How functional is the current law and legal policy regarding unsolicited bulk email or "Spam", and how should it develop in future?

An industrial expert recently stated that according to their observations 97% of all e-mail sent in 2008 was unsolicited bulk e-mail, otherwise know as "spam" [1]. E-mail forms one of the supporting pillars of the "Internet economy" such that its abuse causes major economic detriment, and wider harm to the Information Society. In fact the European Commission estimated that in 2005 the global cost was €39 billion[2]. This problem was initially addressed by the European Commission in articles 20-22 of the E-Privacy Directive 2002[3] to regulate the transmission of communications for "direct marketing purposes". This directive was transposed into British law a month late in the 2003 Act[4] and outlawed the transmission (and the instigation of transmission) of "unsolicited communications for the purposes of direct marketing" via electronic mail unless the recipient had explicitly given prior consent[5]. It also granted rights to claim for damages for parties injured by contravention[6], and granted the Information Commissioner enforcement powers[7]. However only 2 claims for damages have appeared before the courts since the introduction of the Act[8], and spam levels have grown exponentially in quantity[9] and severity. In late 2005 the EC called for new action to deal with this evil, including the need for new legislative efforts to fight Spam[10].

---

[1] Sophos Plc, *Security threat report: 2009* (Jan 2009), accessed on 3/1/2009 at https://secure.sophos.com/security/whitepapers/sophos-security-threat-report-jan-2009-na.
[2] Commission of the European Communities, Fighting spam, spyware and malicious software, COM (2006) 688 final (Nov 2006).
[3] Directive on privacy and electronic communications 2002/58/EC.
[4] The Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003 No. 2426.
[5] Ibid, reg 22.
[6] Ibid, reg 30.
[7] Ibid, reg 32.
[8] *Microsoft Corp v McDonald (trading as Bizads)* [2006] EWHC 3410; *Roberts v Media Logistics (UK) Ltd* (Unreported, October 19, 2005) CC (Colchester).
[9] 7% of global e-mail was estimated to be spam in 2001, 29% in 2002, and 51% in 2003. See Commission of the European Communities, Unsolicited commercial communications or 'spam', COM (2004) 28 final (Jan 2004), p. 5-6.
[10] EC Communication, COM (2006) 688 final (Nov 2006).

This essay will evaluate the effectiveness and appropriateness of the current law regulating spam email in this jurisdiction, and from these findings recommend how it should develop. Unfortunately due to the limited case law there is very little common law precedent in this area, although the lack itself speaks volumes. Therefore, this essay must primarily seek to analyse the legislation, and the underlying policy that it enunciates. The extent to which the law plays its part in complementing the technological and social measures will be evaluated, using evidence from sources of law, commentary and technical concepts, to see how a holistic solution can be achieved. In this way the case study should also provide some useful insights into how best to approach other interfaces between technology and the law.

The legal problem can be crystallised as the tension between the rights to freedom of speech, privacy, and property, of the spam sender, recipient, and network provider respectively. The Data Protection Act 1998[11] introduced regulations governing the use of "personal data" including e-mail addresses, giving persons the right to some measure of control over how their personal information is stored and used, and so the transmission of an unsolicited e-mail can be an invasion of informational privacy. Furthermore, article 8 of the ECHR[12] gives a person the right to some measure of relational privacy, which has been said to be infringed by the reception of large quantities of unwanted messages[13]. In fact the DPA gives an individual the right to require that a data controller cease processing their information for direct marketing, after notifying them in writing[14]. However, completely preventing the dissemination of such messages would constitute a restriction of the marketer's transient entitlement to freedom of speech and expression[15]. Thus there is a tension that has to be

[11] Data Protection Act 1998.
[12] European Convention on Human Rights, Article 8.
[13] Kabel, J, 'Spam: A Terminal Threat to ISPs? The legal position of ISPs concerning their Anti-Spam Policies in the EU after the Privacy & Telecom Directive' (2003) 1, *Computer Law Review International*, p. 6.
[14] DPA 1998, reg 11.
[15] European Convention on Human Rights, Article 10.

addressed to preserve the economic benefits of e-mail marketing whilst placing restrictions on it to protect user privacy. These principles, along with economic and political factors led to the "opt-in" system introduced by the Directive[16] so that marketers can only send such communications where the recipient has given prior notification of their consent or are existing customers, and where they can "opt out" of later transmissions.

