Arts 6-7, ECD; Privacy and Electronic Communications Directive 2002

Canning the Spam and Cutting the Cookies: Consumer Privacy On-Line and EU Regulation

Lilian Edwards[1]

This chapter deals with the new European and UK laws relating to the control of "spam" and "cookies". Spam is best defined as unsolicited junk email (though see below), while cookies (or "web beacons") are small text files placed on the hard disc of a computer user, usually without the consent or knowledge of that user, and used extensively on e-commerce sites to store data records about that user's transactions for purposes of profiling and marketing[2]. To understand the current regulation of spam and cookies and how European law has altered the shape of this area, we need now to extend our reach beyond the principal focus thus far in this volume on the Electronic Commerce Directive (ECD), to look at subsequent European laws. The provisions found in Arts 6 and 7 of the ECD relating to unsolicited (and solicited) commercial communications are only one piece, and at that now of somewhat limited significance, in a much larger jigsaw of regulation.

Spam and cookies, as we shall see below, raise important questions about privacy invasion and consumer protection. Spam in particular however creates more purely economic problems in the domain of e-commerce and the global Internet, of significance to the public interest as a whole, not just to consumers. Thus global spam regulation, of late, has begun looking at ways to preserve the Internet as a whole from collapsing under the deluge of spam, rather than merely attempting to protect individual privacy and consumer rights[3]. In Europe however, regulation in this area has to date, and is indeed still, been embedded in the traditional sectors of data protection and consumer law. It has been a piecemeal affair, taking bites from the general law of privacy and data protection, moving through a guest appearance in the E-Commerce Directive and taking star billing in the controversial passage of the

[1] Co-Director, AHRB Centre for Intellectual Property and Technology Law, Edinburgh University, Parts of this chapter appeared in a much earlier form in Edwards L. "Canning the Spam: Is there a Case for Legal Control of Junk Electronic Mail?" in Edwards L. and Waelde C. eds. *Law and the Internet: A Framework for Electronic Commerce* (2000, Hart Publishing). I am indebted to all at the Centre for Law and Technology at the University of California at Berkeley, where research for this chapter was carried out.

[2] See further http://www.allaboutcookies.org .

[3] A good example of this is the US Can-Spam Act, which combines traditional rules protecting the privacy of recipients of spam with rules aimed at merely reducing the amount of spam in the world, eg, forbidding the use of third party computers

Privacy and Electronic Communications Directive 2002 (PECD)[4], which is the first EC Directive where the question of how to regulate cookies is directly addressed. We will deal below with spam and cookies in turn, considering also, given the global nature of these problems, what solutions to these problems have been found in the United States, from which most worldwide spam emanates.

Spam

Few Internet users will not at some point have received an email message of the following kind:

> *Subject:* **you forgot the attachment**
> *From:* "ExtremePriceCuts.net" <extremepricecuts@extremepricecuts.net>
> *Reply-to*: no-one@microsoft.com
> _____
> From nothing to rich in 90 hours!! I cracked the Code! I made over $94,000!!!!!
> You May Be Closer (Maybe Hours Away)
> To Financial Freedom
> If YOU Needed $24,000 In 24 Hours
> And your life depended on it…
> How Would YOU Do It?
> http://www.esioffers.com/track_link.html?link=3664

Such unsolicited or "junk" e-mails are colloquially known as spam[5]. They are usually sent out to thousands if not millions of electronic mailboxes simultaneously, most often for dubious commercial purposes, though some are also sent by private individuals for non-commercial purposes, for example to spread racist or homophobic hate speech or for political or religious campaigning purposes. Spam can often be casually spotted by its use of multiple exclamation marks and capital letters (the Internet equivalent of shouting), or by enticing subject lines such as "get rich quick" or "hot sex here" (although recent iterations of spam tend most often to

as "zombie drones" to send out spam. See further *infra*.
[4] Directive 2002/58/EC.
[5] The name "spam" is, as a matter of Internet urban myth, supposed to derive from a well known Monty Python TV comedy sketch involving the chanting of "spam, spam, spam" over and over again. Spam is of course, originally a trade

disguise its true nature in the subject line in a bid to up the "click-through" rate, ie, to induce the reader to open it). Although most often found in the context of email, and Usenet newgroups, websites (such as the very popular web-log or "blog" sites[6]) can also be spammed, and for this reason LINX, the London Internet Exchange, and may other leading spam-blocking sites[7], have suggested the best description would be "unsolicited bulk material" or UBM. This type of nomenclature also places the emphasis on the *bulk* in which the spam is sent, not its *contents*, fraudulent or otherwise, which as we shall see below, is a crucial point for would-be regulators of spam to note. Beyond the sheer question of bulk, it is not easy for an automated process to determine which are "genuine" marketing messages and which are what is commonly regarded as "spam" - for example, to distinguish between 10,000 emails promoting a Nigerian bank fraud scheme and 10,000 emails encouraging alumni of a major university to make tax-deductible gifts to that university. The presenting features of the *content* of spam are that they tend to advertise goods or services the recipient has not actively sought (typical examples being pornography, get rich quick schemes, pyramid selling schemes, "phishing" emails[8], dating agencies or software with which to become a spammer yourself); they are often misleading or outright fraudulent; and they are very often offensive, obscene, disgusting or illegal in content. Crucially, spam arrives without the consent of the recipient - hence "unsolicited". The leading spam country of origin is overwhelmingly the US currently, though it is hotly pursued by Far Eastern countries such as China and South Korea as spam havens[9]. Significantly, in late 2004 only two EC countries were in the top 10 spamming countries (Italy and the UK at 9 and 10 respectively) and by February 2005 even they had fallen out of the ranks. It is a major problem for law enforcement, further discussed below, that the majority of spam that circulates in EC countries (estimated at 90% or more) comes from outside Europe.

---

marked term for a form of canned luncheon meat.

[6] The Mel Gibson directed film "The Passion" (released February, 2004) is noteworthy as the first Hollywood film to be promoted by an extensive spam campaign on weblog websites such as Live Journal. It is though the main aim of that campaign was not to spread the word (sic) but to up the Google page rankings of "The Passion" as viewings of blog pages contribute significantly to how these are worked out.

[7] Spamhaus, the UK based private spam filtering organization, which claims to serve up to 200 million Internet users, note that: "The word Spam means "Unsolicited Bulk Mail". Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content. But ask a spammer and he'll claim it's something else… The content of span is and always has been irrelevant. If it's sent unsolicited and in bulk, it is spam plain and simple." See http://www.spamhaus.org/

[8] "Phishing" entices the recipient to go to a fake site imitating a known banking or financial site and to there enter a password or other details. The aim of the scam is to give the fraudsters access to the recipient's details so that fraud can then be committed at the authentic site. Recent UK "phishing" scams have afflicted customers *inter alia* of Lloyds Bank, the Royal Bank of Scotland and PayPal.

[9] The top ten spam origin countries as of February 2005 were USA, China,South Korea, Russia, Brazil, Canada, Taiwan, Japan, Argentina and Hong Kong. Earlier montbs have included EU countries such as UK and Italy at the lower end of this chart. See Spamhaus, supra n 7.

Prior to 2000 or so, there was very little *legal* debate on how spam could, or should, be controlled in Europe. By contrast argument raged among "techies" as to the best technological methods for controlling spam. When spam was still little more than a joke and a minor annoyance to consumers (and lawyers) in Europe, it was already becoming a major concern to network managers and system operators. In the US, always ahead in Internet litigation, running battles commenced in the courts between spammers and those who longed to stamp out the practice - notably Internet Service Providers (ISPs) - in the mid to late 1990s, and a flood of individual state statutes subsequently attempted to grapple with the problem in various ways[10]. More recently, a Federal statute has, after many prior attempts, finally passed which prescribes a uniform approach to spam regulation for the entirety of the USA – the CAN-SPAM Act of 2003[11]. UK and European interest, meanwhile, has increased in direct proportion to the increasing amount of email that is spam – spam in Europe has grown from only 7% of global email traffic in April 2001 to at least 50% of EU email traffic at January 2004[12], while some extents put the proportion of spam in email as high as three-quarters of the total in the run up to Christmas 2003. In the US, estimates vary but go as high as over 80% of all email traffic probably being designated as spam. At these levels, spam is not just an annoyance to users and service providers, but is on the way to making the entire Internet effectively unusable for those without highly effective filters in place. Since spam is also now frequently used as a delivery device for viruses, worms and distributed denial of service (DDOS) attacks it is not uncommon to view every spam email nowadays as a "ticking bomb".

More broadly, the European Union has clearly espoused the view that development of consumer confidence in the Internet as a commercial medium is dependent on consumer and retailer trust, and both spam and cookies are key problems which persistently remind users that the Internet has not yet attained the status of a safe and known environment. Accordingly, spam, once a matter of joke and urban legend, and cookies, of which most Internet users have still probably never heard, have become some of the most pressing issues for modern e-

[10] See David Sorkin's useful inventory of spam laws at http://www.spamlaws.com/ .
[11] This is the informal title of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. The Act passed on November 25 2003 and came into force on January 1 2004.
[12] See EU press release, IP/o4/103, 27 January 2004. A variety of industry based pressure group in Europe are dedicated to the fight against spam, including E-CAUCE, the European Coalition against Unsolicited Commercial Email, web site at http://www.euro.cauce.org/en/index.html . A useful US and Europe based anti-spam site is Junkbusters at http://www.junkbusters.com . Spamhaus, see n 7 above, are a useful source of technical information and statistics: the European Commission also provides up to date information at its www.europa.eu.int pages under Information Society head.

commerce legislation to grapple with all over the globe[13].

Finally it is important to note that legislation in this area is an ongoing process as new types of privacy-invading technologies are invented. Cookies are by no means the end of the story: the PECD also attempts to grapple with the privacy implications of collection of traffic and locational data, which are increasingly likely to be used as means of targeting novel "value added" commercial services at consumers. Most recently, the RFID - Radio Frequency Identity - chip, which reports back its whereabouts like a small microphone bug to nearby electronic readers, has made the leap from laboratory to shop floor and is currently stirring controversy as major High Street retailers and large distributors and manufacturers start to use it to improve efficiency and reduce costs, but at untried risks to privacy. Despite the often–made claims of the EC that it attempts to draft e-Directives in a technology-neutral fashion, it is quite probable that even fairly new legislation such as the PECD and the UK implementing Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the UK PECD Regulations")[14], are already out of date[15]. Do we need new legislation every time a new privacy invasive technology is invented and if so is there any hope that the law will not always lag futilely behind the potential harm created by the new privacy-invading technology (PIT)? One answer may be to use technology or "code", not law, to effectively restrain technologies harmful effects; and in the final section of this chapter we will consider if legal regulation in this domain is not increasingly an irrelevance and even a distraction from the real solutions which may lie in the domains of technology and economics.

