SCRIPT-ed

Volume 1, Issue 3, September 2004

'Regulating' Online Data Privacy

Paul Reid[*]

Abstract

With existing data protection laws proving inadequate in the fight to protect online data privacy and with the offline law of privacy in a state of change and uncertainty, the search for an alternative solution to the important problem of online data privacy should commence. With the inherent problem of jurisdiction that the Internet presents, such a solution is best coming from a multi-national body with the power to approximate laws in as many jurisdictions as possible, with a recognised authority and a functioning enforcement mechanism. The European Union is such a body and while existing data protection laws stem from the EU, they were neither tailored specifically for the Internet and the online world, nor do they fully harmonise the laws of the member states – an essential element in Internet regulation. Current laws face further problems with the ease and frequency of data transfers outwith the EU. An Internet specific online data privacy regulation would fully approximate the laws of the twenty five member states and, if suitably drafted, could perhaps, drawing upon EC competition jurisprudence, achieve a degree of extraterritoriality, thus combating the problem posed by transfers outwith the EU. Any solution, however, is dependant upon our political leaders having the political will and courage to reach and agreement upon any new law.

DOI: 10.2966/scrip.010304.488

---

[*] The author is currently a postgraduate student at the University of Edinburgh. paulreid82@yahoo.co.uk The author would like to thank Andres Guadamuz, Josie Hayes and an anonymous referee for their thoughts, comments and suggestions on previous drafts of this article. They should not, however, be taken to agree with the arguments made and the usual disclaimers apply regarding the content.

1. Introduction

"All this shows that the flowing tide of Community law is coming in fast. It has not stopped at high-water mark. It has broken the dykes and banks. It has submerged the surrounding land. So much so that we have to learn to be amphibious if we wish to keep our heads above water."[1] Could Lord Denning equally have been talking about the Internet and its effect upon the law? It would be no exaggeration to say that the Internet has transformed the world we live in. It has transformed our access to information, our ability to communicate and has created a truly global market place. Yet, while we marvel at its wonder, has our privacy been swept away by this incoming tide, which shows no signs of retreating? Existing laws seem unable to cope with the size and trans-national nature of the Internet. Other areas of law, such as contract and conveyancing, must be reconsidered in light of developing technology. These changes are necessary to keep the law up-to-date with technology. Laws relating to privacy do not need to be updated, they require protection. Developments in technology are threatening the individual's right to privacy and the law, at present, appears unable to meet the challenge it is now facing.

To what degree privacy should be protected is a matter that has long vexed the law not just in this country. Data protection laws have been seen as a potential shield for online privacy, but with these coming under increasing criticism, they will be shown to be ill suited to the demands of the online world. With privacy law in a state of constant change and uncertainly, it is unwise to rely upon these laws to guard us from the ever increasing threat to our privacy each time we venture into the online world, primarily as it cannot be said with any great degree of certainly exactly what the law is today in this country, let alone tomorrow. Furthermore, the value placed upon privacy varies considerably from country to country. By its very nature, the Internet ensures that a country cannot act unilaterally to ensure an adequate degree of protection for their citizens. In effect, privacy can currently be dragged down to the lowest common denominator. While changes have been made to try and toughen the existing system, and proposals have been made to break from the present framework, what is required is a framework that offers identical protection in as many jurisdictions as possible, with an effective body to police and enforce the rules. The European Union, no doubt much to Lord Denning's despair had he still been alive, is such a body, and by taking a harder line on protecting individual rights, a Union "*founded on the principle of…respect for human rights and fundamental freedoms*"[2] could provide the solution.

2. Privacy Law

Although there is no general tort[3] of invasion of privacy, there are many statutes dealing with different aspects of the problem – the Data Protection Act 1998 being one such example. As Lord Hoffmann has observed, "*one of the less welcome*

---

[1] *Shields v E Coomes (Holdings) Ltd* [1979] 1 All ER 456, 462 (Lord Denning MR)

[2] Article 6(1) of *The Treaty on European Union*

[3] Much of the authority in this area comes from England and for simplicity the English 'tort' will be used as opposed to 'delict', although there would appear to be little difference between the law in either jurisdiction.

consequences of the information technology revolution has been the ease with which it has become possible to invade the privacy of the individual."[4] In the absence of an overarching tort of privacy, the courts have sought to fill the lacuna in the law by extending existing common law actions. Breach of confidence is one such action that has been morphed to the point that "*a confidential relationship has become unnecessary*."[5]