Despite the EC's efforts, the directive has not achieved a fully harmonised framework to regulate spam across the community. Member States have utilised the full spectrum of flexibility in their implementations and have completely divergent provisions for enforcement, making cross-border collaboration complicated. The implementation in the UK is one of the most liberal. The wording of regulation 22(3) even contravenes the directive by extending the exception allowing marketing e-mails for similar products to be sent without prior consent. The directive permits this where contact details are obtained "in the context of the sale of a product or a service"[17], but the domestic implementation replaces this with those obtained during "negotiations for [a] sale"[18]. This was affirmed by the Information Commissioner (ICO), by stating that a contract of sale need not have been concluded, but instead e-mails could be sent where an individual "actively expressed an interest"[19] in purchase. This makes the exception much wider, so for example, even addresses obtained as part of a competition would be considered usable[20]. Contrary to the Opinion of the Article 29 Working party[21] the ICO's policy also states that e-mail addresses collected without prior consent before December 2003 may continue to be used on an opt-out basis[22]. These

[16] E-Privacy Directive 2002/58/EC.
[17] Ibid, Article 13, subsection 2.
[18] E-Privacy Regulations 2003, SI 2003 No. 2426, reg 22, subsection 3a.
[19] Information Commissioner's Office, *Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003* (2007), p. 21.
[20] Asscher, L, Hoogcarspel, S, *Regulating Spam* (The Netherlands, Asser Press, 2006), p. 89.
[21] Article. 29 Working Party, 2004, p.6.
[22] Information Commissioner's Office, *Guidance for marketers on the Privacy and Electronic Communications (EC Directive) Regulations 2003* (2007), p. 25.

interpretations have been argued to result in an "opt-out regime" [23], like that of the USA[24]. Neither does Article 13 make any reference to the quantity of e-mail that may be sent once opted in. The majority of Member States have chosen to use their freedom to only require an opt-in system for non-natural persons such that businesses are not protected under the legislation[25]. However, despite the obvious weakening that these limitations cause, these observations alone cannot be used to evaluate the law's overall effectiveness.

In fact the 2003 Act has been successfully used to claim damages from "spammers" on two occasions in this jurisdiction. The first of these, Roberts v Media Logistics[26] in 2005, awarded the claimant damages of £300 against the defendant, for sending unsolicited e-mails to the claimant. Then a year later, in Microsoft v McDonald[27], the appellant was awarded damages and an injunction, in a summary judgement, against a supplier of e-mail address lists, for instigating the transmission of spam to many of the plaintiff's subscribers, thus causing damage to their "goodwill" and the need for considerable expenditure on anti-spam infrastructure. Though only a summary judgement, this case gave interesting insights into the interpretation of the statute, indicating that the class of potential claimants was not limited to individuals but could also include service providers, that remedies beyond £5000 damages including injunctions could be granted, and that damages could be successfully claimed for instigation rather than direct transmission. Thus it would seem that the law can be used remedially, although whether these cases were typical or atypical is not clear. In both, the amount of evidence available to the claimant seemed unusually favourable, particularly as Microsoft's use of a fake "spam trap" address proved that the e-mail addresses were acquired without consent. It is not clear whether the burden to prove whether consent was given lies