Why is spam a problem, and whose problem is it?

As noted above, the historic response to spam before the turn of the century was to regard it as a nuisance, and perhaps to take self help measures such as "flaming" (sending abusive emails to the spammers) - but not to see it as a fit subject for legal or extra-legal regulation. However a number of factors have conspired to make spam, as noted above, a phenomenon to take very seriously indeed.

"Living persons" as victims of spam: offence, annoyance and invasion of privacy

[13] See n 9 supra and further below.
[14] SI 2003/ 2426. The Regulations finally came into force on 11 December 2003 following an extensive consultation exercise by the DTI.
[15] See for similar concerns in the field of e-money regulation, Guadamuz A. and Usher J in Chapter X of this volume.

Most obviously, much spam is annoying, objectionable, distasteful, and in some cases, deeply offensive, to its recipients. Furthermore, traditional direct marketing was usually only directed at solvent adults, while spammers will indiscriminately spam children and other vulnerable groups so long as they have an email address[16]. Spam also now appears in so many media that it is omnipresent both at home and at work. Spam that came as email was bad enough, but in the brave new world of the twenty-first century, unsolicited marketing also arrives as texts to mobile phones, spontaneous downloads to desktops, executable attachments alongside email spam which unknowingly plant viruses and spyware, and perhaps worst of all, "pop-ups", windowed advertisement exploiting bugs in Windows soft ware, which obscure the user's desktop, arrive incessantly to some unlucky users, are difficult to close, endlessly repetitive, and sufficient to incite "spam rage"[17] in the meekest of users[18].

From a traditional European legal perspective, therefore, spam's worst offence is to be an invasion of the privacy of the individual whether the mail box is situated at home or work. Spam has been described as combining the worst aspects of junk mail, unwanted telephone solicitation ("cold calling") and junk faxes[19]. Looked at this way, spam is not a dissimilar problem to traditional, non electronic direct marketing, although it is important to note that the costs of marketing by spam are shifted almost wholly from the spammer, to the recipient who pays his ISP for Internet bandwidth and access. For the spammer, each spam costs less than 0.025 cents to send - for the recipient, the costs will generally be far higher, both in terms of time, money and personal irritation. Given the traditional European view that spam, like ordinary junk mail, was primarily an annoyance to living persons in their private sphere, it was natural that the main legal response in Europe was to cite the protection offered by data protection (DP) law, even though those rules not only pre-dated the deluge of spam, but also

[16] Dallman and Dowling noted in 1998: "The British Government is shortly due for a nasty shock due to their policy of connecting all schools to the Internet. Imagine the reaction when the tabloid press discovers that school children are being sent advertisements for pornography via the email accounts that the government has provided." *Towards Useable Email*, p 2 at http://ww.davors.org/legal/dmaspam.html. Oddly there have been no such scandals, though most schools in the UK now have draconian filtering and firewall systems in place which may have forestalled such.

[17] "Spam rage" was plead in defence in the case of a Silicon Valley computer programmer, who was arrested for threatening to torture and kill employees of the company he blamed for bombarding his computer with Web ads which offered to enlarge his penis: see report of November 21 2003, at http://www.wired.com/news/culture/0,1284,61339,00.html.

[18] Or as the judge at first instance in the US District Court case of *U-Haul International v WhenU.com Inc*, CA 02-1469, plaintively puts it: "Computer users, like this trial judge, may wonder what we have done to warrant the punishment of seizure of our computer screens by pop-up advertisements that require us to click, click and click again in order to return to our Internet work."

[19] See Byrne "Squeezing Spam Off the Net: Federal Regulation of Unsolicited Commercial Email" (1998) 2 W. Va.JL and Tech 4.

were largely formulated before the arrival of the modern Internet[20]. DP law does indeed in general forbid the processing, which includes collection and transmission, of "personal data" which identifiably describes a "living individual[21]" without the consent of that individual. It also bans in particular the use of personal data by direct marketers if the individual whom those details describe refuses to allow them use[22]. Such protection however is not available to corporations who are not living persons and thus incapable of being regarded as data subjects[23]. Since small to medium sized enterprises (SMEs) and sole traders suffer just as much or more economically from spam as individuals this is a major flaw in a DP-centric approach to spam regulation. The UK PECD regulations, as we shall see, do offer some limited extension of protection to juristic persons. In the US the situation is wholly different; not only is there of course no omnibus DP regime, but it has also long been accepted, albeit with some reluctance, that direct marketing is a form of speech and as such protected by First Amendments rights, although the protection given is much less than that which would be accorded non-commercial speech[24].

And of course, for those few individual who do (mysteriously) take up the offers promoted by spammers, spam is not just a matter of disgust and invasion of privacy, but a serious cause of financial loss and personal dismay as a result of fraud. However such loss is usually covered by one or more existing laws relating to fraud in general, to mail fraud, credit card fraud or to abuse of phone lines or telecommunications[25]. Accordingly the EC approach has been that particular regulation of spam based on loss to living individuals should mainly be conceived as relating to dignitary (privacy) rather than economic loss.

[20] See EC Data Protection Directive (95/46/EC), implanted in the UK by the Data Protection Act 1998, and EC Telecoms Data Protection Directive, 97/66/EC, implemented in the UK by Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations SI 1998 No 3170 (relating to telephone solicitation).
[21] See Data Protection Act 1998, s 1(1) and discussion in Edwards, supra n 1.
[22] See Data Protection Act 1998, s 11.
[23] This point is taken up interestingly by Bygrave L. *Data Protection Law : Approaching its Rationale, Logic and Limits* (Kluwer, 2002)
[24] *Virginia State Board of Pharmacy v Virginia Citizen's Consumer Council Inc* 425 US 748. See most recently the failure of telemarketers to have the "Do Not Call" register set up by the Federal Trade Commission declared a breach of the First Amendment: see decision of the 10th US Circuit Court of Appeals in *Mainstream Marketing Service v FTC* at http://www.ca10.uscourts.gov/opinions/03-1429.pdf.
[25] The Communications Act 2003, s 127 (1) makes it an offence to send by means of a public telecommunications network a message that is "grossly offensive or of an indecent, obscene or menacing character". Section 127(2) further provides that a person is guilty of a crime if he persistently uses a public electronic communications network to send messages he "knows to be false" – but, only if this is done "for the purposes of causing annoyance, inconvenience or needless anxiety".

Economic impacts of spam: the Internet, the ISPs and employers

If offence and annoyance to individuals, plus some significant economic loss to a few gullible souls[26] was all the damage spam caused, there would be good reason to leave it solely regulated by DP law, or indeed, to leave it unregulated by law but solely by technologies such as filtering. But spam can also be seen as a problem which is mainly economic, not emotional, in impact; which impacts disproportionately on certain industry groups; and affects the public interest in general, more than private individuals - and this analysis points towards why DP laws are perhaps not the best way to regulate spam after all. DP laws are mainly intended to encourage administrative compliance by responsible businesses, and are ill suited either to punishing in a way that hurts those who flagrantly disrespect the law, nor to compensating those who suffer financially as a result of spam. At the moment in the UK, the maximum fine for breaching an enforcement order served by the Information Commissioner is £5,000 unless the trial goes before a jury, and in practice, prosecutions of any kind are rare to non-existent and fines low[27]. By comparison, ICSTIS, the regulator for breaches of the code of usage of premium rate phone lines, has recently imposed fines of up to £75,000 on spammers who came under its jurisdiction as they were fraudulently encouraging users to run up charges on premium rate lines[28]. There are no jail sentences available for even the most persistent spammers[29]. Individual compensation for victims of breaches of DP law is possible[30], but there are no reported cases of an individual ever succeeding in gaining damages in the context of spam, and given the cost of legal proceedings, the lack of precedents and the likely nominal sum that might be awarded, it is unlikely any will arise[31].

Arguably this will exempt most spammers, who just want to make a buck not cause alarm.

[26] It is often incredulously asked: "But who actually responds to spam? How *do* spammers make money?" A number of explanations are put forward in the literature. One is that most spammers make money from selling other spammers software and mailing lists of spam-able addresses. A variation on this is that spammers are only trying to obtain personal details, not actual customers, so as to perpetrate further frauds and identity thefts. Another view is that the costs of spam are so low and billions of messages so easy to send, that a tiny return rate will still turn a profit. Victims are also often unlikely to complain and reveal their own gullibility so, as frauds go, it is a very safe one. See further, Sauver J. "The Economics of Spam: The Spam Business Isn't Always What You'd Think" at http://cc.uoregon.edu/cnews/summer2003/spameconomics.html.

[27] See Annual Report of the UK INofrmation Commisioner 2002-2003 at http://www.informationcommissioner.gov.uk/.

[28] See report on *ICSTIS v BW Telecom*, a New York company reported in The Register, 17 February 2004 at http://www.the register.co.uk/content/6/35695.html; ICSTIS's website reports all such adjudications at http:www.icstis.org.uk/.

[29] Compare Italy, where jail sentences of up to three years are possible; and Virginia, where a spammer was recently jailed under the state spam statute for nine years (see http://news.bbc.co.uk/1/hi/technology/3981099.stm).

[30] 1998 Act, s 13.

[31] Even Naomi Campbell, a global celebrity, was merely awarded nominal damages for the breach of her data privacy rights at the first stage of her recent battle with the press in the UK courts - see *Campbell v MGN* [2002] EWCA Civ 1373. (At the Court of Appeal, she then had her DP claim rejected on the grounds the breach of privacy was in the public interest – their "right to know" – and although this was reversed in the House of Lords, the DP point was not pursued.) If even Ms Campbell only receives nominal damages for breach of DP rights, what would an ordinary mortal be granted?