Privacy was an issue that gained a heightened prominence through the European Convention of Human Rights[6] and its implementation by the Human Rights Act 1998. Article 8 of the Convention provides:

> *(1) Everyone has the right to respect for his private and family life, his home and his correspondence.*

The entering into force of the Human Rights Act has in fact been said to weaken the case for the creation of a general tort of invasion of privacy[7] and it is clear that not every breach of privacy will lead to an award of damages by virtue of Article 8. To take Lord Hoffmann's example in *Wainwright*: "*It is one thing to wander carelessly into the wrong hotel room and another to hide in the wardrobe to take photographs*."[8] *Wainwright* had nothing to do with hotel rooms; it was about the strip searching of two visitors to a prison. It was concerned solely with an issue of privacy and the House of Lords were invited to declare a general tort of invasion of privacy – an invitation their Lordships declined.[9]

Many of the high profile privacy cases do not concern ordinary private citizens, as was the case in *Wainwright*. Rather, they tend to involve high profile celebrities seeking to prevent newspapers or magazines from publishing details about them.[10] This normally involves the courts having to balance the right to privacy protected under Article 8 of the Convention with the Article 10 protection of freedom of expression, a protection that the British courts have been instructed to have "*particular regard*" to,[11] although neither right has preference over the other.[12] It was such a conundrum that faced the courts when deciding *Campbell v MGN Ltd*.[13] Miss Campbell is so famous that "[e]*ven the judges know who Naomi Campbell is*".[14] The

---

[4] *R v Brown* [1996] 1 All ER 545, 555. For similar concerns recently raised by the European Court of Human Rights, see: *Von Hannover v Germany*, below, at para. 70.

[5] *Wainwright v Home Office* [2003] UKHL 53; [2003] 3 WLR 1137 at [29] (Lord Hoffmann)

[6] Hereinafter "*the Convention*"

[7] *Wainwright*, above, at [34]

[8] *ibid.* at [51]. See also: Keene LJ in *Douglas v Hello! Ltd* [2001] QB 967 at [168]

[9] *ibid.* at [35]

[10] See, for example, *Douglas v Hello* [2001] QB 967; *A v B* [2002] EWCA Civ 337; [2003] QB 195, CA; *Theakston v MGN Ltd* [2002] EMLR 22

[11] Human Rights Act 1998, s 12(4)

[12] Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, para. 19

[13] [2004] UKHL 22. Available at: http://www.parliament.the-stationery-office.co.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm (Sourced: 12 July 2004). Hereinafter "*Campbell (HL)*"

[14] *ibid.* at [129] (Baroness Hale of Richmond)

case centred on a story that appeared in *The Mirror* on 1 February 2001, which exposed Miss Campbell as a drug addict - an addiction for which she was receiving treatment - and the newspaper went on to give details of the treatment she was receiving from Narcotics Anonymous (NA), along with a surreptitiously taken photograph of her leaving a NA meeting. The overall tone of the article was supportive and understanding. These facts were complicated by the fact that Miss Campbell had publicly denied that she was a drug addict, leading her counsel to concede that the newspaper was entitled to correct her earlier false statements.

Although successful at first instance against *The Mirror*, a unanimous Court of Appeal upheld the newspaper's appeal.[15] Miss Campbell thereafter appealed to the House of Lords, who, in allowing her appeal, were sharply divided. By allowing her appeal, the House of Lords accepted that the newspaper could publish the fact that she was in fact a drug addict and receiving treatment, but the majority took issue with the printing of details of the treatment and, in particular, the printing of the photograph. It was suggested that the traditional action for breach of privacy was now better described as a tort of "*misuse of private information*."[16] Although split 3-2, the House of Lords was in basic agreement over how the competing rights found in Articles 8 and 10 should be balanced, with their Lordships differing over the application of the law to the particular facts. In the majority, Lord Hope clearly felt that the publishing of the photograph was the critical element of the case,[17] while Baroness Hale also placed significant emphasis upon the role of the photograph, especially the fact that, by the editor's own admission, the story was worthy of the front page without the photograph.[18] Lord Carswel, however, was unwilling to say which element of the article "*tips the balance*."[19] Lords Nicholls and Hoffmann were much less impressed by the role of the photographs, holding that the covert taking of the photographs added nothing to the complaint made by Miss Campbell[20] and, furthermore, the photograph formed an essential element of the story. Requiring it not to be published would trespass upon the editor's discretion.[21] This difference of opinion in the highest court in the land shows just how subtle some of the distinctions must be and it must surely confuse the 'man on the underground' that a "*prima donna celebrity*"[22] can have her privacy protected while the Wainwright's are left without a remedy.

