Reconstructing Consumer Privacy Protection On-line: A Modest Proposal

By Lilian Edwards

Abstract: Problems with consumer trust and confidence in the Internet as a safe environment in which to shop, browse and associate are well documented, as are the correlations between this lack of consumer trust and fears about privacy and security on line. This paper first attempts to show why existing legal and extra-legal modes for protection of privacy on line are failing to protect consumers and promote consumer trust, and in particular critiques the European regime of mandatory data protection (DP) laws as out-dated and inappropriate to a world of multinational corporatism and ubiquitous transnational data flows via cyberspace. In the second part, lessons are drawn from the crisis currently faced by intellectual property in cyberspace, particularly in reference to MP3s and P2P downloading, and useful parallels are drawn from the solution devised by William Fisher of the Berkman Centre, Harvard in the form of an alternative payment scheme for copyright holders. Finally, the insights drawn from Fisher’s work are combined with original proposals drawn from comparison of the consumer-data collector relationship in cyberspace, with the roles played by truster, trustee and beneficiary in the institution of common law trust. The resulting “modest proposal” suggests that a “privacy tax” be levied on the profits made by data collectors and data processors which could fund no-fault compensation for identified “privacy harms”, improve public privacy enforcement resources, provide privacy-enhancing technologies (PETS) to individuals, satisfy the desire of commerce for less DP-related internal bureaucracy, and possibly create the conditions for better promotion of consumer trust and confidence, thus improving the uptake of e-commerce.

1 This paper was first published in the International Review of Law, Computers & Technology, Volume 18, No. 3, November 2004, Carfax Publishing, Taylor & Francis Inc.
2 The Barbara Wellbery Memorial Fund, established in 2003 to honor the memory of Barbara Wellbery and her contributions to the field of international privacy, seeks to encourage the development of pragmatic and practical privacy approaches to privacy and managing cross border data flows. One of the key goals of the Barbara Wellbery Memorial Award is encourage new, innovative, and in-depth thinking about international privacy issues, and in particular about ways to resolve the issue of global data transfers. Barbara's greatest strengths were an open mind and passion for constructive discourse and exploration.

In that spirit, the board has selected this submission for its scholarship and originality. The ideas and conclusions presented in the paper represent the views of the author alone and do not represent the views of the board. Some members of the panel, in fact, disagreed with substantive parts of the paper though there was unanimous agreement that the paper was creative, scholarly, and provocative. The paper presents a new and radical paradigm that shifts the traditional privacy debate from a harm prevention model to a harm remedy model. In particular, the paper is being recognized for its innovative perspective and analytical model which the board hopes will spark constructive debate and stimulate creative thinking in the field of data privacy.

3 Lilian Edwards is the Co-Director, AHRB Centre for Research into Intellectual Property and Technology and Senior Lecturer, Law Faculty, Edinburgh University, UK.
1. Introduction: the problem with privacy

Despite the many well publicised benefits of the Internet as global marketplace, and to the frustration of the struggling dot.com economy, consumers are reluctant to take to buying goods and services on-line. While headlines trumpet that US consumers spent almost a quarter more on-line in 2003 than they did the year before, they are more taciturn about the fact that total on-line spending is still only about 1.6% of consumer retail business. In Europe things look even bleaker; 84% of EC citizens never engage with e-commerce and when split down national lines, this figure goes as low as 3% of all Greek consumers. In the UK, only around a quarter of consumers have ever bought anything on-line. From some perspectives, this is odd. Fairly plainly, there are important benefits which should impel consumers to use the Internet - such as availability and range of goods, high initial information provision, accessibility, speed and ease of purchase, customisation of goods, and ability to make relevant price comparisons. Furthermore, when consumers give away data when they shop and browse on-line, whether knowingly or unknowingly, the shopping experience is often improved and made both more personalised and efficient. A good example of such is the Amazon.com site, which collects and stores customer data so that it can retain a note of returning customer choices and preferences, can combine outstanding orders to save postage, can retain credit card details, past orders, and delivery addresses,

---

4 Or, more accurately, as Graeme Laurie puts it, why privacy causes problems. See G.Laurie Genetic Privacy: A Challenge to Medico-Legal Norms (Cambridge University Press, 2001) I would like to thank Dr Laurie, whose original suggestion it was that trust might have something to offer in the field of protection of personal information; also Professor Geraint Howells of Sheffield University, with whom I collaborated at an earlier stage of this research; and the participants of the conference on Privacy, Property and Personality, Edinburgh, November 2002; and those at Securing Privacy in the Internet Age, Stanford Law School, March 2004. Any errors are of course the responsibility of the author alone.

5 Figures from the US Department of Commerce: see http://news.bbc.co.uk/1/hi/business/3515287.stm These do not, however, include online travel services, financial brokers and ticket sales agencies, which were excluded from both online and total retail sales figures. If these were included the percentage figure might be as much as doubled.

6 EU EuroBarometer Survey (March 2004). See http://europa.eu.int/comm/consumers/topics/btoc_ecomm.pdf. It is worth noting however that a majority of e-commerce refuseniks, 57% of EU citizens surveyed, said they did not shop on-line simply because they did not have access to the Internet. A total of 16,000 people were surveyed., with distinct differences observed across countries, income groups and age groups eg 37% of Swedes had purchased on line compared to only 3% of Greeks.

uses customer profiling and past orders to advise on new items for sale of possible interest, and offers a convenient ordering platform in the form of a “shopping cart”. More generally, it has been suggested that the voluntary disclosure and exchange of information between website and customer gives some semblance of a “trusted” relationship which is good both for the consumer’s confidence and the enterprise’s profits. Organisations such as Yahoo! claim to have found “permission based marketing”, in which no information is collected (or email sent) without the prior consent or opt-in of the consumer, the best way forward to build a successful trading relationship.\(^8\) For traders, of course, the advantages of collecting data from consumers shopping on-line are obvious: not only do they gain a valuable opportunity to cement the existing commercial relationship, but they also gain a new and valuable asset, namely the customer details. Individually one customer’s email address and shopping preferences may not be worth much; but taken in aggregate, a customer database can be an extremely profitable thing to acquire, not only as internal resource but to sell, wholly or partially, to on line advertisers such as DoubleClick, direct marketers, and even competing businesses in the same market sector. In liquidation, takeover or merger scenarios, such assets may be an important bargaining point; indeed in some dot.com cases the only asset\(^9\).

But there are also major drawbacks which deter consumers from shopping on-line – notably, the fear that the Internet is not a safe or trustworthy place to do business. When consumers are asked to rationalise this fear, they tend to respond with some mixture of beliefs they will (i) suffer economically via financial fraud and (ii) suffer both economically and emotionally as a result of disclosure of personal information on-line. These can be distinguished as the security and the privacy problem\(^10\), but are often in survey statistics, and perhaps nearly always in the minds of consumers, conflated into one. The source of these anxieties is not that hard to see. The media abound with horror stories about consumers whose credit card details have been appropriated and misused.


\(^9\) It is rare to see a value publicly put on a customer database in business sales or mergers. However in one well known incident, when Egghead Software was sold to Fry’s Electronics in 2001, for example, its only major asset apart from some IP rights was acknowledged to be its database of 4 million customers, and the price paid for the company was $10 million.

on-line; whose personal secrets have been inadvertently disclosed on-line to all and sundry\(^\text{11}\); whose entire “identity” has been stolen with terrible ensuing results for job security, bank account, credit history, and personal relationships. Once these stories were mainly restricted to technical sections, or to on-line sites rather than everyday papers and magazines; this distinction has now collapsed\(^\text{12}\). Privacy and identity theft on the Internet are big news, and even the least clued up consumer is now dimly aware of this. At a less sensational level, the business, technical and professional media regularly report news of sales, or transfers on bankruptcy, merger or takeover, of personal information to third parties without the consent of the data subjects in question. Civil liberties pressure groups, law enforcement authorities, and regulators such as the Information Commissioner and the Department of Trade and Industry are also attempting to sensitise consumers to the perils of disclosing information on-line. The net result is that consumer confidence in the Internet as a secure medium is deeply flawed.

This failure of trust is clearly demonstrable by empirical evidence. In survey after survey, failure of consumer confidence in Internet security and privacy is cited as one of the major inhibiting factors in the growth of business-to-consumer (B2C) e-commerce. One of the first key surveys on on-line consumer trust in Europe, the UK National Consumer Council report, *e-commerce and consumer protection*\(^\text{13}\) found in August 2000 that 85% of UK consumers felt safest shopping on the High Street and over a third felt the Internet was the riskiest place to shop. These figures, though eons old in Internet years, probably still largely reflect the fears of current consumers\(^\text{14}\). A survey on cross border shopping conducted for the Department of Trade and Industry (DTI) in the UK in October 2002 found that a third of those questioned would not buy goods from other EC countries via

\(^{11}\) See the Eli Lilly Prozac list, and Microsoft Passport disclosure cases reported in (2002) *Privacy and Data Protection*, Vol 3-2 at 12.
\(^{12}\) *Marie Claire* magazine (US edition) for March 2004 had a major spread on Internet privacy which noted breathlessly: “What strangers can find out about you: Your dress size. Your salary. Your salacious affair! Secrets you thought were yours alone are actually available to the highest bidding marketer. Could the most intimate details of your life become public knowledge?”
\(^{13}\) Downloadable at [http://www.ncc.org.uk/pubs/e-commerce.htm](http://www.ncc.org.uk/pubs/e-commerce.htm).
\(^{14}\) It is difficult to directly compare figures in surveys on Internet consumer privacy, trust and e-commerce, as each survey tends to ask questions in different ways and each also adopts its own methodology, which is not always revealed. In particular, fears about the disclosure of personal data, including credit card details, pertaining to *personal privacy*, are often conflated with fears about *fraud*. The best recent objective survey of surveys on the themes of trust, risk, privacy and the Net can probably be found in C.J. Bennett and C.D.Raab *The Governance of Privacy* (Ashgate, 2003), pp 56 – 67.
the Web because of fears about credit card details and fraud, while 20% also cited worries about giving away personal data\textsuperscript{15}. More recently a Jupiter Research report in October 2003 revealed that 25% of consumers altogether avoid sites where they are forced to give personal details; while the latest of the regular EC EuroBarometer Surveys in March 2004 also found that of the 84% of EC citizens who still never participate in e-commerce, 25% do not shop on-line because they do not trust the medium\textsuperscript{16}. Even if only the 16% of EU citizens who have made an Internet purchase are taken into account, 48% of these are still “concerned about security” when making payments on-line. This eerily echoes the NCC survey of 2000, in which, even looking only at those who self-identified as experienced users of the Internet, 56% felt the Internet was the riskiest place to shop and 32% thought loss of privacy was a major drawback of on-line shopping. It seems that whether old or young, rich or poor, Nordic or Latin, European consumers are not at all happy about disclosing personal and financial information on-line, and if this stops them participating in e-commerce, well, there are plenty more shops in the sea (or more plausibly, on the High Street). As Bennett and Raab\textsuperscript{17} summarise:

“In broadbrush terms, the most common finding in survey after survey is that privacy is regarded as a very important value, and is felt to be strongly threatened by new information and communication practices and technologies used in commerce and government... Levels of knowledge about what happens to one’s data, and about the ways in which they can be misused in the various technologies and sectors, are not high, testifying to a lack of transparency and candour amongst data collectors, and to large deficiencies in consumer and citizen education.”