[23] Asscher, L, Hoogcarspel, S, *Regulating Spam* (The Netherlands, Asser Press, 2006), p. 89.
[24] CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq), USA
[25] Munir, A, 'Unsolicited commercial email: implementing the EU Directive' (2004) 10(5), *C.T.L.R.*, p. 109.
[26] *Roberts v Media Logistics (UK) Ltd* (Unreported, October 19, 2005) CC (Colchester).
[27] *Microsoft Corp v McDonald (trading as Bizads)* [2006] EWHC 3410.

with the claimant or defendant, but should it lie with the claimant it may be difficult to prove that consent was not given, although failure to comply with opt-out requests would be self evident. However, even then most of those harmed would have insufficient powers to be able to identify the true sender of a spam email, which calls into question the appropriateness of encouraging action to be brought in tort by victims, when sufficient evidence may be inaccessible to them. Unfortunately beyond these cases and the ICO's policy, no further light can be shed on the interpretation of the UK legislation as there have been no other cases, in the E-Privacy Act's 5 year lifetime.

This void could be interpreted as a success, if it weren't for the fact that the UK is still ranked as the 4th worst spamming nation in the world by a respected independent organisation[28], the EC's numerous requests for further action[29], and the ICO's frustration at their under financing and inadequate enforcement powers[30]. In fact the ICO has not brought a single action against a spammer, and the law has been widely criticised for not providing an adequate deterrent, granting insufficient enforcement powers to the ICO, and for not implementing preventative measures. Worst of all the under girding assumption that spam is predominantly advertising; an annoyance instigated by legitimate business, is now archaic. Spam is a vector for criminal activity[31], and has been termed "one of the two principle engines of Internet crime"[32]. Not only are vast amounts of malicious software being sent via bulk e-mail to infect victim's computers[33], but a plethora of scams and frauds are being instigated[34], and they work. In 2006

[28] SPAMHAUS, Statistics, accessed on 01/01/2009 at http://www.spamhaus.org/statistics/countries.lasso.
[29] Commission of the European Communities, Fighting spam, spyware and malicious software, COM (2006) 688 final (Nov 2006).
[30] Information Commissioner's Office, *The Directive on Privacy and Electronic Communications (2002/58/EC) DTI Consultation – The Information Commissioner's Response* (June 2003), pp. 5-6.
[31] Federal Trade Commission, *FTC Spam Summit: The Next Generation of Threats and Solutions* (Nov 2007).
[32] Hallam-Baker, P, *dotCrime Manifesto: How to stop internet crime* (Addison-Wesley, Boston, 2008), p. xxi.
[33] According to Sophos every 1 in 200 emails contained some malicious software in September 2008. See Sophos Plc, *Security threat report: 2009*, (Jan 2009).
[34] Statistics available from the Anti-Phishing Working Group, show that in January 2008, 29284 attacks were reported. Accessed on 1/1/2009 at http://www.antiphishing.org/resources.html.

the USA's Internet Crime Complaint Center received 207,492 complaints of such scams leading to reported losses of over $194 million[35]. A report published by Financial Insights, estimates that global financial institutions alone lost $400 million or more in 2004 due to phishing schemes[36]. So although the law sets up a framework for legitimate marketers, to maintain freedom of expression, it appears that it currently fails to facilitate a practical reduction in illegitimate messages.

The DTI's current policy is that the onus is on the individual to ensure their own Internet security[37], but this has been criticised as unrealistic, especially as socially many frauds are very convincing and technically there are no complete security solutions[38]. In the words of the House of Lords report on Personal Internet Security this policy only "compounds the perception that the Internet is a lawless wild west"[39]. The legislature therefore has a responsibility not simply to regulate legitimate business entities, but to implement a combined punitive and preventative policy to target the "vast majority"[40] of illegitimate ones.