Upon whom does spam have the maximum detrimental impact? The European Commission has emphasised in the past, especially when introducing the ECD, that spam is one among several factors which fundamentally impedes the growth in public trust in the Internet as a serious commercial and social medium, by which governmental as well as private services can reliably be delivered. In this respect, the European debate around spam has begun to resemble the older debates around the regulation of encryption and pornography: in both cases, the private/moral interest in protection from offensive content, or protection of privacy rights, eventually carries less weight than the public/economic argument that unless the Internet is cleaned up and made secure for consumers and businesses, electronic commerce cannot thrive[32]. With spam however, the threat posed to the public interest has become somewhat more acute, as it has begun to threaten the potential destruction or at least retardation of the information society the EU has tried so strongly to promote. European Commissioner for the Information Society Erik Likannen put it thus in a speech in 2003:

> "Combating spam has become a matter for us all and has become one of the most significant issues facing the Internet today. It is a fight over many fronts… *We must act before users of e-mails or SMS stop using the Internet or mobile services*, or refrain from using it to the extent that they otherwise would.[33]" [emphasis added]

Certain actors suffer particularly direct economic losses as a result of spam. ISPs, especially the largest ones such as AOL, Comcast, BT Internet etc, suffer the brunt of the immediate damage. The sheer bulk of traffic sent out by spammers - who use special spamming software to sometimes send tens of millions of messages at one go - uses up bandwidth and slows Internet traffic down, not just email but also other services such as the Web. ISP servers from which spam is sent, or to which or through which it is transmitted, may crash, not just as a result of the initial volume of mail sent out but because of "mail undeliverable" messages returned from inaccurate email addresses. Smaller ISPs tend to buy only as much bandwidth as they need to support the estimated traffic of their known subscribers and massive surges of use caused by spammers, often sending vast amounts of spam from or to their server via multiple virus-enslaved computers known as "zombie drones", will tend to crash the ISP's

[32] Dickie has described this as a "market" rather than a "welfarist" focus in regard to regulation of the Internet: see *Internet and Electronic Commerce Law in the European Union* (1999, Hart Publishing), p 101.
[33] Speech of 25 July 2003, quoted in DG Information Society Working Paper, *Issue Paper for EU Workshop on Unsolicited Commercial Communications or Spam*, 16 October 2003.

mail server or require the ISP to waste money buying excess bandwidth as preventative strategy. This represents a major problem to ISP and their system administrators who to retain customer confidence (and avoid potential suits for breach of contract) need to provide 24 hour access and keep networked workplaces going[34]. In *AOL v Prime Data Systems Inc*[35], the court estimated that the real costs of AOL of dealing with each spam message were 0.078 cents per message. Since in that case 130 million junk emails were sent, the court awarded $4000, 000 dollars against the spammer (including a punitive triple multiplier on the estimated damages). In another case it was estimated that handling spam had so degraded the performance of the server afflicted by spamming that emails that should have been delivered in minutes were taking three days to arrive[36]. Another major cost is filtering and its associated problems. Most major ISPs filter spam aggressively in an attempt to service their customer base. AOL estimated in 2003 that of the 2.5 billion email messages they delivered a day, nearly 80% were spam. AOL winnows these out, as the costs of filtering out spam are considerably less than the costs associated with storing and distributing it, plus efficient spam handling is a positive feature in attracting clientele. However the downside of such proactive filtering is dealing with complaints from customers whose emails are wrongly blocked as spam *and* from recipients who fail to receive email which was falsely identified as spam. Block of such "false positives" may lead to valuable transactions falling through and important appointments being missed; although the issues of tort or delict law here are uncharted, it is clear that costs accrue to ISPs whichever way they decide to "play safe". MCI, a large Internet backbone carrier, now receive half a million complaints a month that its network is being used to transmit spam, and when it succeeds in evicting spammers from its network, finds that they rarely pay their accrued bills[37]. Less directly, large ISPs suffer brand tarnishing as they are associated with spam as their directories of customer addresses can be easily "harvested" and thus tend to be heavily spammed. This damages customer loyalty and branch recognition and may have detrimental effects on their capital value or public stock price.

The other group who bear the cost of spam, it is often claimed, are employers. Spam wastes employee time, both when they examine and delete spam, or, worse still, become frustrated (or intrigued) and try to reply to it. Reports (usually commissioned by the writers of spam-blocking software, and so to be taken with a pinch of salt) repeatedly show that companies

[34] Compare the international furore caused, when Microsoft were forced in 2004 by hackers to shut down the free web based email system Hotmail for a few hours as a result of its compromise by hackers.
[35] ED Va No 97-1652-A, 12/10/98.
[36] *Compuserve Inc v Cyber Promotion Inc* No C2-96-1070 (SD Ohio 24/20/96).

lose large amounts of money through spam, with some claiming that employees waste up 10% of their day opening and discarding spam email. Estimates of the annual cost of spam per US worker vary between $1400 and $49, depending on the analyst consulted[38]. The European Union, on whatever calculation, has based its legislative attack on spam on the claim that it is costing European businesses more than 2.25 billion Euros a year[39].

Spam law prior to the E-Commerce Directive: the Data Protection Directive, the Distance Selling Directive and the Telecoms Data Protection Directive

The Data Protection Directive (DPD), and its UK implementation in the Data Protection Act 1998, imposes duties on "data controllers" broadly to (i) to comply with the Data Protection Principles[40] and (ii) to notify with the Information Commissioner as persons who are processing personal data[41]. If these duties are breached, then the data controller may be liable to compensate any individual adversely affected, even if the Commissioner does not serve an enforcement notice[42], and criminal liability may also be incurred[43].

To determine if DP law regulated spam, then, it was first necessary to decide if spammers are "data controllers". A data controller is defined as "a *person who…determines the purposes for which and the manner in which personal data are, or are to be, processed.*"[44] This begs the question, do spammers process "personal data"? Typically, spammers harvest from newsgroups, web sites or ISP mail programs, buy, or otherwise obtain, long lists of personal e-mail addresses, to which a spam e-mail is then sent by special software. Under s 1(1) of the 1998 Act, "Processing" includes "*...carrying out any operation on the information or data*", which seems to fit these activities satisfactorily. "Personal data" itself is defined in s 1(1) as "*data which relates to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller.*" Does an e-mail address, without any other added information, identify an individual, in the same way that a name and physical address would?

---

[37] See generally, Hansell S. "Diverging Estimates of the Cost of Spam", *New York Times*, July 27 2003.
[38] Ibid.
[39] Cited by BBC News website, 15 July 2003.
[40] 1998 Act, s 4(4).
[41] *Ibid*, s 17(1).
[42] *Ibid*, s 13.
[43] *Ibid*, s 21.
[44] *Ibid*, s 1(1)).

There has been doubt on this matter in the past[45]. However, the PECD appears clearly to assume that email addresses if they do belong to a living person are to be regarded as "personal data" and this is also the approach taken, with some caveats, in guidance supplied by the UK Information Commissioner[46].

Assuming the 1998 Act does apply to spammers, it was clear that on most occasions, the act of spamming would be *prima facie* in breach of the 1998 Act in multiple ways. For example, spammers typically fail to register with the Data Commissioner as required, and also fail to respect requirements such as data security and use only for stated purposes. Most importantly however, spammers invariably failed to meet the most significant DP rule, deriving from the First Data Protection Principle, that the consent of data subjects to the processing of their data must be obtained. Admittedly, such consent is not required if one of the other exemptions in Schedule 2 is applicable, but the only one that seems relevant to spam is that the processing is "necessary for the purposes of legitimate interests pursued by the data controller" which interests must be balanced against the data subject's rights, especially to privacy[47] . If the processing is detrimental to the interests of the data subject, as it arguably will always be in the case of spam, then the exemption is highly unlikely to exculpate the data controller.

The DPA 1998 furthermore gave the data subject the specific right under s 11 to demand to cease receiving - or to "*opt out" f*rom – the processing of his or her personal data for the purposes of direct marketing[48] by a data controller. This right was seen as important for consumer protection, even though anecdotal evidence showed that consumers rarely had either the knowledge or the impetus to seek out data controllers and express their desire to opt out. "Opt-out" from traditional direct marketing was facilitated by the creation of the Mailing Preference Service, a voluntary "opt out register" run by the Direct Marketing Association[49], where consumers could register their preference not to receive direct marketing. Direct marketers then came by virtue of s 11 under an effective obligation to check the names on the register and remove "opt-out" names before they sent out a mail-shot. Similar voluntary

[45] See Edwards, *supra* n 1.
[46] See Information Commissioner's Office DPA 1998: Legal Guidance at p 12, available at http://www.informationcommissioner.gov.uk/.
[47] 1998 Act, Sched 2, para 6(1).
[48] "Direct marketing" is defined for these purposes as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" (s 11(3) and so includes spam as well as traditional junk mail.
[49] See further http://www.informationcommissioner.gov.uk/cms/DocumentUploads/The%20Mailing%20Telephone%20and%20Fax%20Prerence%20Services.pdf .

preference services were established for fax and telephone "cold calling". No such voluntary register however existed specifically for email spam, unsurprisingly as, as noted above, spam comes overwhelmingly from spammers who are outside the EU, anonymous and uninterested in complying with EC or UK law. Spammers, of course, nearly always failed to respect the opt-out right even where they ostensibly provided an opportunity to opt out within their own emails or websites (usually of the "click here if you don't want to receive any more messages of this kind" type). Indeed, usually the spammer's reply-to email address proved either to be false or non-working or, as worst case scenario, to be a trap by means of which the spammers could verify the spam victim email address was indeed a valid one.

Other pieces of EC consumer legislation subsequent to the DPD also provided possible opportunities for enhancing protection from spam, but these were repeatedly not exploited, mainly due to the fervent opposition of the direct marketing industry. Consumers were, for example, guaranteed the right under the EC Distance Selling Directive 1997[50] not to receive unsolicited communications relating to distance selling from a business where they clearly objected[51]. This Directive, being of later vintage, was more clearly intended than the DPD to cover communications sent via the Internet as well as conventional mail and phone communications.[52] However since it again mandated only an "opt-out" regime, effectively it required no more protection be given by the UK in relation to spam than s 11 of the DPA 1998 already gave[53]. An "opt-in" minimum requirement, by contrast, would have meant that member states were required to legislate so that consumers would actually have to express a *prior preference* to receive unsolicited communications from the business in question before it would be legal for them to be sent such communications. Given consumer inertia, it was obvious (to everyone but the direct marketing industry) that such an approach would generally be more effective at controlling the increasing problem of spam, and protecting consumer privacy. It was not however at this time seen as the politically appropriate solution, at least in the UK, though several EC member states , notably Germany and Austria, did voluntary adopt an "opt-in" regime (and thus ban spam) relatively early on.

[50] Directive 97/7/EC, OJ No L 144/19**.** See further, Nordhausen A in Chapter 8 of this volume and Appendices.
[51] Art 10(1), Distance Selling Directive.
[52] See Art 2 of the DSD and Annex 1, which specifically refers to "electronic mail".
[53] The consultation paper issued by the DTI in November 1999 included draft regulations which contained alternate opt-out and opt-in schemes - however an opt-out scheme was in the end chosen.