Shortly after the House of Lords decision in *Campbell*, the European Court of Human Rights in Strasbourg issued its ruling in the *Princess Caroline* case.[23] Balancing Articles 8 and 10 was once again in issue as well as issues as to the degree of privacy

---

[15] *Campbell v MGN Ltd* [2002] EWCA Civ 1373; [2003] QB 633. Hereinafter "*Campbell (CA)*"

[16] *Campbell(HL)*, above, at [14] (Lord Nicholls of Birkenhead)

[17] *ibid.* at [121] – [124]

[18] *ibid.* at [155] – [156]

[19] *ibid.* at [170]

[20] *ibid.* at [30] and [73] (Lord Nicholls of Birkenhead and Lord Hoffmann, respectively)

[21] *ibid.* at [77] (Lord Hoffmann)

[22] *ibid.* at [143] (Baroness Hale of Richmond)

[23] *Von Hannover v Germany*, Application no. 59320/00, 24 June 2004. Available at: http://hudoc.echr.coe.int/hudoc/ViewRoot.asp?Item=0&Action=Html&X=712132324&Notice=0&Noticemode=&RelatedMode=0 (Sourced: 12 July 2004)

to be afforded to a public figure in a public place.[24] In the opinion of the Court, when trying to balance these competing rights, the crucial factor should be "*the contribution that the published photos and articles make to a debate of general interest*."[25] Although concurring with the result, Judge Cabral Barreto (President of the Chamber) and Judge Zupancil, felt that the correct test was in fact one of "legitimate expectation" of privacy from the media in a public place. Conceding that this test was somewhat difficult to apply, Judge Cabral Barreto felt that a case-by-case approach was warranted.[26] Space prohibits giving *Von Hannover* and *Campbell* the consideration and analysis that they deserve within the confines of this article. However, they do illustrate the continuing problems that issues of offline privacy pose to the highest courts and thus the unsuitability of the 'offline' laws as a solution for the 'online' privacy problem. Calls have long come for Parliament to legislate in this sphere, although it is yet to grasp the nettle.[27] There remains no general tort for invasion of privacy, although it is far from the case that "*there is still no privacy law in the UK.*"[28] Privacy in the UK is protected by a collection of ill-fitting statutes, such as the Protection from Harassment Act 1997 and the Data Protection Act 1998, alongside the ever growing case law on the subject – there is no overall, coherent framework however. Perhaps, therefore, privacy law in the UK is best likened to the UK constitution: it may not all be committed to writing and what there is may not be found in a single place, but it is not therefore true to say it does not exist.

3. Data Protection Law

Existing data protection laws were introduced in the United Kingdom to implement Directive 95/46/EC[29], which was adopted in October 1995.[30] It required implementation before 24 October 1998, a deadline only Sweden met, with the European Commission[31] having commenced Article 226EC infringement proceedings against nine of the fifteen Member States, with proceedings being brought before the Court of Justice in five of those cases.[32] In the UK, the Directive was implemented by the Data Protection Act 1998[33] which entered fully into force on 1 March 2001. It has

---

[24] Cf, *Peck v United Kingdom* (2003) 36 EHRR 41, which concerned the level of privacy afforded to a private person in a public place as well as issues relating to CCTV cameras and data protection.

[25] *Von Hannover v Germany*, above, at [76]

[26] *ibid.*, concurring opinion of Judge Cabral Barreto

[27] see: *Malone v Metropolitan Police Commissioner* [1979] Ch 344 and *Douglas v Hello! (No. 3)* [2003] EWHC 786 (Ch); [2003] 3 All ER 996 at [229] (Lindsay J), the former being approved by Lord Hoffmann in *Wainwright*, above, at [33].