This problem of lack of trust is particularly pressing in Europe\textsuperscript{18}, where the uptake in B2C e-commerce has historically always lagged behind that in the US, for a number of reasons to do with the slower expansion of the home computer infrastructure, the historical dearness and slowness of home Internet access, a possible higher degree of

\textsuperscript{15} This survey was not restricted to cross border shopping by Internet alone, but included eg purchases while on holiday trips or on business travel.

\textsuperscript{16} Supra n 3.

\textsuperscript{17} Supra, n 11.

\textsuperscript{18} See eg, the EC eEurope initiative 2006, with its particular focus on secure infrastructure, at http://europa.eu.int/scadplus/leg/en/lvb/l24226.htm.
technophobia, and the problem of plurality of local languages, cultures and laws. In an attempt to meet this crisis of confidence, the European Union has spent a great deal of money and regulatory effort in the last ten years attempting to establish the conditions for both greater trust, greater transparency and greater privacy protection on the Internet, by passing not only new Electronic Signatures\textsuperscript{19}, E-Commerce\textsuperscript{20} and Privacy and Electronic Communications\textsuperscript{21} Directives, but also by setting up whole programmes of mixed paradigm initiatives such as the EC Action Plan, and its current successor, the Safer Internet Action Plan\textsuperscript{22}. These ambitious plans, comprising legal, social, technological, educational and financial elements, attempt generally to “clean up” the Internet and restore faith both in commerce and consumers that the Net is a trustworthy place to engage, socialise and trade\textsuperscript{23}. On the legal front, the EC has, of course, already famously adopted (and, where possible, exported) a detailed omnibus legal code which covers the issue of data privacy in the form of the Data Protection (DP) Directive of 1995\textsuperscript{24}. Although this Directive was not drafted specifically to deal with the Internet\textsuperscript{25}, it has recently, following extensive debate, been updated by the Privacy and Electronic Communications Directive (PECD)\textsuperscript{26}, to deal with the novel issues raised by the new digital and mobile technologies, and in particular, spam\textsuperscript{27}, locational and traffic data and “cookies”\textsuperscript{28}. In the US, by contrast, the legal culture has historically been very different, with the regime in relation to private collectors of data (as opposed to the state) one of industry self-regulation and a laissez faire attitude to legal regulation in this area.

\textsuperscript{19} 99/93/EC.
\textsuperscript{20} 2000/31/EC.
\textsuperscript{21} 2002/58/EC.
\textsuperscript{22} At \url{http://www.europa.eu.int/information_society/programmes/iap/index_en.htm}. The current plan runs till 2008. This page also contains an evaluation of the Action Plan which ran from 1999 to 2002.
\textsuperscript{24} 1995/46/EC.
\textsuperscript{25} The Directive was promulgated in 1995, with prior negotiations which began in the early 1990s, a time when the modern commercial Internet had barely begun to evolve. In many ways the Directive owes much of its substance to the earlier Council of Europe instrument on \textit{Automatic Processing of Personal Data} which was issued in 1981. See Swire and Litan, supra n 7, Chapter 2.
\textsuperscript{26} Supra, n 18; and see account in Carey P. \textit{Data Protection} (Oxford University Press, 2\textsuperscript{nd} edn, 2004).
\textsuperscript{27} Spam here is shorthand for “unsolicited electronic mail and similar forms of unsolicited electronic direct marketing”. The PECD refers only to “unsolicited communications” and “electronic mail” (art 13).
\textsuperscript{28} Cookies are small text files typically placed on a user’s hard disc while they are browsing an e-commerce website, which allow the operator of that site to record personal details about that user in a form which can be connected to that user on a subsequent visit to that site. The PECD refers to “so-called spyware, web bugs, hidden identifiers and other similar devices” but only within the recitals (recital 24) and not the main text.
Although considerable privacy legislation does in fact exist at both a state and federal level, it is piecemeal (eg. information collected from children is regulated\(^{29}\); as is information collected about video rentals\(^{30}\)) and not omnibus on the European legislation model.

As the efficacy of traditional legal and self regulation approaches to protecting privacy has proved increasingly questionable when applied to cyberspace, policy makers, government regulators, and privacy advocates in Europe and the USA have looked for solutions, either as additions or alternatives to the regulatory “tool-box”\(^{31}\), in the so-called “privacy enabling technologies” (PETS), and in particular, P3P, the “Platform for Privacy Preferences”\(^{32}\). The debate as to whether these technologies have real value, especially for the ordinary consumer who is neither economically powerful nor technologically savvy, is by no means yet concluded; but at time of writing, it seems unlikely that P3P and its ilk will in the near future become realistic and total solutions to the crisis in legal protection of on-line privacy.

The starting point offered here, therefore, is that neither European DP law, nor the alternative US self regulatory approach to privacy, nor technological means of protecting or enhancing privacy via PETS, can currently claim to give consumers satisfactory guarantees that their privacy and personal information will be protected should they decide to do business on the Web. This conclusion, which is of course a somewhat sweeping one, has been dealt with in depth in earlier work, both by this writer and others\(^{33}\), and can here only be summarised. More has perhaps been written in recent years on the flaws of the US self regulatory mechanisms as applied to Internet privacy than on the comparative flaws of DP law in the same environment; this piece attempts to redress that balance somewhat. The focus of the current paper, if this preliminary claim can be

\(^{29}\) The Children’s On-Line Privacy Protection Act (COPPA) 1998.
\(^{30}\) The Video Privacy Protection Act 1988.
\(^{31}\) Bennett and Raab, supra n 11.
\(^{32}\) Discussed infra at p XX.
accepted, is on a new model, the “modest proposal” of the title, which seeks to present an alternative means to better promote consumer trust and confidence on-line. “Trust”, of course, is not wholly predicated on better privacy protection on-line – or even a public perception of better protection – but the two do seem to be intimately linked. It is commonly asserted that people’s confidence in doing business on line is shaped by beliefs the recipient of personal data will respect and protect their privacy. “After all, goes this argument, wouldn’t you be more willing to buy on line if you knew your own information would not be released elsewhere? Haven’t you hesitated about doing certain transactions because you did not trust how the Web site would handle your data?”

Another factor involved, as a recent Oxford Internet Institute report identifies, is that concepts of trust and privacy are both bound up with identity:

“[consumer] worries … focus on three main aspects of trust in electronic transactions: identity, privacy and security. The potential for difficulties in establishing the authenticity of the identity of a consumer or online business is one of the characteristics that distinguishes trust issues in the electronic environments from most other contexts. For consumers, identity is bound up with concerns about privacy and data protection that have been highlighted ever since computers emerged as an important technology in the 1960s.”

de Hert, writing in a collection of legal essays on the impact of trust on e-commerce, makes similar connections, and notes that since “free choice and control are essential ingredients of privacy”, the collection of personal data without transparency and consent, as with the setting of “cookies”, destroys privacy and along with it, “values such as human dignity, respect, equality, and the necessary integrity of social spheres”. He goes on to conclude that “casual snooping and secret gathering of information about consumers is a breaking of trust – a kind of cheating and breaking of existing rules”.

---

34 Swire and Litan, supra n 7, p 80.
37 Interestingly, de Hert, as here, also goes on to consider if existing legal regimes are sufficient to adequately protect consumer privacy and promote trust and confidence. Like this writer, he has doubts
Finally Rosen interestingly suggests in *The Unwanted Gaze*\(^{38}\) that we connect lack of control over our privacy on-line to fears and anxieties about lack of trust, not just because personal information is almost invariably disclosed in Internet transactions, but because the information disclosed is partial, lacking, and may be revealed out of context with the result that what is disclosed on-line does not mirror the image or profile we feel is a more accurate portrayal of our self\(^{39}\). Whatever explanation is given, there does seem some uniformity among commentators that confidence in privacy protection on-line is an important part of trust in the medium in general.

If trust is closely connected to privacy, and yet privacy on-line cannot be adequately guaranteed by current legal, social or technological fixes, then the next steps must be

(i) to study what harms consumers most often suffer which they connect to invasions or breaches of security and privacy deriving from on-line activity;

(ii) to prevent those harms occurring and

(iii) if these harms *cannot, most or much of the time* be prevented, then to provide for a working and enforceable system of *rectification of, and compensation for*, those harms.

It is important as a first step then, to set out what the dominant harms to consumers are that result, directly or indirectly, from the disclosure of personally identifying information on the Internet. The principal harms may be classified, non-exclusively, and drawing omnivorously on anecdote, survey evidence, legal cases, pressure group activity and political agitation, as:

(i) *Identity theft harms*. Economic and dignitary losses arising from fraudulent misuse of personal data gathered on-line are ever more common. Most publicity relating to this type of harm has centred on credit card fraud, and as we have already seen, this is a common site of consumer worry; but this is merely itself a subset of the wider...
phenomenon of “identity theft”\(^{40}\), where data gleaned from various sources is used to impersonate a person for financial or other types of fraudulent purposes. Although identity theft is a relatively new problem in Europe, the FBI are now calling it the fastest growing crime in the USA\(^{41}\), and UK consumers are also fast becoming sensitised to the phenomenon\(^{42}\). Not all ID fraud arises from Internet activity of course. However APACS, the UK payments clearing system body, announced in March 2004\(^{43}\) that while “traditional” credit card fraud involving the production of counterfeit plastic cards was for the first time on the decline, identity theft was on the whole up by 45%, a growth largely related to “card not present” transactions, many of which of course are Internet transactions.

(ii) Disclosure harms. When personal data gathered on line is disclosed without authority to third parties, or is disclosed in erroneous form, the results can be embarrassing at best and devastating at worst. The classic example here is the much-reported incident when Eli Lilly, maker of the anti depressant drug Prozac, inadvertently revealed the full names of all the subscribers of a mailing list it ran for the users of Prozac to all the other list recipients, with unfortunate results that can be imagined\(^{44}\). Another very familiar type of disclosure harm is where credit reference agencies give out erroneous information as to a data subject, perhaps because two debtors’ identities have become confused. Such disclosure harms may principally result in dignitary loss (since actual financial losses are eventually likely to be recovered via voluntary industry schemes, mandatory schemes, or

\[\text{dc-406187}\]
insurance) but not always; eg, wrongful disclosure of health, or sexuality, or religious
details may adversely impact on current promotion prospects, affect chances of new
employment and increase the costs of relevant insurance premiums.