Similarly, the Telecommunications Data Protection Directive 1997[54], implemented in the UK by the Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998[55], was introduced to deal with the growing problem of unsolicited telephone calls and faxes and was aimed at cutting down on such "cold calling" against the wishes of consumers. Article 12 of this Directive again gave states discretion to implement using either an "opt-in" or "opt-out" system, and again, the DTI chose after consultation to opt for the latter, so that those who wished *not* to receive unsolicited "calls" still had to register their opt-out (with, this time, the Telephone Preference Service) to achieve this effect. The DTI also made it clear during the consultation period on implementing the Telecoms Directive, that the Regulations, and in particular, the word "calls", were not to be interpreted to include e-mail solicitations[56] and thus even the mild regime of opt-out was not extended to unsolicited email either (although mobile phone text messages *were* deemed to be included in the word "calls" and thus, slightly oddly, did fall within the regime.)

It became clear that there were two clear problems with both the Distance Selling Directive and the DPA 1998 in relation to spam. First, the jurisdictional and resources difficulties of enforcing EU and UK rules against predominantly American spammers were almost insuperable. But secondly, even leaving the enforcement difficulties aside, the "opt-out" regime which both sets of rules imposed, was of very little practical help. Human nature is such that even faced with a constant source of annoyance, very few people are equipped to find out that a regulatory scheme exists which may help them, and even fewer will then make the effort to register their veto on spam. Most independent commentators agreed that an opt-in scheme for spam would be more appropriate, under which consumers would have to indicate (however bizarrely[57]) their actual *desire* to receive spam. Interestingly, the Distance Selling Directive of 1997 had already prescribed a very limited mandatory "opt-in" regime for junk faxes and automated calling machines[58], machines which repetitively call certain telephone numbers and then either hang up, play a pre-recorded message or connect the consumer to a

[54] 97/66/EC. The Regulations came into force on 1 May 1999.
[55] SI 1998 No 3170.
[56] See *Telecoms Data Protection Directive Implementation In the UK – Draft Regulations*, para 2.3.
[57] It has however been argued that "opt-in" is rather easier for the seller to secure in relation to business-to-consumer (B2C) e-commerce than in the traditional postal or catalogue distance selling domain. Any consumer who buys something from a web site can be offered a box to click if they want to "receive further information". This will do as "opt-in"; there is no need for it be done via a central register as with "opt-out", so for small businesses, "opt-in" may actually be a cheaper regime under which to operate than "opt-out" where search fees of the opt-out register will be a significant overhead.
[58] See Art 12(1). It is noteworthy that even in the US, the home of free speech, automated calling machines are banned (although enforcement of this is patchy) and this ban has been upheld as constitutional (see *Moser v Federal Communications Commission* 46 F.3d 970 (9th Cir. 1995).

human salesperson (if one is available)when the call is answered. The reason why these means of selling were distinguished from ordinary distance selling was, in the case of faxes, because the costs of marketing were transferred from seller to recipient, and in the case of automated calling machines, because of the extreme aggravation they caused. Both reasons applied just as strongly to spam, and therefore the case grew ever more compelling for the EC to unambiguously prescribe an opt-in regime for spam, especially as spam ceased to be a minor consumer problem, and became the scourge of the Internet around the turn of the millennium.

The Electronic Commerce Directive

At this point therefore, it was particularly puzzling and frustrating that the drafters of the ECD failed to grasp the nettle and impose a spam opt-in regime on reluctant member states such as the UK. Attempts were made in the European Parliament during the passage of the ECD both to ban both spam and cookies outright (see further below) but these were in the end repelled. Instead the EC Commission restricted the reforms introduced by the ECD in this connection to some rather redundant transparency provisions in Arts 6 and 7. First, Art 6 required that (all) "commercial communications[59]" had to be "transparent" in the sense that certain information had to be made available which identified the sender, adequately disclosed the nature and conditions of promotional offers made by the communication, etc[60]. In many respects, these requirements duplicated the work already done in the Distance Selling Directive. Secondly, only *unsolicited* commercial communications had to be "identifiable clearly and unambiguously" as such to the recipient as soon as they arrive[61]. The obvious way to implement such labelling in the case of spam is by requiring a word such as "advertising" to appear on the subject line of any spam e-mail. Spam filters can then in theory read the label and filter out the message. The UK Electronic Commerce (EC Directive) Regulations 2002 do not go into that degree of detail, however, merely demanding in addition to the general rule transposed from the Directive that any promotional offer or promotional competition or game be clearly identified (along with its qualifying or participation conditions)[62]. Even if labelling is adopted by sellers, it is not much of a solution to spam. It may spare the sensibilities of

[59] Defined in the UK Regulations (see n 62 infra) , reg 2 as (with exceptions) "a communication, in any form designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity, or exercisig a regulated profession". The exceptions are a communication which contains merely an address, domain name or email address; and a communication promoting A but sent by an independent person B.
[60] The Commission has suggested that such information might satisfactorily be provided by a hyperlink in the case of a web page making a commercial communication; such a link could also be placed in an email. .
[61] Art 7(1).
[62] SI 2002/1931, regs 7 and 8.

recipients who are spared the experience of opening a message labelled (say) "Advertising: red hot porn", but will do little for the more economic problems caused by spam discussed above, eg, the on-line time they waste being downloaded and deleted, and the clogging up of Internet bandwidth. Labelling *will* give email filtering systems a tag to act upon , but may also interfere with users forwarding spam to ISP postmasters and other spam "vigilantes" so that they can be "blacklisted" (see below) as they are currently encouraged to do. In any case, the practical evidence since the ECD was implemented in 2002 is that again, spam coming from outside the EC (and probably from within it as well) has resolutely ignored these injunctions. Enforcement certainly requires, even within the EC, a considerable budget for investigation, given the ease of falsifying one's origins on the Internet and the untraceability of most spammers operating from free ISP accounts and "zombie drones". Finally, on the great "opt-in" debate, Art 7 finally provided merely that states must "respect the opt-out registers"; a provision so redundant that the UK Regulations did not even transpose it.

The Privacy and Electronic Communications Directive

It was thus left to the Privacy and Electronic Communications Directive 2002[63] to finally make some significant legal headway in Europe against the vice of spam. Article 13(1) of the PECD finally grasps the nettle and demands that all EU member states require prior consent – "opt in" – to the use of personal data to send junk electronic mail. "Electronic mail" further more is widely defined to include "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient"[64]. This is a clear attempt to make the Directive "technology neutral" and less prone to immediate obsolescence as new forms of both communication and communications tools are invented and become popular. At present, this certainly covers not only email, but voicemail, video messaging to 3-G smartphones, text massages to phones, and more. It is interesting to ask why finally after so many lost opportunities the EC has caved in and demanded "opt-in" to spam. One reason clearly is harmonisation – for many businesses, clarity on what they have to do throughout Europe is more important than the actual shape of the rule – but it is also down to the admission by the direct marketing industry itself that spam in its current form has rendered their industry untrustworthy and unprofitable; in short, most sentient human beings will delete unread any

[63] See n 4 *supra*.
[64] Art 2 (h), PECD.

unsolicited mail message from unknown sender as fast as humanly possible, whether it comes from a respectable high street brand business, or from a Nigerian offering to deposit $8,000,000 in your account. Only by re-establishing a culture of trust via prior consent, the argument goes, can "responsible" direct marketing businesses operate effectively on the Internet again.

So far, so good. There are, however, significant exceptions to the new "opt-in to spam" rule. Prior consent is *not* required if the details of the recipient were previously obtained "in the context of a sale of a product or service" so long as

- (a) the recipient is given a clear, simple and free opportunity to opt-out of receiving spam each time a new communication is sent, and
- (b) the goods or services were "similar" to those now being marketed[65].

Privacy advocates might suggest that the correct way to interpret this provision is to regard the exception as only operating where an *actual* prior sale had occurred – ie, *not* where the consumer had merely browsed the site to check out goods, decided not to buy, but perhaps inadvertently given away their details, eg, by having to register to gain access to the website; or by the collection of data via cookies (see below). The UK Regulations however take a different approach. So long as the business has legitimately obtained the contact details (in terms of the requirements of DP law concerning fair collection and processing), details can be used if they have been obtained in the course of the "sale *or negotiations*" [italics added]. Is merely browsing a site, perhaps to gain information or for price comparison, "negotiations"? Guidance from the Information Commissioner – who is of course perhaps more privacy-oriented than the DTI - suggests that "negotiations" require some kind of active expression of interest by the data subject in the company's products and certainly do not include the case where all that has happened has been the browse of a site and deposit of a cookie[66]. It remains to be seen how courts or regulators will interpret this clause when or if a dispute arises.

And what are "similar" goods or services? No elaboration is given in the Regulations but, again, according to the DTI during the consultation period, this should only be restricted by the reasonable expectations of the buyer at the time they gave their contact details. To give an illustrative example of the DTI approach, if a consumer buys baked beans on-line from Tesco's, it seems reasonable for Tesco's to then market TVs and DVDs (say) to that

[65] Art 13(2), PECD.
[66] *Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 1: Marketing by Electronic Means* available at http://www.informationcommissioner.gov.uk/ ..

consumer without prior consent, because the consumer could reasonably have known that Tesco's sold all these types of goods at the time she first gave away her personal information; however if Tesco's, *subsequent* to the baked bean purchase, acquired , say, a horse-riding stables business , it would *not* be reasonable for them to market horse-riding lessons to the consumer, as she could not have reasonably expected Tesco's to offer that service[67]. The Information Commissioner guidance also focuses on the idea of "reasonable expectation" and the availability of opt-out if the goods diverge from what the consumer expects to receive. Does the average consumer really view baked beans and TV sets, plain and simply, as "similar goods"? This seems a technical and privacy-minimising interpretation, which is unlikely to be harmonious with several other member states which have already banned spam entirely and long ago - nor is it likely to instill the trust in consumers which is the whole object of the exercise.

What else does the PECD do to prevent spam? Article 12 (implemented in the UK Regulations, reg 18) strengthens the right of an on-line subscriber to withdraw their name from an on-line public directory of subscribers eg an AOL customer could ask for their email address not to be visible on a publicly accessible list of AOL subscribers. Since spam mailing lists were often culled in the past from easily harvestable open directories of ISP customers, this is a useful right for individuals.