The kernel of the legal dilemma is therefore no-longer how to balance privacy and freedom of expression, but rather how to enforce it, and specifically how the law can function effectively in a technological setting. The current law severely hampers the enforcement ability of the ICO, only permitting the sending of enforcement letters, and fines up to £5000; a fraction of the income of a successful spammer. Unlike the Dutch system[41], the ICO has no

[35] IC3, Internet Fraud Crime Report 2006 (2006), p. 3.
[36] IDC, *Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc*, (Nov 2005).
[37] House of Lords, Science and Technology Committee, *5th Report of Session 2006–07 Personal Internet Security* (Aug 2007), p.24.
[38] Ibid p.25.
[39] Ibid p. 6.
[40] Johnson, B, 'Spam watchdog calls for more powers' *The Guardian,* 9 Febuary 2006.
[41] Telecommunications Act 1998, The Netherlands, Article 18.7.

power to compel ISPs[42] to release customer identities, and even if sufficient evidence can be obtained the ICO must send two enforcement notices[43] before criminal prosecution carrying a fine can result[44], and this may be appealed to the Information Tribunal free of charge[45]. Most companies appeal, and the tribunal can take months to convene, whilst in the meantime the ICO has no powers to obtain an injunction to stop spam being sent[46]. In their 2004 annual report the ICO commented that their "existing enforcement powers are inappropriate" and expressed the desire for "some form of injunctive power"[47], however no such powers have been granted. Improvements should therefore begin by fulfilling the ICO's original requests, to amend s43 of the DPA to require service providers to disclose the information necessary to identify an offender, and introduce provisions modelled on the Stop Now Orders provided for in the EC Directive[48] to enable the Commissioner to apply for a court order to cease non-compliant conduct in clear cut cases[49]. Increasing sanctions to larger fines and possible imprisonment may also prove effective, indeed Australia's provision for this has been highly commended[50]. This has also proved effective in the USA as their contribution to world spam has significantly reduced[51].

Of course with the severity of some of the crimes, the question arises as to whether data protection agencies are the right choice for enforcement? There is an argument that much spam would be better dealt with entirely under criminal law, due to the greater investigative

[42] Internet Service Providers
[43] DPA 1998, reg 40.
[44] Ibid reg 60(2)
[45] Ibid reg 48
[46] Asscher, L, Hoogcarspel, S, *Regulating Spam* (The Netherlands, Asser Press, 2006), p. 98.
[47] Information Commissioner's Office, *Annual Report and Accounts for the year ending 31 March 2004* (July London, The Stationery Office, 2004), p. 42.
[48] Stop Now Orders (EC Directive) Regulations 2001, SI 2001 No. 1422.
[49] Information Commissioner's Office, *The Directive on Privacy and Electronic Communications (2002/58/EC) DTI Consultation – The Information Commissioner's Response* (June 2003), pp. 5-6.
[50] Vine, S, 'Is the end neigh for spam?' (Feb 2005) 7 *E.B.L.* 1-9.
[51] Sophos reports that the USA's contribution to global spam has reduced from 26.8% in 2004 to 17.5% in 2008, whereas the UK's contribution has doubled in that time (1.51% to 3.1%). See Sophos Plc, *Security threat report: 2009* (Jan 2009) and *Security threat report: 2004* (Jan 2005).

and punitive powers available, but there is currently no single complaint centre, comparable to the USA's IC3[52], to investigate these more serious complaints. The FTC[53] in the USA support this view saying that "criminal authorities are best suited to tackle the problems of malicious spam and phishing"[54]. This would cost the state, however, the "high volume, low denomination"[55] nature of the crime mandate state intervention as it is improbable that any individual's losses would be claimable, when national losses could be huge.