(iii) *Invasion harms*. What is meant here is the misuse of personal data positively to
invade what is usually regarded as the personal sphere, whether this is at home or, more
controversially, at the workplace or other public place. The leading example here is spam,
and other types of unsolicited direct marketing via electronic media, such as automated
telephone “cold calling”, unwanted txt messages, “pop-ups”, and non-consensual
downloads. The meteoric growth of spam and its harmful effects, both economic and
dignitary are now well documented. Around 62% of all email traffic was reported to be
spam in February 2004, and if a solution is not found either legal, technical or economic
to this blight, then experts forecast that the Internet may well become effectively
unuseable. Spam is the privacy harm which derives in the purest sense from the
disclosure of personal data on-line, since spammers cannot operate without list of email
addresses to spam, which are themselves of course a type of personally identifying
data. Spam and its cousins may be, and often are intended to be, vehicles to defraud, but
the category of harm can be distinguished from (i) above, since the harm suffered by the
individual consumer is usually not an economic loss resulting from fraud – since only a
very small percent of those spammed ever respond to the message contained therein –
but a dignitary loss, in the form of irritation, disgust, annoyance etc.

In all three cases, laws in both Europe and the US, as well as “code” (to apply the
familiar Lessigian tag to technological means of privacy protection such as P3P) are
currently failing both to prevent the occurrence of these harms, and to provide
enforceable remedies to the consumers who do, inevitably, suffer from these harms. This
is not a status quo from which a future leap in consumer confidence in the Internet can

46 It is true however that some spam addresses are generated randomly by computer programs.
However the majority of spammers are still using “real” addresses harvested from the Web, ISP
membership databases, etc. It is interesting to note that until the 2002 Privacy and Electronic
Communications Directive there was residual doubt as to whether email addresses were indeed
protected as “personal data” under DP law (see Edwards L. “Canning the Spam”, supra n. 31, p321) :
this now seems a settled matter.
47 Lessig L *Code and Other Laws of Cyberspace* (Basic Books, 1999)
reasonably be extrapolated. It is thus the contention of this paper that we must move away from attempting to paper over the cracks in the privacy regulation instruments with which we are already comfortably familiar, towards the more radical step of devising new models or paradigms of legal or extra-legal protection of privacy on line. In particular from a European point of view, it is crucial, if understandably difficult, that academic discourse progresses from focussing on yet more tweaks and patches for the data protection regime to looking at wholly new, or at least only partially derivative solutions to the problem with privacy. Much excellent work on DP has been done in the last five years, both by scholars and European policymakers\textsuperscript{48} – yet the evidence is that public fears about privacy in cyberspace are as intense as ever. To adapt the old joke, if we were to start regulating privacy in the on line environment today, we probably would not start here, with a legal instrument whose origins were entirely pre-Internet, designed for a pre-globalisation commercial world, where models of corporate merger and acquisition strategy were completely different, and where information was a relatively scarce and static commodity which relatively few non-state actors collected and processed in relatively unthreatening ways.

So, finally, the “modest proposal”\textsuperscript{49} of this paper’s title is an attempt to lay out the outlines of such a new paradigm. It should be regarded as more of an academic thought experiment than a blueprint; more of a Green Paper than a draft bill. Nevertheless the intention is (unambitiously!) to start a new debate about the shape the protection of personal privacy and personal information should take in cyberspace and to leave behind, at least for a while, the more derivative debates about how existing laws, can be reconfigured, to deal with problems which are fundamentally beyond their conception.

\textsuperscript{48} See \textit{inter alia} work by Bennett and Raab, Kuner, Bygrave, Carey, Charlesworth, Reidenberg and Swire and Litan cited at n 48 infra., as well as much more. The Art 29 Working Party set up the DP Directive 1995 has also closely monitored the need for changes to DP law and produced many useful policy documents. It is also worth noting the work being done in the Asian-Pacific area on building a Privacy Charter to deal with all aspects of privacy on and off line (version 1.0 circulated September 2003 by Baker & McKenzie Cyberspace Law and Policy Centre, Faculty of Law, University of New South Wales); while in theory separate from DP law, it must be noted that its draft principles bear a certain family resemblance.

\textsuperscript{49} The phrase of course originates with Jonathan Swift, whose original satirical “modest proposal” was that to deal with the Irish famine and over-population problem, Irish babies should be fattened for English tables. See Swift “A Modest Proposal: For Preventing The Children of Poor People in Ireland From Being A Burden to Their Parents or Country, and For Making Them Beneficial to The Public” (1729) , available at \url{http://art-bin.com/art/omodest.html}.
and scope. Although the details will be explored below, it seems important to stress that this is a model which is addressed less towards attempting to prevent privacy related harms - since the Internet seems by its nature to be irretrievably public and insecure - then towards providing adequate, enforceable, affordable and reassuring remedies to those who are likely to be the victims of such harms. To take a motor accident analogy, we cannot ban all dangerous cars and drivers from the roads in advance, nor control factors such as bad weather, poor visibility, lack of sleep and lack of concentration – but we can provide for adequate systems of compulsory third party insurance, negligence laws that can be enforced, and, where appropriate, no fault compensation schemes.

We shall begin by reviewing existing legal and extra-legal paradigms for protection of privacy both in the EC and the US, and summarising the major problems preventing these from working effectively in the cyberspace environment.

2. The existing European solution to the privacy problem

2.1 Data protection law

The European system of “hard” data protection (DP) laws, as opposed to “soft” law or self regulation, is perhaps well enough known not to need rehearsed again in detail here.\textsuperscript{50} European DP law demands in essence that (with certain important exceptions) consent\textsuperscript{51} be given to the collection of personal data from data subjects\textsuperscript{52}. Furthermore, those who process\textsuperscript{53} personal data (“data controllers\textsuperscript{54}”) must publicly notify the purposes for which

\textsuperscript{50} Good accounts of the differences between the US and European regimes can be found in Charlesworth, A. “Data Privacy in Cyberspace” in Edwards L. and Waelde C. eds Law and the Internet: A Framework for Electronic Commerce (Hart Publishing, 2000); Reidenberg J. “Resolving Conflicting International Data Privacy Rules in Cyberspace” (2000) 52 Stanford Law Review 1315; and Swire and Litan, supra n. XX. Bygrave L. Data Protection Law: Approaching Its Rationale, Logic and Limits (Kluwer, 2002) is an excellent recent critical account of EU data protection law with particular reference to its application (or rather, not) to (a) juristic persons and (b) personal data profiling on-line; Kuner, C. European Data Privacy Law and Online Business (Oxford University Press, 2003) and Carey, P. Data Protection (Oxford University Press, 2nd edn, 2004) are both detailed descriptive accounts of the system from, respectively, a mainly European and primarily UK perspective.

\textsuperscript{51} DP Directive 1995, Art 6 and 7 and Art 2(h).

\textsuperscript{52} Ibid, Art 2(a).

\textsuperscript{53} “Processing” is given a very wide meaning in DP law: Art 2(b) of the DP Directive 1995 defines it to include “collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination,
the data is being collected\(^{55}\) and not then go on to use or disseminate the data in ways outwith these purposes\(^{56}\). Notification of these purposes must be given to a body independent of state or commerce\(^{57}\) (in the UK, the Information Commissioner) which is also responsible for ensuring compliance with the entire DP regime. Requirements as to data security\(^{58}\) and how long data can be retained\(^{59}\) are also part of the general scheme, as is the right of the data subject to access their personal data from whoever holds it\(^{60}\), and, if necessary, correct it\(^{61}\). Special rights and duties exist in relation in particular to “sensitive personal data”\(^{62}\) and the use of data for direct marketing\(^{63}\).

This scheme is generally regarded as in principle a careful and comprehensive approach to the protection of personal data and on line privacy, applying internationally recognized Fair Information Principles. The practice has however been less satisfactory, and the rise of the Internet as a direct marketing medium has in particular revealed dismaying gaps in the tapestry of DP law, which the EU has recently tried to patch in the form of the Privacy and Electronic Communications Directive. The leading analysis of the compatibility of DP law with the new information and communication technologies (ICTs) and the globalised data flow society, despite being almost six years old, is probably still Swire and Litan’s *None of Your Business* from 1998\(^{64}\) in which the authors cogently analyse why “the challenges to the data protection regimes [of IT and electronic commerce are] immense”. The question asked there, and still demanding an answer six years on is: is data protection really a practical answer to protection of privacy in cybrspace? What are the challenges that have arisen to make DP more problematic as a regime since it was first harmonised by the EC in the 1995 Directive? And does the Directive operate to protect privacy in a substantive as well as a formal manner?

\(^{54}\) See DP Directive 1995, Art 2 (c).
\(^{55}\) Ibid, Arts 18-19.
\(^{56}\) Ibid, Art 6 (1) (b) –(c).
\(^{57}\) Ibid, Art 28.
\(^{58}\) Ibid, arts 16 and 17.
\(^{59}\) Ibid, art 6(1)(e).
\(^{60}\) Ibid, art 12.
\(^{61}\) Ibid, art 14.
\(^{62}\) Ibid, defined in art 2.
\(^{63}\) Ibid, art 11.
\(^{64}\) Supra, n 7.
History and focus of DP legislation: from mainframes to client/server

Historically, the European DP regime (or perhaps, more correctly, regimes, as the Directive is implemented quite differently in the various EU member states, and many had domestic legislation in place before the Directive was promulgated\(^{65}\)) derived from the particular historical and cultural context of Europe at the beginning of the computer revolution, and in particular from fears that the mainframe and databanking computer technology emergent in the 1970s might be used to create a Stalinist-type “Big Brother” state. The language of the Directive itself evokes mainframe technology: consider the terms “data subject” and “data controller”\(^{66}\). The origins of DP law were thus primarily to provide protection from state surveillance and data processing, with little consideration of threats to privacy from the private, commercial sector; and DP law was tailored to deal with mainframe technology, where a few large, mainly public sector, always obvious actors, who generally wished to at least seem to be law-compliant, had the sole ability to collect, hold and process huge amounts of data about ordinary citizens. Such actors – helpfully described by Swire as “elephants”\(^{67}\) - are clearly within the ambit of national jurisdiction and national enforcement authorities, usually have the funds to pay fines imposed, and are willing to comply on notice or warning rather than complete legal action. As a result, DP generally has a tendency to encourage negotiation-based settlement rather than aggressive top-down policing, and sanctions for DP breaches in the UK at least are laughably low\(^{68}\). “Elephants” are unlikely or unable to hide, run away, change name or be unidentifiable in the first place. They are susceptible to public opinion and consumer/citizen complaints, and will have an

---

\(^{65}\) See J.Klosek *Data Privacy in the Information Age* (Quorum Books, 2000).
\(^{66}\) Swire and Litan, supra n7, p 50ff.
\(^{67}\) Ibid, pp 100ff. See also Swire P “Of Elephants, Mice and Privacy: International Choice of Law and the Internet” 32 International Lawyer 991.
\(^{68}\) The top penalty for a breach of the UK Data Protection Act 1998 is currently £5,000. One of the few recent prosecutions for DP infringement in the UK resulted in a total fine of under £3,000, for sixteen offences ie £150 for each offence. The offences were committed by a debt collection agency which rang various agencies and companies illegally obtaining personal data. It is hard to see how such a level of fine could act as much of a deterrent. See [http://www.out-law.com](http://www.out-law.com), 21-4-2004. Compare the recent fines levied by the regulator for abuses of premium rate phone calls, ICSTIS, established under a later piece of legislation. ICSTIS has recently imposed several headline-grabbing fines of £50,000 to £75,000. No jail term can be imposed under the Data Protection Act 1998, no matter how serious the breach: compare the EC Copyright Enforcement Directive and the US Federal “Can the Spam” Act 2003, both of which allow for serious prison terms to be imposed in respect of “digital” offences of arguably no greater degree of moral culpitude than infringement of privacy.
internal bureaucracy including staff whose job it is to be knowledgeable about and comply with data protection hurdles and hoops (such as registration/notification). In an environment where “elephants” are the main target of the legislation, DP thrives, is practical, is affordable to enforce, and is a successful paradigm for protecting data privacy and data subject’s rights.