Finally as noted above, the UK PECD regulations are significant in going some small way towards extending the protection of DP law to juristic persons as well as living individuals. Regulation 22, as discussed above, extends *only* to individual users, not to "corporate subscribers" as defined in the Regulations. As Carey notes[68], this is not that crucial an omission, as most spam emails sent to businesses will still go to a named individual's email inbox and fall within the rules; only spam emails addressed explicitly to the business name would remain legal. But Regulation 23[69], which makes it unlawful to send a marketing email with no valid return address, or with the identity of the sender disguised or concealed, *does* apply to emails received by corporate subscribers, thus providing UK companies *as such* with their first real remedy in the fight against spam.

[67] Interstingly, the Art 29 Working Party Opinion on Art 13 of Directive 2002/58/EC also emphasises that "only the same natural or legal person that collected the data may send marketing emails… subsidiaries or mother companies are not the ame company." (para 3.5, 11601/EN WP 90, 27 February 2004).
[68] Carey P *Data Protection* (2nd edn, OUP, 2004), Chapter 12.

Assessment of legal solutions to spam, and alternative solutions to spam

The PECD brings one chapter in the battle to regulate spam by law to an end. The "opt-in" wars are over. But it still has to be asked, as it has been repetitively in this chapter, if this time-consuming hard-fought legal effort has been worthwhile. What will happen to spammers who continue to operate without obtaining prior consent? Spammers mostly operate outside Europe and pay little attention to European law; they are generally very hard to trace; even if traced they can move swiftly from server to server in different countries; even if found, the work needed to bring them within European enforcement jurisdiction will be enormous; the resources to fight spam in this way simply do not exist in most European countries where spam law enforcement is primarily the remit of the under-funded data protection authorities. There are very many spammers and very few data protection officials. To adopt Peter Swire's useful metaphor, spammers are "mice" not "elephants"[70]. To add insult to injury, as noted above, DP sanctions in most of Europe are hardly at the punitive level which would seriously cripple a determined spammer or put others off entering the trade, the obvious message is that there has to be a better way to fight spam than this.

The Americans, with more years of experience at fighting spam via the law than we Europeans, are faring no better. Impeded, as in Europe, by the lobbying forces of the direct marketing industry as well as by constitutional concerns about free commercial speech, the recent US Federal Can-Spam Act of 2003 is widely regarded as a damp squib and even by some more radical anti-spam campaigners as actively promoting spam. The main planks of the Can-Spam Act are (a) mandatory opt-*out (not* opt-in) and (b) prohibition of false or deceptive subject lines to spam email. "Sexually oriented" spam must also be identifiable in advance by a warning label. So far, so very similar to European law at the stage of the ECD: and we have already seen how effective that was. The US's own relevant enforcement body, the Federal Trade Commission, is so unconvinced of the benefits of opt-out that it has indicated its unwillingness to set up a "Do-Not-Spam" register to implement opt-out, on the perfectly sensible ground that such a public list will simply be used by spammers as a validated list of email addresses ripe to receive yet more spam[71]. To be fair, the US has the advantage over Europe of having a high proportion of spammers within its enforcement jurisdiction; and the

[69] Implementing Art 13(4) of the PECD.

[70] See Swire P "Of Elephants, Mice and Privacy: International Choice of Law and the Internet" 32 International Lawyer 991 – the metaphor of elephants and mice is then adapted to the landscape of on-line privacy in Edwards L "Reconstructing Consumer Privacy Protection On-Line: A Modest Proposal" (2004) 18 Int Rev Law Computers and Technology 313 .

Act also goes further in some ways than the ECD or even the PECD, particularly in prohibiting the use of third party computers ("open relays" or "zombie drones") to send spam without the consent of that computer's owner. These provisions get nearer to the heart of what might actually make spam unworkable as opposed to traditional privacy and consumer law solutions. Most ISPs nowadays prevent any subscriber, guest or paying, named or anonymous, sending out mail-shots in the bulk which spammers need to use to have any hope of profit – that is, millions not thousands of messages. Spam is therefore now overwhelmingly sent either from ISPs or servers in developing countries which have no effective legal regulation in this area, from mail-server machines which have been, contrary to good security practice, left open so anyone can use them to send mail, not just registered users of that server ("open relays") - or far more commonly now, from networks of "zombie drones"[72]. These are computers which, usually by means of a virus infection (or "trojan horse"), have been "enslaved" by a remote user (the spammer, or zombie network owner) usually entirely without the knowledge of that computer's legitimate user or owner. If the enslaved computer has mail-server software on it, or (more commonly) if that software can be implanted by a virus attached to the spam email, then the "zombie" can be used to send out spam without any of the usual problems of getting it past an ISP's safeguards. Legal provisions such as those in the Can-Spam Act making it plain that creating "zombie drones" is itself a crime in spam law, are thus extremely useful, though again, hardly easy to enforce without detailed computer forensic help.

A second useful provision in the Can-Spam Act is a ban on falsifying the header information or origin of the email sent by spammers. Again, one of the key technical tricks spammers use is always to disguise the true origin of their messages, perhaps by using proxy servers, "zombie drones" as discussed above, and anonymisers to modify originating IP address, as well as by more obvious tricks such as using dud return mail addresses. This prevents their being traced by law enforcement authorities or besieged by angry replies from disgruntled spam recipients. It also prevents the spam messages easily being caught by ISPs and system administrators who filter out email from known spamming domains and addresses. Thus again it is a sensible legal strategy to ban the falsification of email origin data. This prohibition arguably exists in UK law on the basis of common law fraud as well as regulation 23 of the PECD regulations, but it is not entirely clear how far modifying header information,

[71] See "Do-Not-Email list is pointless, reasons FTC" at www.Out-Law.com, 17 June 2004.

[72] See for example, Leydon J "Zombie PCs spew out 80% of spam" at The Register, 4 June 2004 (http://www.theregister.co.uk/2004/06/04/trojan_spam_study/) reporting that four fifths of spam now emanates from computers contaminated with Trojan horse infections. Many well-known viruses are sent out, the report claims, purely to

say, as opposed to providing a false name or a non-existent email return address, would be a breach of regulation 23. The US clear statute law reference to "origin of email" is to be preferred to the PECD emphasis on "identity of sender".

But although both these provisions are helpful to the cause of stamping out spam, again both fall foul to the problems of the resources needed for investigation, the number of spammers, the jurisdictional problems and the huge forensic difficulties of establishing that a particular Trojan horse virus (say) was released by a particular spammer. Just as in Europe, spam volume in the US has continued inexorably to rise, even since the Can-Spam Act came into force on 1 January 2004[73]. While it is of course essential to criminalise or otherwise sanction the activities that enable spamming, passing laws is really only a first and rather unsatisfactory step in the process of catching spammers or blocking spam activity. Would it not be better to concentrate the effort that has gone into legal solutions into technical solutions which might actually, conceivably succeed in reducing the actual volume of spam? Concentrating on technical standards rather than laws also has the key advantage that technology largely operates on a global basis. Difficult though the task still is, it is surely easier to get a few major IT players (all of whom hate spam) to agree on standards, than it is to globally harmonise *legal* regulation of spam via the slow and tortuous domain of international treaty making[74]. A third point is that although the EU has attempted to draft "technology-neutral" laws to fight spam and more generally protect consumer privacy, it has inevitably and continually lagged behind in the spam "arms race". Technical standards in their nature would have at least a better chance of dictating to spammers, rather than, as is currently the case, spammers using technology to outwit and out-race the law.

Technical solutions – the answer?

Within the knowledgeable Internet community itself, there has been consensus for several years that the best results will come not from legal regulation, but from "self regulation" by

---

establish networks of compromised machines as future spam relays.

[73] However "sexually explicit spam" *has* reportedly dropped by 78% since January 2004 reported the Internet company Postini, in October 2004. This bolsters the view taken in this article that spam regulation is mainly about economic loss and gain and not about "privacy" primarily.

[74] The EU have continually attempted for the last few years to broker international co-operation on spam, particularly between the EU and USA, as has the UN organization, the International Telecommunications Union (ITU), but the process remains slow despite mutual good intentions. Even intra-EU co-operation on spam law enforcement has been difficult to achieve. See latest communications from the EU Commission at http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=en&guiLanguage=en on encouragement of cross-Europe spam hotlines accessible to all EU citizens for the reporting of spam, and EDRI

technical strategies[75]. There are a number of less or more successful approaches. The first line of defense has always been that ISPs, local network managers, and individual users can use filtering software to winnow out e-mails sent from the addresses (IP addresses and/or URLs) of known spammers. This however is only ever partially effective as the addresses of spammers change constantly and are in any case, as described above, usually disguised. There is some degree of co-operative "blacklisting" of sites and ISPs known to harbour spammers: one such blacklist often consulted by system administrators is known as the Real Time Black Hole List and is available on the Web[76]. Traffic coming from a blacklisted site will not be transmitted on via other networks or ISPs where administrators have consulted the blacklist, with the effect that the black-listed site becomes isolated from the rest of the Internet, effectively "sent to Coventry". However no such system is foolproof, and a site which is being unknowingly made use of by spammers against its own policies (a "zombie drone" perhaps), or one which is sending out multiple copies of an e-mail for a valid reason (eg an alumni e-mailing from a university) may find itself black-listed alongside the "guilty" sites. It has also been suggested that mistaken placing of a site on the list might be seen as libelous, which provides a disincentive to co-operate in providing information to the organizers or re-publishing the list. Philosophically, Lawrence Lessig, the highly respected Internet law guru, has lead a movement against "black hole lists" on the ground that they represent undemocratic unaccountable vigilante justice[77]. An extreme solution is to use a "white-list" ie, *only* accept email from a list of prior approved senders: this has obvious difficulties for agencies such as the government and universities, which constantly receive enquiries from strangers, as well as for most individuals.

The most currently promising technical solutions involve variations on configuring email servers, or more radically, redesigning the email standard format itself, to make it possible to spot any attempt to falsify or disguise the true origin of an e-mail message. Filtering out all mail with fake reply addresses or falsified header information will effectively filter out almost all spam. Promising attempts are being made, notably by the IETF (Internet Engineering Task Force) and a loose confederation of major industry players (the Anti-Spam Alliance[78]) to develop what are known as "trusted email systems": systems where, by various different

---

comment at http://www.edri.org/edrigram/number3.3/spam .

[75] See Dallman and Dowling, *supra* n 7 and Edwards (2000), *supra* n 1.

[76] Run by the Mail Abuse Protection System (MAPS). See further http://maps.vix.com.