The existing infrastructure for international cooperation and information sharing also make criminal agencies appropriate. Enforcement is often hampered due to insufficient mutual investigative and information sharing powers. The EC has highlighted the importance of international cooperation, and has started the "SpotSpam" service for this very reason to provide a centralised point of communication[56]. However the law doesn't allow the ICO to share information, investigate for foreign agencies, or guarantee the confidentiality of reciprocal information it requests. It was suggested in the Lord's report that the laws of evidence could be relaxed in this context, to allow evidence to be given from outside the country concerned[57]. The implementation of legislation mirroring the much praised "US SAFE WEB Act"[58] could drastically improve cooperation through: broadening reciprocal information sharing, expanding investigative cooperation, and authorizing expenditure of joint projects[59]. The common argument that the majority of the world's spam originates outside the UK can be said of every country of the world, and the domestic problem cannot

[52] The Internet Crime Complaint Center (IC3), see http://www.ic3.gov/.
[53] The Federal Trade Commission, see http://www.ftc.gov/.
[54] Federal Trade Commission, *FTC Spam Summit: The Next Generation of Threats and Solutions* (Nov 2007).
[55] Ibid.
[56] The SpotSpam Project, see http://www.spotspam.net/.
[57] House of Lords, Science and Technology Committee, *5th Report of Session 2006–07 Personal Internet Security* (Aug 2007), p. 75.
[58] U.S. SAFE WEB Act of 2006, USA.
[59] Federal Trade Commission, *The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud, A Legislative Recommendation to Congress* (June 2005).

be solved without sufficient statutory powers and funding to enable international collaboration.

However legal reform to encourage and empower enforcement would not be sufficient without facilitating prevention. The core problem in the e-mail is the lack of accountability, and thus the ability to shirk one's responsibilities. Technological reform must address this, but legal incentives can be given to encourage it. The development of "domain authentication" technologies is the most hopeful solution to the spam problem as they authenticate whether a message genuinely originated from the internet domain it claims to. This can prevents the falsification of an e-mail's sending domain, such that e-mail filtering can be based on a domain's reputation, and thus forces e-mail service providers to proactively reduce the amount of spam they relay. However for this to be effective service providers must adopt it. In 2007 ENISA reported that according to their surveys most providers spent more time on filtering spam than on its elimination, and although almost 50% of service providers allowed others to use these technologies to authenticate their domains, only 5% actually made use of this to check incoming e-mail[60]. Procedures to react to complaints were said to be poor, but proactive methods to prevent customer's sending spam looked more promising, with 50% of providers preventing their customer's sending spam without authentication by managing "port 25" through which it is sent[61]. This so called "egress filtering" if more widely deployed could have a drastic impact as almost all spam is now sent through hijacked computers called "bots" which would be unable to relay spam if port 25 were blocked.

Although these technical measures could be very effective, they are inadequately implemented because they are selfless and don't directly help their customers, but rather

[60] ENISA, Manzano, P, Rossow, C, *Provider Security Measures, Survey on Security and Anti-Spam Measures of Electronic Communication Service Providers* (Sept 2007), pp. 9-10.
[61] Ibid pp. 11-12.

reduce the spam sent to their competitor's customers. There is therefore the need for intervention to encourage the adoption of such altruism. In fact aligning responsibility to those with the ability to act[62] to gently steer the development of technology for the betterment of all stakeholders (not just the industry's), may prove to be an important strategy in regulating other areas of technology. The Lords have suggested that this should be achieved by introducing best practice kite mark schemes, and by removing the "mere conduit" immunity implemented in the Electronic Commerce Directive regulations[63] "once ISPs have detected or been notified" [64] that machines on their network are transmitting spam. This should "give third parties harmed by infected machines the opportunity to recover damages from the ISP responsible", although "they should enjoy a time-limited immunity when they have themselves detected the problem" so as not to discourage the monitoring of outgoing traffic[65]. Although it has been argued that this would violate the "end-to-end" principle[66], it would really only confer a duty to react to complaints, and so, for example, is very different to the filtering copyrighted material addressed in the recent Sabam vs Tiscali[67] case. However such a reactive approach may prove ineffective in practice, and despite the time-limited immunity could significantly discourage service providers from trying to detect problems themselves.