In 2004, the situation is very different. As Swire and Litan point out, the trend since the dawn of the Internet in 1981 has been away from the mainframe model and towards a much larger number of smaller, more decentralised computers processing and collecting personal data. The information revolution has facilitated this by producing ever cheaper computing power and chips small enough to fit intelligent processing into smart phones, TVs, watches, and toasters (to name but a few recent developments). The client-server model has to a great extent displaced the mainframe/dumb terminal model: the Web, of course, is predicated on the client/server model. Servers, unlike mainframes, are easily moveable to wherever the legal, social and financial climate is most amenable, and this is one among several reasons why transnational data flows have become ubiquitous, with attendant issues of jurisdiction, choice of law and enforcement. E-commerce has opened up transnational selling and buying to a world of retailers and consumers who would never have had the resources in the pre-Internet world to transact across national borders. Web publishing and related data collecting activities have become available to almost everyone, rather than the domain of large companies with specialised staff, and so the number of potential “data controllers” is suddenly in the hundreds of thousands if not millions, rather than tens of hundreds. “Data controllers” of this new kind – who fit into the category Swire terms “mice”, since they are numerous, fast moving, fast increasing in numbers, easily able to run away and hide and generally likely to be lacking in resources - will tend to be entirely untutored in DP, indeed may not even know what obligations it imposes, and lack access to professional expertise in the area. They will be less inclined towards legal compliance as they will in all likelihood lack a longstanding public profile and customer base, lack internal bureaucracies to deal with the paperwork (sic) of DP, be less amenable to public

---

69 See report at [http://www.pcmag.com/article2/0,1759,1130826,00.asp](http://www.pcmag.com/article2/0,1759,1130826,00.asp).
71 See further Swire, “Of Elephants, Mice and Privacy”, supra n 65.
complaints and press pressure, and be inclined to disappear, possibly to “data havens” if realistic sanctions are imposed on them (or even the threat thereof).

The effect of all this is that, as was accurately predicted in 1998: “Even within Europe, it is far from clear that a DP regime conceived for a limited number of mainframes can assure compliance in a world of pervasive personal computers. Outside of Europe, US and other website operators are even less likely to comply with the Directive, and many of these operators may remain beyond the jurisdiction of European law. Web sites will also likely be established outside of Europe to process data in ways that are forbidden by the Directive.”

The sheer size and scope of cyberspace: compliance, oversight, awareness and resources

The trends which have been outlined so far, towards decentralised data control, transnational data flows, and multiple data controllers have created problems for DP laws. But these are further aggravated by the sheer size of the Web, the enormous volume of personal data it contains, and the speed of its continuing expansion. To give some idea of the problem, the leading search engine Google currently searches over four and a quarter thousand million web pages. These figures tend to increase exponentially. Naturally many of these pages will not collect personal data. However, it is also well known that search engines cover only a small percentage of the sites on the Internet. Data controllers of the “mice” type, even those who are well inclined towards legal compliance, regularly report ignorance as to the requirements of DP law, its duties and procedures and even how much personal data they actually collect and store. The first survey by the Information Commissioner’s Office into compliance of UK websites with DP laws in May 2002, found that 42% of their sample of 170 web sites did not provide any kind of privacy statement, even though all sites surveyed collected at least some kind of personal, demographic or

---

72 Swire and Litan, supra n 7, pp 69-70.
73 Noted in April 2004. In July 2003 this figure was around 3,000 million; in August 2002, it was two and a half thousand million.
74 “Study of Compliance of UK Websites with Data Protection Law, May 2002, by UMIST for the Information Commissioner’s Office. Copies now only available on request from the ICO (see http://www.dataprotection.gov.uk/dpr/dpdoc.nsf). Sites surveyed were not chosen randomly, but to represent a range of different variable, including large and small web sites, and sites collecting certain types of information, eg, sensitive information, and information from children.
sensitive information. Of those sites that did post policies, only about 5% of privacy statements were intelligible to the average reader.75 Only 18% of sites told surfers how to access data held about them, and only 27% of sites gave any information on how to complain about privacy or misuse of data. Perhaps most worryingly, less than 40% of sites even had procedures for recording what personal data they actually held. In terms of security, only 37% of small companies had any kind of data security policy, and less than half of all companies held a back up copy of their data off-site. More recently, a 2003 survey found that although 94% of a sample of 50 FTSE 100 UK companies had notified with the Information Commissioner, only 4% could provide legally required subject access to data on request, leading to the conclusion that such companies were only paying “lip service to the law.”76

If data controllers left to themselves are unable, willing or unlikely to comply with DP law, pressure to comply might come from the public, and/or the independent regulator, the Information Commissioner, whom each state implementing DP law is bound by law to put in place77. DP law however is a peculiarly difficult area to police, even beyond the sheer size of the Web. Consumers regularly report that they do not know what legal rights, if any, they have to privacy in cyberspace and so although they clearly have concerns, they are unlikely to find out what complaints they are entitled to make and to what legal authority.78 In some cases, notably the receipt of spam, the connection of the harm caused to the origin cause (misuse of personal data) may be entirely opaque to the average consumer. Indeed, 44% of UK consumers think they have less legal protection in general when buying on line than when shopping on the high street. This is unfortunate, as given the impoverished resources allocated to website compliance (see below) one can only imagine that compliance activity must be mainly complaint directed. Consumer associations again of course have a campaigning and profile role here, as does consumer education in general. There is little impression however of consumer organisations concerned with on line

75 See p 14, NCC report, supra, n 10.
76 See study at http://www.marketimprove.com/FTSE100_Data_Protection_Study.pdf.
78 NCC report, supra n 10. To give some perspective to how careless (or carefree) consumers are about protecting their personal information privacy, a recent experiment at London Liverpool Street Station found that 71% of office workers stopped by researchers were prepared to give away their office password for a chocolate bar. See http://www.out-law.com, 20-04-2004.
79 See for example the very useful NCC publication Consumer Privacy in the Information Age, available at http://www.ncc.org.uk.
privacy having the same high profile in Europe that organisations like the Electronic Privacy Information Centre (EPIC), the Centre for Democracy and Technology (CDT) and the Electronic Freedom Foundation (EFF) have acquired in the US\textsuperscript{80}.

The task of policing data collection on the web, even if only European or UK sites are looked at, is thus not for the faint hearted. If we translate this problem into the kind of privacy harms outlined above, we find that estimates are that only around 10\% of the spam circulating in Europe actually originates from European spammers\textsuperscript{81}, with obvious implications for law enforcement. Yet in general the resources so far devoted to web compliance with data protection laws are puny. The UK Information Commissioner’s Office, for example, employs only about 250 staff of whom by no means all are concerned with website compliance. It has recently been announced that, following the dismaying results of the recent study, website compliance will be the major focus of the new UK Information Commissioner’s enforcement strategy\textsuperscript{82}. But it has to be questioned how effective such a focus can be without a huge injection of cash and manpower which the low profile of privacy activism in UK and Europe is unlikely to demand.

The globalised nature of the Internet and modern corporate business models

Even if we momentarily leave infrastructure, compliance, awareness and resource problems aside, the fact remains that Europe is not an island in the new virtual ocean. The USA is still the hub of the Internet and the e-commerce world, and most personal information about UK consumers will be collected by US based businesses, websites or servers, or the subsidiaries in Europe of such. Since the US successfully deflected fears of a trade war with the EC after the passing of the DP Directive in 1995\textsuperscript{83} by means of the

\footnotesize
\textsuperscript{80} UK organisations concerned with rights of privacy on line generally seem to get more attention when campaigning against state invasions of privacy – eg. CCTV monitoring, national biometric ID cards and Internet surveillance by national security – than they do when looking at consumer privacy. However even the anti-surveillance blog-site SpyBlog (http://www.spy.org.uk/) recently rather sadly commented that “Although there is a general lack of interest in privacy and civil liberties issues amongst the British public and politicians, we have now been persuaded to continue with this website, partly by Liberty who are now campaigning for a Privacy Act.”

\textsuperscript{81} See Spamhaus site at http://www.spamhaus.org/.


\textsuperscript{83} At issue here was Art 25, introduced for the first time in the 1995 Directive, which forbade the export of personal data from the EU to countries which did not have “adequate” data protection - notably, the USA.
much-criticised “safe harbor” compromise\textsuperscript{84}, it has shown little or no interest in moving further towards a European style omnibus legal data privacy regime. Indeed such tentative moves as there were in the direction of more not less harmonisation with Europe after the 1998 negotiations seem to have vanished in the wake of the obsession with national security at the expense of privacy post 9/11. On the commercial front, the number of companies signed up to “safe harbor” is so few in relative terms as to make it look increasingly like a dead letter\textsuperscript{85}; instead it seems that now the EC has approved a set of contractual conditions for “private export” of personal data from the EC to the US\textsuperscript{86}, this is the route of choice\textsuperscript{87} for legitimate data export, notwithstanding that the protection this gives EC consumers post-export must be questioned\textsuperscript{88}. Still more anecdotally, one suspects that small US web based businesses and especially those ever-breeding “mice” who operate on the grey legal fringes such as pornography sites, gambling sites and spammers, continue, beyond the reach of codes of conduct and EC Commission surveys, to simply ignore EC DP law.

This leaves those who would still posit DP law as a viable way to protect data privacy in global cyberspace with a number of awkward questions to answer. What is the use of having (allegedly) effective DP laws in Europe if information is transferred to, or collected on the Internet by, US based companies who are mostly not signed up to “safe harbor” or who may be using contractual conditions to avoid Art 25 proscriptions? What is the use of Europe regulating spam and cookies when 90% of spam is sent from outside Europe, and most cookies are set by US based websites and advertisers? Even if

\textsuperscript{84} See Charlesworth, supra n 48; note by six US privacy professors (Cate, Reidenberg, Schwartz, Swire and Litan) archived at \url{http://www.ita.doc.gov/td/ecom/comabc.htm}.

\textsuperscript{85} 493 members listed on \url{http://www.export.gov/safeharbor/}, visited at 28/04/04.

\textsuperscript{86} Art 26, DP Directive 1995 allowed the EC to set up model contractual conditions under which personal data could be lawfully transferred to a country outside the EU without “adequate” privacy protection. Those model clauses can be found at \url{http://www.privacydataprotection.co.uk/documents}.