[77] See Lessig L "The Spam Wars", December 31 1998 at http://www.lessig.org/content/standard/0,1902,3006,00.html . Lessig' attitude may have been coloured by the fact that his former employer, Harvard University, was at one time black-listed on the Real Time Black Hole List.

means, the standard format of email is altered so that the true domain origin of a message is always apparent and cannot be successfully disguised. Email can thus always be authenticated as coming from a verifiable, and traceable, source; if it does not, it is spam and can be filtered out or bounced back. There are many obstacles still in the way of developing a trusted email system acceptable to all players – technological interoperability, proprietary standards and patents, trade secrets, industry rivalry, and privacy concerns about the possible loss of anonymised email – but in the end this is likely to be the most promising route to stamping out spam. It is quite possible that in five years technology may have succeeded where law has failed and succeeded in removing spam from the regulatory agenda.

Economic solutions

While we wait for technology to do its stuff, another set of possible answers to the spam problem has emerged which might be termed economic solutions[79]. These start from the not unobvious observation that spam is based on the fact that spamming costs spammers almost nothing regardless of how many emails are sent[80]. Both senders and receivers of email largely pay almost zero to send and receive spam, despite that fact that spam does have marginal costs, such as electricity, storage and network congestion. These costs are , however absorbed by persons other than the spammer. So for the spammer "this represents a sure-win strategy: mail as much as you can, because even one hit out of a million is profitable"[81]. The obvious solution then is to charge (on top of dial-up or broadband costs) for sending each email. This will of course be unpopular with ordinary, non-spammer, users; but if the charge is kept very low, then arguably it will only really bite as an economic disincentive against those (like spammers) who send out millions, not tens or even hundreds of emails per day. With this in mind, Bill Gates, CEO of Microsoft, proposed in early 2004 that an email "postage stamp" be purchased before email could be sent[82]. Set at a very low figure, of say, 0.01 cent per item, this would barely scrape the pockets of ordinary users but would be a real financial burden for spammers.

---

[78] The group includes Yahoo!, Microsoft, EarthLink and America Online.

[79] It is interesting to note that spam as a problem has now engaged all four of the modalities of regulation Lessig famously identified in his seminal text *Code and Other Laws of Cyberspace* (Basic Books, 1999). Spam was originally tackled by *norms* in the form of netiquette and flaming, as doled out by the early Internet community to the original Green Card spammers; then by *law*; then (or simultaneously) by "*code*"; and now finally solutions are emerging from looking at how *the market* propagates spam.

[80] See Leyden J "The economics of spam", *The Register*, 4 March 2004 at http://www.theregister.co.uk .

[81] "Make 'em pay", *The Economist*, February 14 2002.

Although in some ways an attractive idea, charging for email has so far failed to gather overwhelming support. Many critics voice concerns in principle about abandoning the democratising and free speech advantages of "free" email. What, for example, of non-commercial community information sites which send out notifications concerning, say, breast cancer news, or important public meetings to thousands of subscribers? Free "weblog" sites also often regularly send out many hundreds of thousands of emails notifying participants of comments to their postings. Handling the many millions of micro-payments a "postage stamp" system would demand is also problematic. Would such payments be made in only one currency or every local currency? Who would collect them – the ISP? Who would oversee their collection mechanisms and enforce the "postage stamp" regime? What would be done with the money? The area is fraught with unanswered concerns. One possible retrenchment would be to make a would-be email sender do a short puzzle before they sent an email, with no monetary payment involved: plausible in time costs, it is argued, for a sender of a single email, but not for a spammer sending millions. However a quick and highly unscientific straw poll by this author found that ordinary users were even more unwilling to waste time doing puzzles to send their everyday email than they were to pay for "postage stamps". A final, slightly more promising wrinkle, is to ask senders not to actually pay in advance, but to put a certain sum of money up front as a bond or guarantee[83]: if the email they send is then rejected by the intended recipient as spam, the bond comes into operation, and a cost per email would be deducted. However a solution like this virtually requires recipients involved in the scheme to maintain a "white-list" of who they are willing to receive email from; which as noted above, is for many individuals and associations who anticipate email from strangers as well as friends, not a practical exercise.

Another quasi-economic approach focuses on *enforcement* of anti-spamming laws. As we have noted above, one of the obstacles to the success of all spam laws is the vast amount of spammers, the difficulties of bringing them to justice, and the limited amount of resources which can be devoted by law enforcement agencies, both criminal and civil, to the project. Lessig has suggested that one way round this would be for the law to offer a "bounty" to private individuals who track down spammers. His proposal is for a law which would (a) require effective and mandatory labeling of all spam messages in their header so they could be filtered out – eg, by words such as "SPAM" or "ADVERT"; and (b) allot a "bounty" of, say

[82] See "Fee-based Email Way To can Spam?", March 5 2004, at http:///www.CBSnews.com,.
[83] The Economist, *supra* n 81, cites IronPort Systems in Silicon valley as already offering such a bond system to "legitimate bulk emailers" so they can differentiate themselves from spammers.

10c per spam message to an individual who tracked down and produced evidence that a spammer had broken this law. The "bounty" would be paid out of the fine imposed on the spammer once successfully prosecuted, and to reduce transaction costs, would be limited to cases involving the sending of at least 100 or more spam emails[84]. Superficially this seems a strange suggestion from a man who strenuously opposed in public the "vigilante code justice" of "black hole lists" (see above). However Lessig argues that while black-hole listers are using "code" to make their own rules as to who should be punished for alleged spamming, without legal backing or evidential hearings, his bounty system merely employs effective incentives to enforce constitutional anti-spam laws made by normal democratic processes. *"[W]ith automated black holes, no judgment is required before harm is done, nor do the victims have any effective appeal.*[85]" Lessig's argument sufficiently convinced a US member of Congress to introduce a Bill based on these principles, though it has not come into force.

The argument, although neat, can again be criticised. The "bounty" system is dependent financially on the successful prosecution of spammers once tracked down, which implies their being brought before the jurisdiction of the local courts with attachable assets. This may be a plausible assumption in the US, where the majority (though only just) of spammers are still based, but it is not a realistic expectation in Europe. (It also assumes successful prosecution, which surely cannot always be guaranteed.) From a constitutional perspective, would it not be better to use realistic and punitive fines paid by spammers (an excellent idea in principle[86]) to provide adequate funding (possibly in arrears) to existing agencies[87], already trained, accountable and responsible for tracking down spammers rather than pass it to "trigger-happy" private bounty hunters with no knowledge of law, evidence, jurisdiction, human rights or due process?

Further challenges to consumer privacy: cookies, traffic data, locational data and the PECD

[84] See account in McCullough D "A Modest Proposal To End Spam", April 28 2003, at http://news.com.com and also *infra.*

[85] Lessig L "Code-Breaking: A Bounty on Spammers", September 16 2002 , at http://www.cioinsight.com/.

[86] This is an area where UK DP law can certainly learn from US law. The Can-Spam Act provides for fixed damage levels of up to $100 per email sent to a cap of $2 million, or triple that amount if state attorneys prosecute in criminal courts. Compare the UK maximum penalty of £5,000 in DP law (unless a jury trial is convened) and the actual highest fine in the last statistical year of around £3,000.

[87] This writer has also proposed another model for the better funding of agencies such as the Information Commissionwr's Office to meet under-resourced challenges such as the prevention of spam: see Edwards L "Reconstructing Consumer Privacy Protection On-Line: A Modest Proposal" (2004) 18 Int Rev Law Computers and Technology 313

The PECD deals not only with spam, but with a variety of challenges to consumer and on-line privacy which the Data Protection Directive was perceived as not being able to manage satisfactorily. Indeed, the explicit intention of the PECD is to update the DPD for the Internet era. Recital 5 states that "*New advanced digital technologies are currently being introduced in public communications network in the Community, which give rise to specific requirements concerning the protection of personal data and the privacy of the user… The successful cross-border development of [digital network] services is partly dependent on the confidence of users that their privacy will not be at risk."* The PECD thus attempts to regulate not just spam but other threats to on line privacy such as, notably, cookies. Challengingly, the intention is also to be "technology neutral", ie, to set up rules which may fairly and effectively regulate technologies not yet in existence as well as those already in the market. Whether the PECD actually achieves this goal is something we will briefly consider in this chapter's conclusion.

Cookies

Cookies are small text files (usually less than 1 Kbyte in size) which reside on the local hard disc of the computer, or terminal equipment of, a user, and contain a limited amount of profile information about that user[88]. Cookies are usually visible to users if you know where to look (the directories they are stored in depend on the configuration of the system, eg C;/Windows/Cookies) but frequently, the information in the cookie even if located will be apparently gibberish to the user, because it is merely acting as a unique identifier which connects the computer where it has been deposited, to information held server-side by the business which deposited the cookie. Typically, cookies are used on e-commerce sites such as Amazon, Ebay, etc. When a user browses such a site, or buys an item, then personal information is collected – what pages he views, what search terms he types in, what images he clicks on, what items he selects – and stored in the website's server –side database. That information is then connected to the user on subsequent repeat visits to that site via the cookie which acts to identify the user. (Sites cannot simply use IP address to recognize the user as many users access the Internet via ISPs such as AOL which dynamically assign different IP addresses to users each time they log in.)

Cookies of this kind are very useful to e-commerce businesses – and to on-line advertisers – as they enable a profile of the user's shopping habits and preferences to be built up. User X,

[88] See Sharpe A "The Way the Cookie Crumbles" (2002) 2 Privacy & Data Protection 6.

for example, may be revealed by cookies to be repeatedly surfing various websites which sell Nike or other brand trainers. This is valuable information, which can be used by the business itself, sold to competing businesses or to advertisers or used in combination with other information for data mining purposes[89]. Cookies of this kind are also useful to users: they enable sits to know you are, in essence, and are sometimes said to give the site a "memory"; there is no need to log in every time, and data such as delivery addresses and credit card details can usefully be remembered and filled in automatically for the user. Cookies of this kind are called "persistent" cookies, because they are not deleted but remain on the hard disc of the user more or less indefinitely. "Session" cookies are a very different animal. These are used as a technical device to maintain continuity during one Internet website browsing session. Session cookies are deleted at the end of the visit to a particular website and do not normally involve the processing of personal data or any possible invasion of personal privacy.

Cookies became an object of contention during the debates over the 2002 Electronic Commerce Directive, when the European Parliament became aware that personal information about consumers browsing the Internet was being collected using cookies and processed in large amounts, usually without the consumers' consent, and almost invariably without even their knowledge. So horrified were the Parliament, that, at one point, the total banning of cookies without explicit prior consent appeared to be on the cards, to the utter consternation of European industry[90]. The matter was not resolved within the ECD and by the time of the PECD, as ever, a compromise had been reached. The final version enshrined in Art 5(3) of the PECD requires merely that cookies may only be set if the consumer "is supplied with *clear and comprehensive information*... about the purposes of the processing, and is offered the right to *refuse* such processing by the data controller" [italics added].

