by few "elephants" (Swire) as opposed to many "mice" was relatively easy to police. "Elephants" generally compliance-friendly, hence negotiation-based enforcement, low level sanctions worked. "Mice" - websites, on line businesses, spammers, fraudsters, most trading outside Europe - are numerous, hard to spot, run away, hide and lack resources and legal knowledge for compliance.
- **The sheer size of cyberspace and lack of resources for compliance:** Post Internet, many 1,000,000 s of "mice". Data Protection Commissioners generally under-funded, under-staffed, reactive not pro-active. Poor DP compliance reported by website sector in UK (ICO/UMIST study , May 2002- 40 % of UK commercial websites don't even know what personal data they hold.) 2003 study found that although 94% of large UK companies had notified only 4% could provide data subject acces rights on request. "Lip service compliance".
- **The global cyberspace environment**: Most processing of personal info goes on outside EU (around 90% of spam from outwith EU, only UK in top 10 origin of spam countries list) yet no global harmonisation on DP law. Rapprochment exercises such as EU/US Art 25 DPD "safe harbor" not outstanding successes (only 493 US companies signed up at April 04.)

DP regulation: problems (2)

- **Lack of customer pressure to enforce** : as level of knowledge and exercise of DP rights, and of dangers of giving away info generally, very low. 44% of UK consumers think they have less rights on line than offline. 71% of UK consumers were prepared to give away passwords to strangers for chocolate (April 04).
- **Key notions** of consent, opt-in, opt-out, "personal data", "domestic purposes", etc **contested, vague and unharmonised** (see eg *Durant v FSA*, *Lindqvist v Sweden*.
- **Does not fit US or EU corporate business models of data sharing** after mergers, take-overs, liquidations etc. Also costly & fiddly. US business unwilling to regard daat as property of consumer; EU businesses regard it as compliance hurdle and annoying business cost and paperwork.

Solution 2 – the USA/self regulation model

- Main approach is self regulation, some piecemeal legislation.
- Privacy policies semi mandatory
- Codes of Practice
- On line self regulatory bodies – trust marks or kite marks – TrustE, Online Privacy Alliance etc,
- Some (increasing) FTC compliance action
- Generally seen as inadequate by EU model
- Industry hostility to costs of full DP regime
- Personal data seen as *property of collector, not subject*

US/Self regulation: Problems

- No real "market" of choice for consumer as many privacy policies similar
- "Notice"? Do privacy statements get read, understood by consumers?
- How effectively are privacy standards upheld *after* data collection? Eg on liquidation, sale, merger?
- Sanctions by trust seals? TrustE etc have notably failed to adequately punish serious breaches by prominet members (Geocities, Microsoft) Egghead.com case.
- FTC's own verdict : "*self regulatory initiatives to date fall far short.. cannot ensure that the on line marketplace as a whole will emulate standards adopted by market leaders*" (2000)
- Industry not so willing now post dot.com implosion to pay to belong to trust seals anyway – TrustE's numbers have fallen.

Solution 3 - Code

P3P (Platform for Privacy Preferences)

- In theory enables consumer to bargain as to when and why they will allow their personal information to be collected via pre-selections on security made in browser
- Pushed as solution for US consumer who lacks faith in self regulation but does not want to resort to full PETs (Privacy Enhancing Technologies) eg anonymisers, proxy servers, encrypted email etc.
- Reflects "*propertisation*" of personal data – appropriate?

Code : Problems

- P3P:
  - Automation may get round "notice" problem but are there real choices to be made between the privacy options offered by websites? P3P is essentially automated bargaining which requires a marketplace of choices to work. See back!
  - And again, what about *post-collection* enforcement?
  - Disingenuous – not privacy "firewalls"
  - Can consumers bargain fairly when they don't know the value of their personal information *in aggregate*?
  - Do consumers care enough to *learn how to use* P3P especially if little actual choice enabled? Favours "techies". Time overhead/technophobia. Even more true for full PETS. Only true privacy fundamentalists likely to spend the time/effort/money.

Assessment

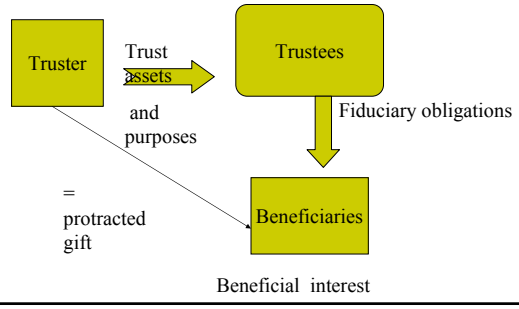
- DP is most sophisticated global model for *privacy harm prevention*, but for reasons noted, in trans-national cyberspace, does not prevent privacy harms listed at start. In terms of privacy *rights*, mainly provides little used data subject access/verification rights, not real privacy protection, nor *compensation* for harms such as ID theft, spam.
- Even if US was likely to embrace EC DP regime in full (implausible) increasingly ineffective even in Europe, even after tweaks in Privacy Directive 2002.
- Self regulation similarly does not effectively prevent privacy harms.
- P3P : encourages consumers to sell their privacy too cheaply as does not reflect aggregate value of data collected & provides no post collection safeguards
- Do we need to look to a different model? *Privacy harm compensation* rather than *privacy harm prevention?*

Preventing or compensating privacy harms? Control vs Compensation.