\textsuperscript{87} There are in fact five legal bases for data export other than the “adequacy” of the country of destination: model contract clauses, ad hoc contracts, unambiguous consent of data subject, transfer “necessary” for performance of contract between data subject and controller and codes of conduct. See Kuner, supra n 48, pp 124 ff.

\textsuperscript{88} “Safe harbor” had if anything more explicit post-transfer safeguards for data subjects built in to the regime than does transfer of data by contractual conditions; yet safe harbor itself was trenchantly criticised on its compliance record, eg repeated scandals relating to misuse of personal data by prominent TrustE members such as Microsoft, Yahoo! and GeoCities. See supra n 82.
jurisdictional rules theoretically exist to try to deal with these problems\(^{89}\), do the resources and the political will exist to effectively enforce European rules outside Europe? This was, of course, the issue at the heart of the EU/US “safe harbor” wars, and although a partial solution was eventually reached there, it does not give this writer enthusiastic confidence that the US and its policy makers and industry lobby groups can be cajoled into moving towards any kind of full EC DP regime anytime soon. The simple fact is that US industry does not want to take on the financial burden of full DP compliance, nor does DP still fit with the model of national and international data sharing between affiliate and subsidiary companies which has evolved in a competitive and increasingly merger-and-acquisition concentrated market\(^{90}\). Both points were made strongly in a paper submitted to the European Commission in August 2002 by the Global Privacy Alliance, a consortium of major US companies\(^{91}\). Tellingly, the same points are increasingly echoed in European industry itself\(^{92}\), which is already struggling both to survive the IT recession and to catch up with the natural advantage the US has had as first nation into the e-commerce market. Kuner, writing in a text oriented towards European business practice, notes:” There have been increasing complaints by companies that European DP law is based on outmoded regulatory models and does not sufficiently take the requirements of electronic commerce into account”, and then goes on to list seven factors underlying this statement.\(^{93}\)

\(^{89}\) See Art 4 of the DP Directive 1995, para 4(1)(c) of which states that a member state may apply is national laws to a data controller if “the controller is not established on Community territory, and for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said member state, unless such equipment is used only for the purposes of transit through the territory of the Community.” Such a definition appears to catch the typical US based e-commerce website (eg Amazon.com) which sells goods or services to UK consumers and collects personal data about UK consumers using “equipment” here. “Equipment” is not defined, but is usually deemed to include conduits necessary for the “processing” such as UK ISP wires, cables, routers etc. It is less obvious if it catches, say, a US weblog site, where users in the UK write personal information straight to the US based server, since there may arguably be no “collection” or “use” and hence, no “processing” of personal data (see definition in Art 2(b).)


\(^{93}\) Kuner, supra n 48, pp 45-48.
Conceptual and harmonisation problems

Finally a problem unconnected directly to the rise of the Internet, but again, probably aggravated by it, has been a growing dissatisfaction at the degree of vagueness in the DP Directive and the consequent diversity of interpretation of key words and phrases throughout the EC member states. One of the strengths of the DP regime, given that it deals with transnational data flows, should be that at least it harmonises the law in Europe; but even this claim, it seems, is no longer really true. Debates have broken out about basic notions in the Directive such as “personal data”\(^{94}\), “equipment”\(^{95}\), and “domestic purposes”\(^{96}\); some rules are so overly broad their interpretation is wholly unpredictable; enforcement policies vary hugely from member state to state, to the extent that multinational companies operate in a sort of “regulatory limbo”\(^{97}\); and in particular, the lynchpin of the Directive, the notion of “consent”, which looks so clear on the page, is increasingly deconstructed by the realities of commercial standard-form contracts, Web click-through forms and consumer ignorance and lack of time. Consent is defined in the DP Directive to mean “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”\(^{98}\). This looks good, but begs many questions: what is informed consent? What is freely given consent? Most consumers browsing the Net who almost unknowingly tick or fail to un-tick boxes for donation of personal data on a website may afterwards feel that their consent was neither – yet such tick-boxes are the standard release \textit{de nos jours}. The crucial lobbying question of the last seven years has been whether consent to use of personal data for direct marketing needed to be given prior to such marketing – “opt-in” – or whether consumers need only be given the option to “opt-out” of such marketing after it had begun. (Naturally in the latter case, which was the minimum required by European law prior to the Privacy and Electronic Communications Directive2002, typical consumer inertia favours the direct marketing industry.) That battle has since been

\(^{94}\) Ibid, pp 49-54.  
\(^{95}\) Ibid, pp 95ff.  
\(^{96}\) See \textit{Lindqvist v Sweden}, 6 November, 2003, ECJ Case C-101/01.  
\(^{97}\) Kuner, supra n 48, pp 37ff.  
won and the 2002 Directive now requires an “opt-in” rule of all its member states\textsuperscript{99}. Yet again it has to be questioned if this is the major victory for consumer rights it has been touted as, when many consumers still report huge confusion as what they have to do to preserve rights of privacy that in any case they are not very sure they have\textsuperscript{100}.

\textbf{2.2 The US response to the privacy challenge: self regulation, “code”, PETS and P3P}

US industry is of course not immune to the demands of consumers for better privacy protection. To some extent, the growth in popularity of US trust seal schemes such as TrustE, and BBBOnline, as well as the ubiquity of privacy policies, has been driven by public and pressure group outcry as much as the need to comply with Art 25 for the purposes of European data exchange. In the US, where there is only minimal or sector-specific legislation, the norm is that privacy policies, trust seal or trust mark programmes, and industry sector codes of practice, take on the role of providing the basic framework of protection\textsuperscript{101}. A privacy policy is “a comprehensive account of the privacy practices relating to that web site that is located in one place on a web site.”\textsuperscript{102} Privacy policies have attained a fairly high profile in the USA in recent years, as a result of action by the FTC, who view the absence of a privacy policy as a pointer towards “unfair or deceptive practices” under the Federal Trade Commission Act and other fair trading legislation.\textsuperscript{103} In principle, privacy policies should allow the market to regulate privacy by presenting consumers with notice of, and choice between, a selection of more or less privacy-friendly policies which they could choose between when they shop or browse on the Web. Unfortunately there is little or no evidence that such a market in different types of policies exists, nor that consumers take account of them. As noted above, in the recent UK study on website compliance it was estimated that only about 5\% of privacy policies were actually


\textsuperscript{100} See discussion in Edwards L., supra n 31 (“Edwards IJLIT”), at pp 239-240.

\textsuperscript{101} Self regulation is well explored from a social policy perspective in Bennett and Raab, supra n 11, chapter 6; they divide self regulatory instruments int privacy commitments, privacy codes of practice, privacy standards and privacy seals. See also J. Strauss and K. Rogerson, 'Policies for Online Privacy in the United States and the European Union' paper presented at conference on \textit{Regulating the Internet: EC and US Perspectives}, 27-29 April 2000, University of Washington, Seattle.

\textsuperscript{102} See Study of Compliance with the Data Protection Act 1998 by UK Based Websites, supra n 72.

\textsuperscript{103} Privacy policies have also become more popularly known as a result of the impact of the P3P technology. See below, pXX.
intelligible in plain English terms by ordinary non-lawyer consumers. Further research in this area would be highly desirable.

A number of seal programmes and industry initiatives have developed in the US to promote good privacy practice, prominent among them the TRUSTe seal and the Better Business Bureau's BBBOnline seal. In addition to seal programmes there are also industry codes of practices which often take on board Internet privacy issues. To the forefront here have been trade associations such as the Direct Marketing Association. However, trust seals have had a bad press since the glory days of dot.com boom, and writers such as Strauss and Rogerson have often noted that industry associations involved with self-regulation, like the Online Privacy Alliance and TrustE, continue to include among their number members who have been frequently criticised for their information practices.\footnote{104} There is a pervasive worry, particularly among European writers, that self regulation is really a useful device with which to popularise the industry-friendly condition of little or no state regulation at all. As Bennett and Raab put it: “Self regulation will always suffer from the perception that self-regulation is more symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data.”\footnote{105} Since a series of well-publicised consumer privacy scandals in the late 90s and early 2000s involving prominent information-based businesses such as Microsoft, Real and GeoCities, where sanctions imposed by trust seals these companies were party to appeared minimal or non-existent\footnote{106}, the Federal Trade Commission has taken an increasingly stern approach in relation to privacy violations and made the ground-breaking declaration in 2000 that self-regulation alone was not enough for viable consumer protection on line\footnote{107}. In any case, there is evidence that since the IT recession struck, trust seal programmes are losing their client base as businesses reconsider if they are worth the cost and trouble of membership in terms of public recognition of the seal brand: TRUSTe (which was founded in 1996) had 1200 sites accredited in 2000\footnote{108}; in 2003, its Annual Report for 2002 stated that it now

\footnote{104} Supra, n 99.
\footnote{105} Supra, n 11 at p 134.
\footnote{106} See accounts in Charlesworth, supra n 48, pp 103-106; Edwards and Howells, supra n 31.
\footnote{108} Ibid.
has only “over 1500” signatory websites accredited, and admitted that both membership, sponsors and revenues were falling following the dot-com implosion\(^{109}\).

These weaknesses with privacy policies, self-regulation and seal programmes do not mean that they are all worthless, or, as Charlesworth comments “[it] would be unfair to suggest that all industry self regulatory schemes are simply conspiracies to avoid effective oversight”\(^{110}\). They can provide a useful internal educational function for trading companies, and can inspire consumers with confidence that the issue is being taken seriously. However, their lack of comprehensive industry take-up, and lack of meaningful sanctions, mean they can be viewed at best only as a supplement and not a replacement for mandatory legislation when setting the standards for Internet commerce and data privacy.

Instead, in recent years emphasis has switched to persuading the consumer that technology (“code as code” in Lessig’s terminology) can preserve privacy where law and self regulation have failed. Similar arguments after all, have already prevailed in the great Internet pornography debate, where unsuccessful or unconstitutional laws (eg, the Communications Decency Act) have largely given way to a reliance on filtering software such as CyberSitter, NetNanny, PICs and RSaci, etc. Some privacy enhancing technologies—PETS—have been under development since the earliest days of the Internet. These include software packages used to anonymise transactions such as email and web browsing by removing or falsifying headers and traffic data; “cookie cutters” used to “cut out” or block or categorise cookies; spam filters; or entire “privacy firewalls” with elements of all the above - the best known example of such being the EC Commission-recommended privacy product, Freedom, produced by Zero Knowledge\(^{111}\). These products are sometimes complex, sometimes (though often not) expensive, and most significantly, almost always not easy for the average non-technological consumer to operate. Most, it would be fair to say, are rather more commonly used by privacy activists

---

\(^{109}\) [http://truste.org/truste_annual_report.pdf](http://truste.org/truste_annual_report.pdf) In 2003 itself there seems to have been some recovery however; although the site does not admit its membership, it reports that 900 members have “returned to the fold”.

\(^{110}\) Charlesworth, supra n 48, at p 120.