This is in many ways an extremely watered down version of the original intent which was to introduce a positive opt-in requirement in relation to cookies, just as was eventually the case with spam. Instead, the provision retains an opt-out system, albeit with added requirements of clear information. It seems that in Europe, cookies may no longer be simply invisibly set and collected. But how will this information and opt-out opportunity be supplied? Will a hyperlink to a privacy policy be sufficient? What if the privacy policy is unintelligible? In the UMIST/UK Information Commissioner study of compliance of websites with data protection

[89] See further Edwards L and Howells G Anonymity, Consumers and the Internet: Where Everyone Knows You're A Dog" in Nicoll C, Prins and van Dellen eds. *Digital Anonymity and the Law (*Asser Press, 2003)**.**

[90] See Mackay and Lomas "The Cookie Monster" (2002) *Computers and Law*, vol 12, issue 6, p 14.

law[91], the study team found only 5% of privacy policies were intelligible to the average consumer, using recognised plain English indices. What if (as seems anecdotally to be the case) consumers never read privacy policies anyway? What if a tick box is supplied, already ticked, which gives permission to set cookies, unobtrusively tucked away at the bottom of the page? Or a box whose rubric reads "Tick this box if you don't want us to set cookies", so putting the onus on the unsuspecting consumer? Neither of these would surely have been acceptable under a requirement of explicit prior consent, but may well be in an opt-out regime. The PECD recitals, from a consumer point of view, provide both bad and good news here. "*Information and the right to refuse,* " runs recital 25 of the PECD, "*may be offered once... also covering any further use.*" So it seems that if the consumer *once* has an "opt-out" style tick box offered to her on her first visit to a particular web site, and fails to notice it and take the appropriate action (assuming she even knows what it means), she need never be offered it again; and meanwhile persistent cookies can be set which will continue to gather information every time she subsequently visits that site. On the other hand, the recital goes on to require that "*the method for giving information, offering a right to refuse or requesting consent should be made as user friendly as possible*". One might hope that this might rule out the scenario described above.[92] However, leaving such important detail to the recital part of the Directive will do little for European uniformity, an obvious problem when websites largely operate without notice of or concern for national boundaries.

Another interesting point in Art 5(3) is that setting cookies is allowed without consent where "*strictly necessary* in order to provide an information society service *explicitly requested* by the subscriber or user" [italics added]. Many web sites at present, whether by intent or laziness, are designed not to work without cookies. These are however often cookies of the non-privacy invasive, session cookie type. Some *will* work without cookies, but not as well; the Amazon site is a good example of this, as it (unusually) provides fairly good functionality without cookies, but popular features such as the "shopping cart" and "your preferences" do disappear. Many sites simply fall over if the user chooses to "turn off" or delete the persistent cookies for that site cookies. So depending on the interpretation of "strictly necessary", this provision may well be an open invitation to bypass the requirement of consent at all - in other

[91] This survey is unfortunately no longer available on the Web but can no doubt be obtained from the Information Commissioner's office.

[92] The NCC survey *Consumer Privacy in the Information Age* (December 1999, PD65/L/99) spoke to focus groups of consumers about privacy, and one of their strongest resulting findings was that consumers did not like the current variation in how consent is sought by tick boxes, and felt opt-in was much more in the best interests of consumers than opt-out. The report attaches a model standardised tick box format.

words, to retain the *status quo*. What it should do, however, is clearly distinguish between the setting of site-specific cookies (eg when Amazon sets an Amazon cookie), and the setting of third party cookies by the likes of DoubleClick[93]. Since such ad-server cookies are invariably set invisibly, and not at the request of the consumer (for who would explicitly request ads?) it seems these cannot be covered. Hence it appears European consumers will in future have to be persuaded at least *not to opt out of* receiving cookie-enabled advertisements, at least once - an interesting opportunity if consumers are informed enough to grasp it[94]. In fact however, the majority of Internet ads are now served without the use of third party cookies at all, as popular browsers, such as later versions of Microsoft's Internet Explorer, are usually now set to block third party persistent cookies, using built in P3P[95] controls. The most pressing need to regulate cookies in the interests of consumer privacy may in fact thus have already come and gone. Again, as with the spam problem, the cookie problem seems to have been solved (or at least on the way to solution) more effectively and speedily by "code" than by law.

The UK government has indicated in its consultation document and subsequent regulations for implementing the Privacy Directive[96] an approach which is, in this writer's opinion, disappointingly un-privacy friendly. On the question of *how* consumers should be offered the right to refuse cookies, the Regulations are entirely silent, except for asserting that the right to refuse cookies need not be offered more than once. The Information Commissioner's guidance suggests that the requirement to offer a way of refusing cookies can in fact be met if websites merely offer guidance on how consumers might use the facilities of their browser program (eg Internet Explorer, Netscape, Safari or Mozilla) to reject cookies[97]. This seems entirely inadequate to provide most consumers with a "user friendly" way to vindicate their legal right to refuse. The position is muddied further in the UK regulations where the consumer is using a computer while at work; here it seems the person with the right to refuse cookies may well be the employer, as well as the employee/consumer - and whose wishes should prevail in the case of conflict is not entirely clear[98]. On the question of what is "strictly necessary" in

[93] See further Edwards and Howels, supra n 89.
[94] Of course most consumers ads are served to US web sites from US ad servers and hence at least in practical terms outside EC jurisdiction.
[95] P3P is the Platform for Privacy Preferences, a software means to (*inter alia*) control cookies. See discussion in Edwards L "Consumer Privacy, On-Line Business and the Internet: Looking For Privacy in All The Wrong Places" (2003) 3 IJLIT 226.
[96] Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426 and *Implementation of the Directive on Privacy and Electronic Communications*, DTI, March 2003, URN 03/762, at http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html.
[97] *Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003, Part 2: Secuirity, Confidentiality, Traffic and Location Data, Itemised Billing, CLI and Directories*, para 2.4.
[98] *Guidance*, para 2.6.

response to a request by the consumer, the Regulations again say nothing, although the guidance notes do specify that "*such storage of or access to information should be essential as opposed to reasonably necessary*" and most importantly, cookies must be set "... for the provision of the service requested by the user, *rather than what might be essential for any other uses the service provider might wish to make of that data*."[italic added][99]. This looks a lot like the cry of "essential!" cannot be co-opted for cookies which are there merely to enable third party advertising (or even advertising directly provided by the website owner?) , as that is *not* usually the service the user was requesting.

What next?

Locational and traffic data

Spam and cookies are no longer the only privacy invading technologies (PITs) in the e-commerce market. The most novel parts of the PECD relate to control of locational and traffic data, where their use by service providers might have negative impacts on consumer privacy. Locational data broadly refers to information that reveals the whereabouts of the user of a mobile phone or similar telecommunications device whose location can be traced and shared. It can also includes information as to *when* a particular user was using a mobile phone at a particular location. Traffic data is data processed by the provider of an electronic communications network (such as a telecommunications or cable company or ISP) which relates to routing, duration or time of a communication.[100] While traffic data has long been collected by telcos and ISPs for the purposes of billing, capacity management, and other internal procedures, locational data is a relatively new concept. It is hoped that exploitation of locational data to provide "value added" services to mobile consumers will usher in a new profitable wave of mobile e-commerce ("m-commerce"). Locational data can be shared with or sold by the company originally collecting the data, to third parties who wish to provide services to users such as, eg, taxis, or fast food, or flowers. Typically, the third party service providers would use the locational data to provide the user with either information or the actual goods or services from the physically nearest relevant outlet. Locational data might also conceivably be used to serve relevant ads to mobile consumers direct to their phone, or even

[99] *Guidance*, para 2.5.
[100] Full definitions of both terms for UK purposes can be found at reg 2 of the UK PECD Regulations. Interestingly the UK definition of "locational data" is wider than that stipulated by the PECD itself.

hypothetically to direct tailored ads at computer-equipped billboards the consumer is passing by – the "intelligent billboard" concept.

In principle both traffic data and locational data have their quite proper, and potentially profitable, reasons to be collected. But they can also be privacy-threatening technologies. It hardly needs to be elaborated how useful it might be to a government, or an individual stalker, or a criminal, or a commercial competitor, to know exactly where a mobile phone user is; or who exactly a telephone subscriber has rung in the last month; or what websites they visited via their ISP and what individual pages they visited and what search terms they entered into a search engine. All this information can fall under locational and traffic data. When such data is stored and archived for long periods, rather than as is currently industry practice, deleted relatively fast when its billing or commercial purposes are done with, the potential privacy violation implications become even more severe. Yet in the post 9/11 world, enormous pressure is being put on telcos and ISPs, both by law and by extralegal means, to store and retain exactly such data for periods well beyond existing commercial good practice, in the interests of future hypothetical criminal or national security investigations. The balance between security and privacy is finely drawn in this area, and thus the regulation of traffic and locational data in particular is increasingly controversial. The data retention regime of the UK *for security and law enforcement purposes* is currently prescribed principally in the Regulation of Investigatory Powers Act 2000 and its subsidiary regulations, and is beyond the scope of this chapter; but it is worth noting that if the PECD restrictions on use of traffic and locational data noted below come into conflict with national security and law enforcement powers, then it is clearly the latter which win[101].

The PECD and the UK implementing Regulations do explicitly attempt for the first time to place limits beyond those of general DP law on how traffic and locational data can be processed. Art 9 of the PECD provides that locational data can only be processed, which includes use, sale and sharing, with the consent of the user or subscriber, and only where it is necessary to provide "value added" services. The key exception to this is if the data is anonymised. Furthermore, the service provider collecting and processing the locational data must inform the user or subscriber *prior* to obtaining consent of what the locational data may be used for – eg, what third party it might be given to provide "value added" services, and for how long. Users must also have the option to "opt out" of releasing locational data at any

[101] UK PECD Regulations, regs 28 and 29.

particular point, even if they have given this prior consent. The consent required thus resembles the positive opt-in required for spam more than the consent required to receive cookies, and thus reflects serious concerns about how locational data might be used.

Traffic data processing is also restricted. Traffic data, according to reg 8 of the UK PECD Regulations, can only be collected for limited purposes defined as:

- management of traffic or billing;
- customer enquiries;
- prevention of detection of fraud;
- the marketing of electronic communications services[102]; or
- the provision of a value added service.

As discussed, a "value added service" is an extra service provided to a user/subscriber by use of locational or traffic data – possibly by a third party other than the telco or ISP. It is technically defined as any service which requires the processing of traffic data or locational data beyond that which is necessary for the transmission of a communication or the billing in respect of that communication[103].