The problem is one of incentive. Though the "mere conduit" immunity is fair in principle, the current wording of regulation 17 is counter productive in that it actively encourages service providers to take a "hands off" approach, since if they begin to monitor and manage outbound

[62] Hallam-Baker, P, *dotCrime Manifesto: How to stop internet crime* (Addison-Wesley, Boston, 2008), p. 368.
[63] The Electronic Commerce (EC Directive) Regulations (2002) SI 2002 No 2013, reg. 17.
[64] House of Lords, Science and Technology Committee, *5th Report of Session 2006–07 Personal Internet Security* (Aug 2007), section. 3.68-3.69.
[65] Ibid section 3.69.
[66] Wright, T, Hodgkinson, D, 'House of Lords Science and Technology Committee Report on personal internet security' (2008) 14(1) *C.T.L.R* p. 14.
[67] *Sabam vs Tiscali (Scarlet)* Belgium. 2007.

traffic, they may be accused of being publishers, and suddenly find themselves liable. Similarly if the law made service providers directly liable for the continuing transmission of illegal data once detected, there would be a tendency to cease monitoring to evade liability. The problem is that although the "commandment is holy, righteous and good"[68] instead of encouraging the praiseworthy quality which it seeks to enforce; it often induces the opposite: trying to do the minimum possible to comply. Thus techniques are required which actively encourage those who have the ability to act, to do so. To this end a distinction should be drawn between liability arising due to the relaying of some harmful data, for which immunity is and should rightly be granted, and the responsibility of the conduit to take proactive technological measures to help prevent such data entering their systems. Currently there is a disincentive to do the latter and suggestions tend seek solutions by reducing the former immunity, but a more constructive approach may be to impose certain duties to take "reasonable care" in the latter. If instead of being made responsible to act when abuse is detected (and thus discourage detection), service providers were given a duty of care to take certain preventative measures (including egress filtering) or else be found vicariously liable, they would be encouraged to take practical steps to improve the infrastructure. If this were to be achieved, legislation like the Health and Safety Act[69] would need to be enacted to give these "mere conduits" a duty of care to employ various preventative measures, and under these circumstances to override the general common law rule laid down in Caparo v Dickman[70], whereby the relationship must be proximate for a duty to be found. This is important since for reform to be effective the incentive must be for the remote provider to prevent the sending of spam, rather than just for the receiving provider to detect it, and is legitimate as the requirements imposed would not be particularly onerous. Thus if spam was received from a negligent service provider who did not meet some agreed national standard,

[68] Romans 7:11.
[69] Health and Safety at Work etc. Act 1974 (c. 37).
[70] *Caparo Industries plc v Dickman* [1990] 2 AC 605.

they could be found vicariously liable for any damages caused to either peer service providers, or the recipients themselves.

In conclusion, the current law to regulate the sending of unsolicited bulk e-mail is grossly ineffective, not primarily because the law has no part to play its regulation, but rather due to inadequate enforcement powers based on an archaic understanding of the problem. Spam e-mail is now a conduit for criminal activity and so the government should repent of their complacency[71], heed the warnings voiced by the Information Commissioner and the Lords, and urgently review the enforcement powers and policy. It is important that the EU and Member States continue to investigate legislative reform that seeks to provide a harmonized framework for international enforcement with effective penalties and information sharing provisions[72]. Finally this example indicates that at the boundary between technology and the law, the law may be most effective when taking a complementary role in encouraging the adoption of preventative measures through assigning appropriate duties to service providers. This policy could also be considered for other contentious areas of Internet law like copyright regulation, such that service providers still aren't held liable for the acts of their user's, so long as they have implemented any preventative measures that they should reasonably be expected to employ.

[71] Wright, T, Hodgkinson, D, 'House of Lords Science and Technology Committee Report on personal internet security' (2008) 14(1) *C.T.L.R* p. 15-17.
[72] Commission of the European Communities, Fighting spam, spyware and malicious software, COM (2006) 688 final (Nov 2006).