\(^{111}\) See [http://www.zeroknowledge.com](http://www.zeroknowledge.com). In fact Zero Knowledge’s website (visited at 28/04/04) seems to indicate that they have re-oriented their commercial product range towards the ISP market as opposed to the savvy consumer market, an interesting observation in itself.
or “fundamentalists”, libertarians, and technology “geeks”, and their penetration into the everyday consumer world has been minimal.

P3P, the Platform for Privacy Preferences is, on the other hand, by intention aimed at the ordinary Web consumer. P3P was officially launched in April 2002, and is already incorporated into Internet Explorer v. 6 and other major browsers. It is important to note what P3P is not. It is not a “privacy firewall” of any kind - it does not block cookies or anonymise transactions or hide user data. It is not a law or a norm: it does not require a site to meet any particular level of privacy. It is simply a standard or specification developed by the international research consortium the World Wide Web Consortium (W3C). What P3P does is to read the privacy policy a site already has (or may adopt), in a standardised machine readable form. The consumer using the P3P enabled browser can set their own preferences such that sites are accepted or blocked depending on whether the site’s privacy policy matches up to the user’s settings. Future implementations may well allow the user to trade their personal information eg for micro-payment or loyalty points, as well as simply avoid non-conforming sites.

Yet P3P is in no way a satisfactory substitute for European-style DP protection. It is merely an automated bargaining mechanism, which makes no allowance for a multitude of problems including the imbalance of power between consumer and website; the general technical ignorance of consumers either as to data collection or how P3P works; the lack of a real marketplace of choices in privacy policies; and the lack of any kind of enforcement mechanism to make sure that privacy standards as stated in the privacy policy are still enforced after data has been collected. But most importantly, P3P rests on the free market idea that a consumer can plausibly bargain about what is appropriate compensation for the knowing sale of his or her personal data. This premise is here wholly false, because consumers cannot know what the value of their data is until it is

112 See http://www.w3.org/P3P/. The latest iteration of P3P, v. 1.1 was released as a working draft on 27 April 2004 so the system is still very much a work in progress.
113 For a fuller version of this argument, see Edwards (“Edwards IJLIT”), supra n 31, at pp 244-247. The EU has so far largely theoretically embraced PETS while in practice remaining suspicious of the value of P3P. However in March 2004 a 16 million Euro project funded by the EU (PRIME) commenced which intends to develop Privacy and Identity management tools for Europe to enable “end-user’s sovereignty over their private sphere and enterprise’s privacy-compliant data processing”. See http://www.prime-project.eu.org .
aggregated with data taken from all the other customers of a particular website, and possibly with sundry other databases owned by the data collector. Collation, data-mining and preference profiling is what “adds” the value to the data they give away for free, and the true value of that data as a percentage of an aggregate good is therefore unknown to the consumer/data subject, who can only reliably know the amount (usually very little) their individual details are worth alone. This is a point we will take up when devising a new model for privacy harm compensation in the final section.

3 New approaches

3.1 Assessment and ways forward

What seems to be needed is a new approach. European data privacy culture is legally sophisticated, but far too resource intensive to police, unsuited to cyberspace, inimical to modern multi-national mega-corporatism, and unacceptable to US industry in general. It is also going through an internal crisis of diverging interpretation in member states, with knock on effects on Europe wide harmonisation. Consent, the key that unlocks the right to process personal data under DP rules, is becoming a devalued and muddied concept.

US self regulation and piecemeal regulation, on the other hand, has its own well-canvassed problems. Privacy policies are ineffective unless there is a true market of policies to choose from, consumers actually read them, and can understand them, and enforcement of those policies post-data collection is taken seriously both by consumer and data collector. Sanctions imposed by trust seal organisations on recalcitrant members must be clear, transparent, respected, public and effective. Consumers should have direct rights of action against data collectors who breach the basic rules, and not have to rely on the vagaries of the FTC or internal workings within trust seals. Privacy rules, whether imposed by self-made privacy policies, trust seals or codes of practice, should remain extant and enforceable, even where the data collector goes bankrupt, is taken over, or merges with another organisation. Doubts about and flagrant breaches of many of these basic concerns contribute to the conclusion that US data privacy law, like European DP

114 Unreported civil damages court cases on “identity theft” where individual addresses or social security numbers are “stolen” put these item at almost nominal value.
law, has also failed satisfactorily to instil consumer confidence\textsuperscript{115}. And as noted above, there are also serious doubts that the brave new hope of PETS and, especially, P3P can, as yet, pick up the slack of legal regulation of on line privacy, either as alternative or addition to law and “soft law”.

Yet as Swire and Litan noted earlier, the “elephants” – the larger, legitimate companies trading on the Net – will generally wish to be compliant both with law and consumer expectations of privacy, if only to avoid bad press. Is there not some new approach which could be taken to meet US self regulatory culture halfway, perhaps in tandem with existing DP laws continuing to operate in Europe, which might provide a more internationally acceptable model for data privacy protection? Consumers too might prefer a system where it is easier to understand their rights than is the case with data protection. The emphasis of DP law on consent to data collection, is, as we noted above, in real life rather formalistic. Consent, a seemingly simple idea, is much less clear when faced in terms of opt-in and opt-out, pre-ticked tick boxes, half-buried links to privacy policies, and incomprehensible legal language. What (most) consumers seem really to want is the ability to surf the web, making the most of the convenience, choice and competition offered by Internet businesses, without suffering any of the privacy-related harms listed above, and without having to take on the onus of protecting themselves either by struggling to spot privacy tick-boxes or by using sophisticated PETS. Restricting the collection of personal data by personal “firewalls” such as “cookie cutters” also restricts the convenience of Internet shopping which is perhaps its best feature: features such as “shopping carts” and customised detail disappear, and many sites will not work at all, or rather stutteringly, if cookies are disabled. Is there not a better way of keeping the convenience factor and yet protecting the consumer from privacy harms?

\textsuperscript{115} This is not to say that the US data privacy is in real terms \textit{worse} at protecting on line privacy than the European model. Indeed, for many of the reasons listed above, although EC DP law may look as if it provides more stringent protection, US self regulation and sectoral provision may sometimes indeed be more effective at protecting consumers. This was in fact exactly the finding of a Brookings-AEI study published in 2003: however see critique at \url{http://www.enn.ie/frontpage/news-9370133.html}.
3.2 Lessons from the crisis in intellectual property

While consumer privacy has been suffering under the impact of the information society, intellectual property has been going through its own parallel crisis. In particular, the music industry has claimed vociferously that downloading and file-sharing of near-perfect digital MP3 copies of songs via Peer To Peer (P2P) networks such as Napster, KaZaa and Grokster, has reduced its profits to an extent that threatens its future survival\(^{116}\). In response, an “arms war” has developed, whereby as newer and more popular P2P networks are developed and attract millions of users, the music and film industry response grows ever more draconian. Legal action has been taken first against the software writers themselves\(^{117}\), then against “super-nodes” and sites of frequent down- and uploading such as universities, and finally against “ordinary” downloaders including such unlikely criminals as students, children and senior citizens. While this action has had partial success\(^ {118}\), it also runs the risk of alienating the very customers the music industry wishes to woo back. Technological means of protection such as copy-protecting CDs, are also (literally in some cases) likely to blow up in the faces of the music publishers. Lobbying from the arts industries has led to ever more stringent laws and decisions protecting copyright in both the US and Europe\(^ {119}\) which commentators fear are unsettling the delicate balance between economic incentive for artists and maintaining the public interest in freedom of information and expression.

Whether “home downloading” is really killing music is a debate for another place. What is relevant here is the innovative solution to the current crisis that has been put forward by William Fisher at the Berkman Centre in Harvard\(^ {120}\). Fisher agrees that downloading

---


\(^{117}\) See A& M Records v Napster, 239 F.3\(^{rd}\) 1004 (9\(^{th}\) Circ., 2001) (the “Napster” case); MGM v Grokster US District Ct, Cen D Cal, CV 01-08451-SVW, CV 01-09923-SVW, (the “KaZaa case”) at [http://www.eff.org/IP/P2P/MGM_v_Grokster/030425_order_on_motions.pdf](http://www.eff.org/IP/P2P/MGM_v_Grokster/030425_order_on_motions.pdf).

\(^{118}\) See the Napster case, supra. As Cornish describes it, Napster (as a free downloading service) collapsed due to “martyrdom by slow stoning” by the music industry. KaZaa/Grokster however, so far, survives due to a less centralised architecture. See Cornish W.R. Intellectual Property – Omnipresent, Distracting, Irrelevant? (Clarendon Press Lectures, 2004), p 52.


\(^{120}\) [http://tfisher.org/](http://tfisher.org/).
is indeed illegal as the law stands and that artists and copyright holders deserve to receive a return on their creative works. However instead of the current litigation campaign, which he views as retrogressive and unhelpful, he proposes a radical alternative compensation system for the rewarding of creators of digital music. In Fisher’s scheme, music (and films) would be released free on to the Internet but in a form which would be trackable per download (achieved using digital watermarks and unique filenames).

Meanwhile the government would, quite separately, raise money to reward creators via taxes – either direct taxes, as an add-on percentage to income taxes, or indirect, taking the shape, for example, of targeted taxes on items associated with downloading such as blank CDs, broadband access, or computer hardware. This pot of money would then be divided between the copyright holders according to their respective percentage of total tracked downloads. Once this system was in place, copyright would more or less be abandoned, so music and films would be readily available, legally, for “free” to the public, but artists would still be fairly compensated. The public would be free of the fear of being sued, and the flow of artistic work to the public would be maintained rather than locked up behind digital fences, and perhaps even increase. Society in general would benefit from the drop in litigation and transaction costs, and music would lose the extra costs added by intermediaries in the retail chain.

What useful insights does this simple and elegant idea give us on how to deal with the very different problems of on line privacy? For one, the beauty of Fisher’s scheme is that it no longer fights the tide. Instead of trying more and more desperately to hold back the flood of deliciously easy, digitally perfect copying of music, it accepts this phenomenon as something that is here to stay and which cannot be put back in its box. It embraces copying but finds a lateral way for artists to be paid. But if information wants to be free, in the famous words of John Perry Barlow, what about the lesser known corollary, that data wants to be shared? Is there some parallel scheme under which we could give up fruitlessly attempting to regulate and control the flow of data in the seamless globalised

121 Such “levy” systems have also been proposed by other writers – Netanel, Jamie Love and Peter Eckersley for example – but Fisher’s is probably the best known and most worked through proposal. Details can be found in a chapter from his forthcoming book available at http://cyber.law.harvard.edu/people/tfisher/PTKChapter6.pdf. A short version can be found at http://news.com.com/2010-1071_3-1024856.html?tag=fd_nc_1.
cyberworld we now live in, and instead attempt to compensate ordinary consumers for harms that occasionally occur as a result of such data flow?