Even when traffic data falls within one of these permissible categories, further restrictions apply[104]. If it is to be processed for the purpose of marketing electronic communications services, or to provide value-added services, the user or subscriber to whom the data relates must give their consent. This consent may be withdrawn at any time. Even then, the data must be processed and stored only for the duration necessary for the relevant purpose. Aside from these particular exceptions, the general principle is re-stated from general DP law that when traffic data has fulfilled its function – it aided the transmission of a communication – it should be either deleted or anonymised[105].

The future?

The outstanding question remaining is, is the PECD really "technology neutral"? Does it update the DPD with sufficient generality to protect consumer privacy against all foreseeable

[102] As defined by s 32 of the Communications Act 2003.
[103] UK Regulations, reg 2(1).
[104] Ibid, reg 7 (2)(3)(4).
[105] Ibid, reg 7(1).

threats arising from new technologies? Sadly, the answer already seems to be no. One type of technology currently under much scrutiny from privacy activists worldwide is the RFID chip. RFID chips are tiny microchips attached to an antenna that receives and transmits location information by means of radio waves. RFID chips are small, very cheap (costing around 6p each), come in many varieties, and are currently used for a multiplicity of commercial purposes[106]. Most commonly, they are used for product tracking and inventory control, access control to sealed areas ("smart doors"), contact-less smart cards (eg the Oyster card used by London Transport commuters) and animal tagging. More novel applications include using it as a hands-free payment mechanism[107] and people-tagging[108]. Most consumer concern around RFID has centred on their use in high street stores, basically as a more advanced form of bar-code. If RFID tags, which are very small, are attached to, say, shirts, and not removed or de-activated at point of sale, whether deliberately or by accident, then the fear of privacy advocates and consumer groups is that they will operate as a sort of micro-bug, revealing the whereabouts of the buyer to unknown parties for an indefinite time after sale. In fact, RFID chips themselves usually carry no information except the inventory code and description for the particular item to which they were attached, and thus in themselves, do not identify the buyer, nor disclose personal data describing the buyer. However the identity of the buyer *could* conceivably be discovered if the RFID data was associated at point of sale with the personal identifying details of the buyer derived who bought the item using a means such as credit card, smart card or store card. Although this kind of scenario has caused a great deal of angst both in the US[109] and Europe[110], the privacy concerns are actually rather limited. RFID chips are usually passive : that is, they do not broadcast their location as such, but need to be *detected* by readers at very short range, usually no more than six or seven metres away (many need even closer range[111].) RFID readers cost £250 - £3000 each and therefore it is

[106] See useful overview of RFID chip technology available at http://www.philips.com; also Brown A "RFID: An Unlawful or Just Unwanted Invasion of Privacy?" (2003-2004) Computers and Law December/January 27.
[107] See Morton S "Barcelona Clubbers Get Chipped", 29 September 2004, at http://news.bbc.co.uk/1/hi/technology/3697940.stm.
[108] See description of tagging of school children in Tokyo to reassure parents, reported widely October 2004, eg http://www.cbsnews.com/stories/2004/10/11/tech/main648681.shtml . Anecdotal reports also exist of the RFID tagging of often absent academics in one US university so that they could be speedily located.
[109] See the site of CASPIAN, Consumers Against Supermarket Privacy Invasion and Numbering at http://www.nocards.org/, which asks, "Is Big Brother in *your* grocery cart?".
[110] See "Consumer Concern Over RFID Cards" , at http://news.bbc.co.uk/1/hi/technology/4247275.stm, 9 February 2005, which claims that 50% of UK consumers polled were very concerned about the use of RFID in shops.
[111] RFID should not be confused, as it often is, with GPS , the Global Positioning System, which uses satellite technology to track locations or persons or objects from very great distances. RFID chip, by comparison to GPS systems, are extremely cheap and small and thus far more suitable to the inventory and stock control of many millions of manufactured items – however this cheapness comes at a price, in that the passive RFID chip can only be read at a very close distance by a specialised reader. Non-passive RFID chips, which have their own power supply and can broadcast over a wider range, do exist, but are currently too large and expensive to be used in most commercial applications.

impractically expensive for RFID tags to be used as "bugs" except within a relatively small and circumscribed area like a school, supermarket, library or campus.

The question of how far RFID chips are truly a significant threat to consumer privacy is not however the point here. What is germane is that it is not at all certain if RFID technology is controlled by data protection law, even as updated by the PECD, and if it is, *how* it is so controlled[112]. As noted, RFID chips themselves do not contain "personal data", ie information identifying a living person. An RFID chip attached to a Gillette razor blade typically reveals nothing other than "I am pack 23340000 [say] of this type of razor blades", sometimes with additional shelving, inventory, expiry date or supply chain history information. As such, *prima facie* RFID chips do not fall within the UK DP regime as it applies only to data which "*relates to a living individual who can be identified*" (DPA 1998, s 1). However as noted above in relation to spamming, conceivably RFID processing does fall within the data processing regime if the RFID chip data *taken with* credit card details (say), do, in the point-of-sale scenario described above, combine to identify a living individual. (The second part of the definition of "personal data" in s 1 of the 1998 Act, it should be recalled, includes the case where a living individual can be identified from the data in question and any other information which is "*likely to come into the possession* of the data controller".) If this were to be the case, the DPA 1998 duties of fairness in data processing, as laid down in the Eight Data Protection Principles[113], might apply to some but not all data processors operating RFID chip systems in shops. So, for example, if Tesco's, the supermarket chain, attach RFID chips to the packets of razor blades they sell in order to monitor and prevent shoplifting, and legitimate buyers of razor blades pay by electronic means, then conceivably Tesco's will be able to tie the individual buyer to that packet of razor blades as it leaves the shop, and thus will be processing personal data during and after the purchase[114]. In that case, they might fall under duties including the need to give adequate notice of processing to consumers so as to obtain implied consent; they would have to notify the purposes for which they were collecting the data; and the security implications might have to be considered[115]. But if payment is made

[112] There is a small but growing legal literature on RFID. See Brown supra n 106; Ustaran E "Data Protection and RFID Systems" (2003) Privacy and Data Protection 3.6(6); the Ontario Privacy Commisioner has published legal guidelines on using RFID tags in libraries at http://www.ipc.on.ca/docs/rfid-lib.pdf . In Europe, the EU Art 29 Working Party has published as Working Document on RFID, 10107/05/EN WP 105, January 19 2005, at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf .

[113] Data Protection Act 1998, Schedule 1, Part II.

[114] See BBC website, "Big Brother at the supermarket till?", 27 January 2005 at http://news.bbc.co.uk/1/hi/business/4211591.stm .

[115] Fuller consideration of how the DP Principles might apply to processors using RFID chips can be found in Art 29 Working Party Document on RFID, supra n 112.

with cash, and Tesco's remove the tags at point-of-sale (as Marks and Spencers did, in their RFID test trials with clothing, to the approval of privacy activists) do any DP implications arise? Perhaps not. The area is grey in the extreme.

A further complicating factor is whether RFID tags fall under the new "locational data" regime in the PECD described above. Locational data is technically defined solely as " any data processed in an electronic communications network *indicating the geographic location of the terminal equipment of the user* of a public electronic communications service". As Brown notes, it is hard to say that an RFID tag – or even the goods to which it is attached or embedded – are "terminal equipment of the user"[116]. Undefined in the UK PECD Regulations, the obvious natural language interpretation would be that it refers to a mobile phone handset, a handheld PC, a laptop, or the like. The PECD also fails to define "terminal equipment" and interestingly, recital 35 of the PECD seems to imply that all locational data is also traffic data , ie data used to facilitate electronic communications– which makes it look even less like the kind of data stored in RFID chips or collected using them. RFID chips fundamentally track *objects* (including people); traffic data tracks electronic communications or *messages*. Yet if RFID chips are to fall within the DP regime, it would seem only sensible that they also fall within the locational data regime. What RFID does, then, is show that the supposedly "technology neutral" regulation of the EC's latest Privacy Directive falls down badly as soon as applied to even the first major commercial privacy-invasive technology to be developed since cookies.

To add insult to injury, the scenario explored so far, of RFID in supermarkets, is one where it is relatively easy to minimise privacy violations by simple means such as removal of the tags before the purchaser leaves the store. What of the more novel applications of RFID mentioned above, such as tagging of children, and of hospital patients, and even the already common use of contact-less RFID-chipped smart cards in business HQs and on public transport?[117] In these scenarios, the RFID chip persists and stays active and associated with the card-holder, and the privacy risks seem much higher.

[116] Ustaran (supra n 112) however seems to take the view that RFID tags do constitute "locational data". Interestingly though, the Art 29 Working party document, also supra n 112, does not take a view on whether RFID tags collect or constitute locational data, though the document does assert that in many concrete cases, data processed via RFID tags *will* constitute "personal data".

[117] Out-Law.com reports at 14/10/2004 that the US Food and Drugs association has approved the implant sub-dermally of RFID chips into patients so that they can be used to access what drugs the particular patient needs, with less chance of

In conclusion then, the terrain we have surveyed above, of the legal regulation of privacy-invasive technologies such as spam, cookies, traffic data and RFID, is not an inspiring one for lawyers and legislators. Law faces many problems in this area; the problems of jurisdiction, of enforcement, of trans-nationality, of making the public aware of and comprehending of their rights; of financing and training of enforcement authorities, and of interpretation when new technologies or new tweaks on old technologies come along. Overwhelmingly, the conclusion cannot be resisted that law will always be running behind technology in this area and that solutions may perhaps best be found not in new legislation, but in international and business investment in technical standards and development. Spam has not been arrested in the slightest by international legal developments but may be decimated in a few years if changes are made to the basic Internet and email technical standards. Cookies were argued over sempeternally in the European Parliament, but now as of early 2005 are almost a forgotten problem for technologists, and third party advert serving is almost a thing of the past. RFID is the new privacy problem on the block and already has muddied the new legislation which might have been hoped to control it in advance. Real control of privacy invasion by RFID is more likely to come from good practice in the commercial sector or a supervening technology which (say) blocks or de-activates RFID chips, than DP law reform. As Lessig might have said, it is easier to fight code with code, than code with law. Indeed, code usually trumps law. It will be interesting to see if in five years time the legal framework for the protection of consumer and citizen privacy in Europe from technological threat has begun to recognize this hard truth. We need more, cheaper and easier to use privacy-enhancing technologies and less new law: discuss.

human error. They could also recognise and record data about allergies.