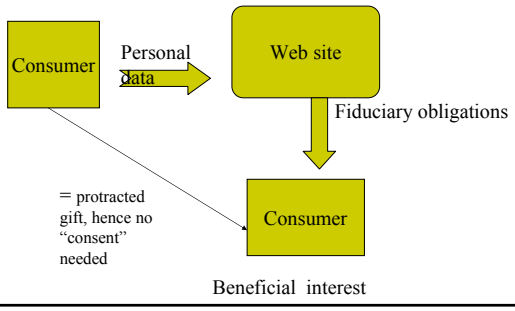
Alternate model? – the "trust model"

- Inspired partly by Terry Fisher's (Harvard) approach to P2P illegal file sharing/downloading problem
- Information wants to be free, data wants to flow?
- Fisher advocates *giving up* futilely trying to control illegal copying of copyright work by rights-holders – instead, give it away, abandon trying to enforce copyright rules against downloaders.
- BUT – still provide *compensation* to rights-holders via an appropriate *tax* eg on broadband, computer hardware, blank CDs – re-distributed fairly in proportion to downloads
- Transfer to privacy context – instead of trying to *prevent* privacy harms by rigorous DP rules, consumers get *compensated* for privacy harms
- In privacy context – who should pay? A. – the businesses who make money out of collecting and processing data and currently get it (largely) for free. Some kind of "privacy tax".
- *Clearly not ideal* to only compensate breaches, not prevent them
- BUT - If data collectors and processors are made to *pay* for privacy harms, will they be incentivised to try harder to prevent privacy breaches?
- *Different from ordinary tort/delict model* because enforcement will be by independent body (as in DP) not left up to individual consumer
- NB Human rights of those who care deeply about privacy still need attention.

Justification for "privacy tax" on data collectors/processors - the "trust model"



The trust model applied to on-line data



Benefits - 1

- Data subject as beneficiary has part interest in *aggregate* value of "trust" assets ie data collected from *all* data subjects/consumers by one website.
- Focus is on *external effects of data collecting/processing* – not "indoor management" of trust. Aim is to provide *remedies for harms* = "abuse of trust", not to require/enforce internal bureaucratic regime -> perhaps more popular with, and practical for, industry?
- Clear under model that data collector owes *high duty of care & fiduciary obligations* to data subject to care for info collected even if (as in US ethos) collector regarded as owner of data and not data subject
- Data subject has *individual right of action* against data collector for abuse of trust – but backed up public enforcement (by FTC/Inf Comm'r/new enforcement body).

Benefits of model - 2

- Does away with need for defining "consent" and associated nuances as personal data is *given away* (some privacy fundamentalists will object – see later)
- Goes after "elephants" (visible data collecting businesses) not "mice" spammers, ID thieves etc) to get remedies for those harmed
- Harmonisation. "Trust" is well known common law model , yet contains elements key to DP/civilian approach. Trust as an institution is increasingly seen as useful solution for harminsing EC property law systems. May be more acceptable in USA than detailed EU DP regime.
- Perhaps "Trust" as a rhetorical notion may inspire confidence where DP has failed

Issues - 1

- How should "beneficial interest" of consumer be redeemed/distributed? Many issues:
  - What is value of trust property? Value of dbase on actual sale? On nominal sale? % of profits made by collecting sites?
  - Option 1: distribute "dividend" to consumer pro rata as per data collected from subject, or time subject spent at site, or money spent? – problems: high transaction costs; privacy threat itself in audit trail needed to work out usage
  - As above, but simply *per capita* distribution?
  - Consumers get multiple "dividends" from multiple "trusts" for each website visited – fiddly small change
- Answer: move to Fisher's "tax" model and ask data collectors to pay a "privacy tax" on their profits. Will go into single compensation fund pot, to be applied to prevention of privacy harms =>

Compensating privacy harms

- Uses for "privacy tax" compensation pot?
  - Provide statutory compensation pay-outs for recognised privacy harms, reported to and accredited by enforcement body. No need to prove fault, causality, economic damage. No need for consumers to bring own actions. Data collectors who pay privacy tax can retain common law rights to pursue actual wrong-doers to compensate *themselves*.
  - Improve enforcement. Create new watchdog body, or top up funding of existing national bodies such as FTC, national DPCs, to aid in compliance with national laws/self regulation measures
  - Provide PETS for free (and public education) to consumers who *refuse* to give away personal info (privacy fundamentalists)

Criticisms

- Why *should* the "elephants" agree to pay for the sins of the "mice"?
  - Natural justice - currently personal information is a "free gift" to them they profit from (although query if the value is in the data or in the post collection processing?)
  - Pragmatic argument – taxpayers are those most closely connected to the data collection which leads to privacy harms, therefore the tax will encourage them to improve in-house privacy standards (cf ISPs improving access to member databases)
  - PR incentive – putting what is effectively an industry "no fault" compensation scheme in place will reassure consumers enormously and engender trust? hence increase e-commerce uptake?
  - Reduction of red tape incentive – *quid pro quo* of no longer having to comply with DP notification, access requests and other compliance fuss. No more interference with "indoor management".
  - Could be transitional device till technology/code and consumer savvy catches up and provides better solutions – eg payment by anonymous stored-value smart card, buying "anonymous browser IDs" from a digital Post Office

Summary

- Attempts to break the impasse in global cyberspace between US and EU approaches to data privacy
- Prioritises prevention of, and compensation for, privacy-related harms to consumers, rather than industry compliance with bureaucratic structures
- Regards personal information collected as an *aggregate* good held for benefit of data subjects
- Doesn't throw away the baby with the bath water – companies still get to collect, process and mine data, and consumers still keep convenience factor on-line
- Abandons "one size fits all" omnibus privacy protection
- If it works - engenders trust?