This brings in to play Fisher’s second insight. Under his scheme, musicians gain guaranteed and fair compensation, but they lose absolute control over their creations. They must submit to what is effectively the compulsory licensing of their music, otherwise the incentive illegally to download on the “old” P2P systems persists and the new scheme will not operate fairly. Under a scheme which allowed data to flow, but compensated data subjects if harm resulted from that flow, data subjects, it seems, might similarly have to give up the “right to control what is known about them”, a right which is sometimes seen as a fundamental part of the definition of privacy. However this need not be so: just as artists who truly wish never to lose control of their creations might refuse to release them except in encrypted form, so data subjects who wish to maintain as tight control as possible over the “unwanted gaze” of the world on their data, might make use of the kind of PETS we described in the last section. Only a few “privacy fundamentalists” might want to go to the effort of using full-scale PETS, but as privacy is a fundamental human right, their views cannot simply be disregarded just because they are not shared by the majority. Thus, we will come back to this point of the availability of PETS in the model described below.

Finally, Fisher’s third key insight is that the compensation justly owed to copyright-holders in his example, and data subjects who suffer harm in our ours, need not come directly from the traditional sources of that revenue. Instead, in his example, enforcement of copyright can be abandoned; in ours, traditional forms of data protection law can be abandoned. Instead, in both cases the compensation “pot” comes from a tax that seems just and appropriate and which is fairly applied against those who should pay the money. In the domain of data flow, the people who are making money out of the collection of personal data are the data collectors and subsequent data processors. (From here on in

122 Although the element of total “control” is not essential to privacy according to some writers, notably Ruth Gavison. See discussion in Wacks’ introduction (p xi) to Wacks R. ed Privacy (Dartmouth, 1993) drawing on ideas in his earlier book Personal Information: Privacy and the Law (Clarendon Press, 1989).
123 See Rosen, supra, n 36.
124 See Bennett and Raab, supra n. 11, p 62, deriving the term from Westin.
this section, the phrase “data collectors” will be taken to embrace both categories.)
Consumers give away their personal data all the time on the Net, partly out of ignorance,
partly because they often have no way of preventing the data being collected, but partly
also because they sense that individually that data has little or no value. However in the
hands of data collectors, and their colleagues, the data miners, that data in aggregate
becomes an asset of considerable worth. Essentially, this is an asset acquired for free. It
seems quite equitable then, that data collectors should pay some of their profits acquired
through data collection into the “pot” out of which compensation for privacy harms can
then be paid. It will be said that this is an unwarranted new tax on a specific industry
sector, and a tax on e-commerce at that. But the tax in Fisher’s proposal is also a new tax,
and it is a tax on the public, whereas I am proposing a tax on a sector of industry which is
currently effectively making stealth profits at the expense of much less powerful and
informed consumers. It seems hard to argue that such a tax cannot be justified, especially
given the history of uncorrected and uncompensated privacy harms which has
accumulated over the last five years or so of Internet trading, profiling, spamming and
advertising. Such a tax would certainly be unpopular with Internet traders, ISPs,
publishers and the rest of the relevant data collectors (although see some of the
sweeteners for them discussed below at p 39); but that is not the same as saying it is
either inequitable, unwarranted or impractical.

3.3 The “modest proposal” - from trust model to “privacy tax”

Intellectual property and alternative compensation systems are not the only place we can
look for inspiration if we are looking for new models with which to compensate for
“privacy harms”. Throughout this article it has been asserted that data collectors and
processors accumulate an aggregate asset of substantial worth – databases of customer
personal information and preferences - which is cumulated from the individual data of
shoppers given away almost always unknowingly or without informed knowledge of its
potential value. When we talk about the equitable management of an asset that is created
from the gifts of multiple small contributors, but which forms an item of substantial
worth only in aggregate, then historically, at least in common law jurisdictions, the legal
institution used to manage such an asset has been the institution of trust. In a pension or
superannuation trust, for example, many workers contribute to a trust fund which eventually pays a dividend or beneficial interest to each pensioner at the date of retirement, departure or death. In a strike fund, much the same approach is taken, with contributions to the trust fund coming from strikers, unions and supporters. Secondly, the institution of trust, as discussed below, involves in essence the making of a gift by the trustor to the beneficiaries via the trustees who hold the trust assets for some interim period. A trust is not a contract; it is a species of donation. Thus, using trust as our legal model may take us away from the problems mentioned above, which dog data protection law, as to what “consent” is in data collection and processing. If we turn to a trust-like model, we can imagine a regime in which data is given away freely and yet data collectors and processors still owe duties of care and trust to data subjects; just as in Fisher’s scheme, music is given away freely and yet payment is still owed to creators or copyright holders. Such a scheme, where use of data is divorced from the traditional pass-key of consent, is far easier to manage, and less likely to become litigative, than one where arguments break out all the time about what “consent” is; or in the IP parallel, whether some right to evade or not pay copyright exists, such as fair use, fair dealing, parody etc.

Let us turn then to considering what shape a model might take which seeks to absorb all the above insights and implement them in some kind of working alternative to current paradigms for data privacy protection. A lateral approach, as we have already hinted, might be to compare data collection on the net to the common law trust. Trust is essentially a kind of protracted gift, an institution whereby property is transferred by the trustor(s) (or settlor(s)) to the trustee(s), who have formal ownership of the trust assets, but whose use is restricted by a continuing set of trust purposes, and by the beneficial interest of the beneficiaries. The trustees owe fiduciary duties, including a stringent duty of care set at a far higher standard than the normal negligence standard, to

---

126 See Figure 1.
127 In Scotland, being a mixed system with strong Continental influences on its property law, the right transferred to trustees is the real right in the trust assets – dominium. However in pure common law systems, the right trustees have over the trust assets may be an interest less than absolute ownership, although it is common to say that trust property is “vested” in the trustees. As is noted above, whichever approach is taken, the rights trustees have are in any case limited by trust purposes, and the interests of the beneficiaries (and possibly by other parts of the law).
the beneficiaries. In an *inter vivos* trust, with discerned beneficiaries, the beneficiaries have the principal title to enforce trust purposes. In other cases, such as public or charitable or discretionary trusts, where, eg, the truster may be dead or absent, or the beneficiaries may not yet be discerned, an enforcement role to prevent abuse of trust is usually taken by some kind of state body, such as, in England, the Charities Commission.
Compare the situation when consumers shop on the Internet. Personal data is given away by the data subject/consumer to the data collector/website, who holds that information and makes money out of it by selling it, sharing it or using it better to market or target their products. What if the data subjects were seen both as the trusters and the beneficiaries of a trust, and the data controller/website as the trustee? That would imply that the trustees owed fiduciary duties to the beneficiaries who would have title to sue for damages and to enforce them. It would mean that the data collected, or perhaps more usefully, just the profits derived from its collection and/or processing, formed the trust property. (How “profits” will be defined is of course a topic that will need further detailed discussion.) It would also mean that the question of “consent” and all its difficult nuances would become irrelevant, as all transfers of personal data would be assumed to be gifts, though made in the knowledge that the assets gifted did not become the absolute property of the data collector.

128 See Fig 2. It is perfectly legal in most if not all systems that have trust, for a truster to also be a beneficiary, so long as there is at least one or more third party trustees: see eg Gardner S Introduction to the Law of Trusts (Clarendon Press, 1990), p 3.
What are the potential benefits of this elaborate model or thought experiment? At least three key ideas come through strongly, even at this preliminary stage, if the trust model is accepted in some form:

(a) the data subject as beneficiary of the trust is owed a share of the profits made by the data collector from the collection of data. This is perhaps the most controversial and the most exciting result of the trust model. Currently neither the European nor the US regulatory models acknowledge that an asset of considerable value is being amassed by the data collector/website. Both models, less or more successfully, simply try to give the data subject the option to opt out of data collection at the start, rather than the option to opt in and gain a share in the proceeds deriving from data collection. P3P, as discussed above, is a form of automated bargaining mechanism, and thus, interestingly, does (i) accept that data on the Net has become a propertised and tradeable commodity, and (ii) tries to provide a rough framework for that trade – but because each consumer individually trades their data, no consumer can bargain for the true value of what
they have given away. A trust model – where personal information collected (or the profits derived therefrom) would be seen *in aggregate* as the jointly owned trust property – allows all data subjects/beneficiaries to make a claim on an asset of considerable value. As we shall discuss below, this aggregate asset might also provide the kind of “pot” of money which in Fisher’s example is raised by taxation, and which in our example, could be used to compensate for privacy harms. In effect, what we are proposing is a kind of “data” or “privacy tax”.

(b) It is clear that data collection is *not just* for the benefit of the data collector but that the data collector holds for the benefit of the data subject/beneficiary. In the context of this thought experiment, this clearly should not mean that the data collector need hand over all the profits that are made from data to the data subjects; but it should mean that the data collector acts in the interest of the data subject and not against them, by, for example, being deliberately privacy invasive. More precisely, in trust law, a trustee owes stringent duties of care to the beneficiary. These could be replicated as the duties owed by data collector to data subject. The exact scope of the duties can (and should) be debated eg, should it include the duty to keep that data secure and not to negligently disclose it. Indeed the duty not to disclose without consent might be construed as strict. However the key point is that a high duty of care would be implied at common law.

(c) This duty of care owed by data collectors, would under trust law, also be enforceable by each beneficiary. As a corollary, in the data trust model, the data subject would be given an *individual right of action* against an abusive data collector, something which at moment is almost wholly lacking from the US model (barring the dubious possibility of enforcing a privacy policy as contractual terms)\(^{129}\). Extending the trust model, it would be possible to give the data subject the right to demand what English law calls an “account”\(^{130}\), ie, to ask the data collector what data they held and more importantly, what they had done.

\(^{129}\) There are no individual data subject rights to enforce under safe harbor, nor under most, if not all, seal programmes. Enforcement is a matter for the FTC and therefore subject to their own internal priorities and resource issues. See further Schachter M. *Informational and Decisional Privacy* (Carolina Academic Pres, 2003), p 199 ff.

\(^{130}\) See Gardner, supra n 126, p 216.
with it and what profits they had made out of it. It needs debated, however, if this is desirable, given the emphasis in this model on reduction of bureaucracy for the data collector, an empirical background of lack of uptake of subject access rights by data subjects in existing DP law, and the aim of the model which is to transfer legal attention to compensation for external harms caused, rather than to regulate the “indoor management” of the data collector’s operations.

So far, we have reconceptualised data subjects as both creators and beneficiaries of a “data trust”, and data collectors as trustees. Under this model, data subjects give away their data for free, and have no rights, legal anyway, to give or withhold their consent to data collection. Thus, “consent” and its irksome nuances of whether sufficiently “informed” or “free”, becomes an irrelevant concept. Furthermore, just as Fisher abandons copyright law once he has up and running other, more practical and less avoidable ways of rewarding creators, in this model, DP law, at least as mandatory law, would also be abandoned, since now we have to hand a better way to compensate data subjects who suffer privacy harms. This “better way” comes in the form of the trust assets we now have available to benefit the data subjects. The trust assets, if we recall, are the profits derived in aggregate from data collection. Applying a “privacy tax” model, the trust assets need not be all of the profits but some reasonable percentage thereof. (This would make it rather more attractive to the data collectors, who, obviously, also need to make a profit.) How should this “privacy tax” best be used to benefit data subjects?

The simplest solution, and that most analogous to how an ordinary trust works, would be to distribute the trust property, in each “data trust”, to all consumers who had given away data to that data controller, based on, say, on their time spent on line at that site, or number of visits to that sites, or amount of data revealed. This however would require monitoring and identification which would itself be heavily privacy-invasive. Furthermore, the transaction costs involved in monitoring all the websites each consumer

---

131 However they may have technological means to withhold their data from data collectors: see further below.
132 There is no reason why it could not be retained as an excellent voluntary code of practice for certain organisations or industry sectors. Common law rules as to negligence and invasion of privacy torts or delicts would of course remain in place.
visits, and distributing small amounts of money to millions of consumers would be wholly prohibitive. There is no evidence furthermore that what consumers want in return for giving up their privacy is small change: what they would prefer instead, it is asserted, is protection from, or, failing that, compensation for, the privacy harms described in the introduction. It is proposed therefore that the trust assets of all “data trusts” should be combined in one large pot or fund – effectively the proceeds of the aforementioned “privacy tax” on data collection - which could then be used to do (at least) three things:

- **Provide for statutory set levels of compensation for privacy harms.** Here we refer back to the discussion of the types of privacy harms in the introduction (identity theft harms, disclosure harms, invasion harms). The scheme here envisaged is one of public compensation, and is based on the idea of no-fault compensation in tort. It may be said that there is no need for such a scheme as victims of privacy harms already have common law rights of action against privacy tortfeasors in most jurisdictions. But negligence actions, or ordinary actions for invasion of privacy, are necessarily dependent on showing that a duty of care was owed to the victim; that a causation trail can be established between the person who owed the duty and the victim who suffered harm; that there was no intervening factor which broke that chain; and (in many jurisdictions) that the harm suffered caused some more than nominal economic detriment which can be reliably quantified. Almost all of these factors are extremely difficult to establish in respect of many privacy harms, especially spam. Spam is intensely annoying and distressing for many consumers to receive, and is almost certainly the result of their having at some point given away personal details to a data controller which a spammer has later acquired; but it is almost impossible to identify which disclosure to which data controller lead to the receipt of a particular spam mail; even more difficult to establish if that data controller was negligent in allowing a spammer to (say) harvest their public directory of user email addresses. In a no fault scheme, there would be no need to worry about any of these factors. The data subject spammed, would merely need to establish that they had

---

133 See pXX.
suffered a harm caused by a prior breach of their information privacy, and the compensation could then (it is suggested) be set at statutory levels, based simply of number of spam received (with a limit threshold to prevent nugatory pay-outs?), or more sophisticatedly on content, distress or damage caused, and context (eg, age of recipient). There is plenty of experience of setting statutory levels of damages when claims are made by ISPs against spammers\textsuperscript{134}; there seems no reason why this knowledge of what spam usually costs should not transfer to compensation payouts to individual consumers, adjusted as necessary to remove the punitive element. However it would still of course be open to (and desirable for) a body such as the FTC to pursue individual companies to improve data security practices (and see the point below on fundibg better enforcement). Existing negligence law and liability for fraudulent breaches of data security should therefore persist in this domain even as mandatory DP law is abolished.

- **Improve enforcement.** Top-up funding could be provided to an existing regulatory, public and independent body concerned with safeguarding consumer privacy, such as the FTC or the Information Commissioner in the UK, or if none such existed, a wholly new body, in each state, which could provide the public oversight and enforcement of private rights necessary in a consumer area. This would help meet the crisis of resources for enforcement of privacy in cyber space which is referred to in the earlier critique of data protection law\textsuperscript{135};

- **Provide PETs to privacy fundamentalists.** Here we refer back to those consumers (or perhaps more appropriately, citizens) who under no circumstances wish to give away their personal data. This ties in with the point made above that it is a breach of fundamental human rights to force the unwilling to give away their data privacy. Most consumers, it is imagined,

\textsuperscript{134} See several US state anti spam laws, and most recently, the federal “Can the Spam” Act 2003 in which both basic and aggravated damages when spammers are sued by either ISPs or the government are laid out in detail.

\textsuperscript{135} See pXX.
will be happy with a regime where they, in most cases, continue to act exactly as before but have new access to decent enforceable compensation rights when privacy harms occur. However this will not do for a small hard core of “privacy fundamentalists”. Their concerns can be met by products such as the Freedom privacy “firewall” software being provided free for download to all who wished it, with the licence being paid out of the data trust “pot”. Money from the trust pot might also go to fund better development of PETS that are more accessible to non-technophiles and consumer-friendly, as this seems to be lacking in the market.

Two additional comments on the possible benefits of this scheme can be made. First, it is helpful that, in providing remedies to consumers for privacy harms, the “privacy tax” targets, in Swire’s neat phrase, the “elephants” not the “mice”. Although privacy harms by big companies like Eli Lilley and Microsoft Passport receive massive publicity, most privacy harms are in fact perpetrated by the small players, a.k.a., the “mice”: for example, spammers, who are hard to track down and even harder to sue; small companies who have little or no expertise in either law or information security; individual domestic websites that give away vital personal details of a person’s life. It is unreasonable and inefficient to expect ordinary consumers to track down and sue such “mice”. Instead it makes sense for individuals to recover from a public compensation fund to which contributions are made by “elephants” and, one hopes, also as many “mice” as possible. Of course, it would not be desirable either for the sins of the “mice” to be entirely paid for by the funds of the “elephants”. But it should be possible – as discussed above – for public enforcement bodies, now properly funded, to go after recompense from a reasonable percentage of “mice”; and it will also remain possible for the “elephants” to undertake their own litigation to seek compensation back from “mice” where those can be identified and tracked down and there is a causal relationship between the privacy-invading acts of the “mice” and the loss to the “elephant”. So, for example, it is envisaged that the major ISPs, who currently undertake a great deal of the litigation against spammers, would continue to do so, for all the reasons that currently apply, plus the new incentive to reduce the total number of privacy harms that needs to be paid for by the privacy tax.
This leads to the second point, which both anticipates a criticism of the “privacy tax” scheme and suggests another long term benefit. The scheme described here is in many ways a standard no-fault compensation scheme in which relevant industry players pay into the compensation pot, rather than the fund coming solely from government or general taxation funds. It is often argued that such schemes are unsuccessful in policy terms, since they do not encourage the paying contributors into the fund to improve their practices, as no matter what they do, they will end up paying – for their competitors’ lapses in good practice, if not their own. Will data collectors who pay into the “data trust” under the existing scenario cease to maintain even what safeguards for customer data privacy they already have in place? This would not be a good outcome. However the “trust model” does not need to be set up that way. All data collectors should certainly pay into the central pot since all make money out of data collection. So far we have assumed that the tax paid would relate directly to the profits made by each data collector out of the data they gathered/processed, and no other factor. But it would not be difficult to relate the percentage tax on their data profits to, say, the number of privacy harm complaints made, or proven, against them in the preceding year. In this way, the rate of tax, initially set at a level playing field for all, would be adjusted in rather the same way that motor insurance premiums are depending on the number of accidents or claims involving the insured. Accordingly, the advantages for the data subjects of a no-fault compensation fund can be combined with the advantage of a standard negligence model, namely that there is a real incentive to data collectors to improve their privacy practices.

The other recurring problem with no fault compensation schemes is, of course, the fear of free riders who will leap on board the gravy train and render the fund bankrupt before too long. Although the possibility of this cannot be discounted, it is hoped that keeping the list of privacy harms which justify pay-outs to a fairly solid and concrete level – as discussed at p 8 – with some limiting threshold on, in particular, the degree of harm caused by spam that has to be reached before a pay-out is justified - will prevent this particular tragedy of the commons arising. Also, as the “elephants” adjust their privacy practices, and the “mice” are tracked down, in due time, the drain on the fund itself should diminish.
But why would the data collecting and processing businesses – the “elephants” as well as the “mice” – go along with such a scheme? Why would they accept what is effectively a new “privacy tax” taking away a percentage of what so far they have kept for free? What, we may crudely ask, is in it for them? There are a number of plausible answers.

First, for European industry, and industry outside Europe who wish to legally transfer data from Europe, there could be a tremendous reduction in bureaucratic overhead. Data protection is fiddly, costly, boring, requires intensely specialised expertise, is different in every EC country and is, off the record, cordially hated by most captains of industry. As noted above, it is counter-opposed as a practice to the modern data sharing that is a crucial aspect of the information-intense industries we have now developed, and it involves data audits and data management of a kind that very few companies, whether huge transnational conglomerates, or the new “mice” of the e-commerce industry, find helpful or easy to manage. The new “trust model”, however, is one that concentrates on the external effects of data collection and processing - obvious harms that result - and as far as possible, ignores what in company law is often called “indoor management” or internal bureaucracy. Under this model, subject access requests, for example (which are in any case rarely used, and at that mainly in odd cases like dismissal disputes, rather than real privacy cases) would disappear, as would rules on data retention and worries about consent, opt in, opt out and legacy databases when the law changes.136

Secondly, public awareness that industry was actually paying out money to provide compensation for privacy related harms would be a massive public relations bonus (particularly if it was downplayed that that money had actually come from the consumers in the first place). Such an act in itself might do more to improve public confidence in using the Internet for e-commerce than DP law, TrustE and P3P combined have managed over the last five years. As discussed above, this could only be good news for the dot.com economy, especially in Europe. It would also of course, be good news for society, and indeed, for consumers.

136 The latter has been a conspicuous concern in the UK during the introduction of the change in the law from “opt out” to “opt in” under the new PECD 2002 rules on databases and direct marketing.
Thirdly, the idea of trust is itself both a harmonising and a reassuring principle. Trust is an institution which is best known in common law Anglo-American legal systems but which is also found in most Continental systems. Major efforts are currently being made in European property law to use trust as a bridge between the common law systems of England, Scotland and Ireland and the civilian systems of the rest of Europe\textsuperscript{137}. A system to protect data privacy founded in an institution like trust might enable a sort of working rapprochement between EC and US notions of privacy protection which so far has eluded negotiators. The notion of “trust” itself, it is perhaps naively thought, might also contribute to greater trust and confidence in the general population of consumers.

In conclusion, this is clearly at present merely the beginnings of an academic modest proposal with, as can be seen, many details still to be worked out for which there is no space here. However, it is asserted that we need to start thinking seriously about alternatives to the current stalemate in legal debate between the advocates of principled, but impractical European DP law, \textit{versus} the defenders of ineffective and likely to stay that way US privacy protection. We also need to build systems for privacy protection which recognise that while consumers deserve to have their privacy protected, they also need and want to retain the convenience factor that goes with sharing a great deal of personal data with e-commerce sites. Looking beyond law to “code as code”, neither privacy technologies such as P3P which presents a façade of consumer control that is ultimately misleading, nor more serious PETS which do allow such control but are inaccessible and inappropriate to ordinary consumers, are the way forward either. A compromise and a fresh eye to possibilities are required.

\begin{footnote}
\textsuperscript{137} See discussion in the (2000) 8 European Review of Private Law special issue on European trusts.
\end{footnote}