[28] Bhogal, *United Kingdom Privacy Update 2003*, SCRIPT-ed, Issue 1, March 2004, available at: http://www.law.ed.ac.uk/ahrb/script-ed/docs/privacy_comment.asp (sourced on 22 April 2004)

[29] Hereinafter "*the Directive*" or "*DPD*"

[30] This Directive included the three additional member of the EEA (Norway, Iceland and Liechtenstein) although all references will remain to the EC and EU although should be taken to include the EEA

[31] Hereinafter "*the Commission*"

[32] http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/03/697|0|RAPID&lg=EN&display= (sourced on 21 April 2004); for further details on Article 226EC infringement proceedings see: Craig and De Burca, *EU Law (3rd Ed.)* (Oxford: OUP, 2003) chapter 10

[33] Hereinafter "*the Act*"

been described as a "*cumbersome and inelegant piece of legislation*",[34] although Lord Philip's consideration of the Act in the Court of Appeal has been of considerable assistance to understanding the Act.[35] Space prohibits an exhaustive discussion of this complex and often controversial Act[36] and attention will therefore be focused upon the features that are of particular interest in relation to protecting online privacy.[37] In short, the Act regulates the processing of personal data, splits such data in to two categories, with 'sensitive personal data' afforded additional safe-guards, and concerns automated decisions. The rationale behind the Directive was the facilitation of the single market. With the continued development of the quaternary industries within the EU, it was feared by the Commission that strict data protection laws could be used by Member States to distort the market and interfere with the achievement of the aims of the common market.[38] Consequently, the aim of the Directive was to harmonise European data protection laws and avoid any interference with the internal market. As the Directive addressed an area that many Member States considered had human rights implications, and consequently were reluctant to lower any level of protection, negotiations were particularly difficult.[39] None of the provisions were designed specifically with the Internet in mind. Most important in terms of the Internet, however, are the provisions relating to cross-border transfers, for no matter how successful the mechanics of the Directive may be, weak regulation of such trans-national transfers will render the provisions worthless when trying to guard online privacy.

3.1 Article 25DPD and 'adequate' protection

There is an inherent conflict between facilitating international trade and individual's data privacy that is faced by any attempt to regulate. This is recognised in the Preamble of the Directive.[40] Article 25DPD requires member states to prohibit the transfer of personal data to a third country that does not ensure an "*adequate*" level of protection. This is a task that would have proved difficult prior to electronic communication and is something that now borders upon the impossible. To ensure uniformity throughout the Community, most major decisions on adequacy will be taken at the Community level.[41] With few countries considered 'safe' by the Commission, exporting data outwith the EU/EEA is far from easy. [42] "*Adequacy*" must be assessed in "*the light of all the circumstances*"[43] with regard being had to,

---

[34] *Campbell (CA)*, above, at [72] (Lord Philips MR)

[35] *ibid.* at [72] – [137]

[36] For details of the recent controversy relating to the Soham murder case, see: Wildish and Nissanka, *A deletion too far: Huntley, Soham and Data Protection*, Computers and the Law, Vol. 14, Issue 6 (Feb/Mar 2004), p. 28 (http://www.scl.org/services/default.asp?iss=27&mov=1&p=156)

[37] For a full and practical guide to UK Data Protection law see: Carey, *Data Protection: A practical guide to UK and EU law* (2nd Ed.)(Oxford: OUP, 2004)

[38] Charlesworth, *Data Privacy in Cyberspace*, in Edwards and Waelde, *Law and the Internet*, at p. 85

[39] Charlesworth, above, p. 86

[40] Recital 56DPD

[41] Lloyd, *Information Technology Law* (3rd Ed.), p.187

[42] Carey, above, at pp 106-107

[43] Article 25(2)DPD

inter alia, the nature of the data transferred, the purpose of the transfer and the laws in force in the third country. Where the Commission finds a country not to have an 'adequate' level of protection, member states must "*take the measures necessary to prevent any transfer of data of the same type to the third country in question.*"[44] By prohibiting transfers to countries that do not meet European standards, the Directive allows the Commission to pursue any member state that allows the rights of their citizens to be subverted by allowing such transfers. There are exceptions to this export ban, contained in Article 26DPD which allow a transfer despite a country not being designated 'safe' where, *inter alia*, the data subject consented to such a transfer, the transfer is necessary for the performance of a contract between data subject and data controller or the transfer is required to protect the data subjects' vital interests.[45] An original draft of the Directive contained an absolute ban upon transfers to countries that did not have 'adequate' protection. Thus, the adopted position represents a considerable compromise.

3.2 The US approach, adequacy and safe harbours

When Warren and Brandeis were penning their seminal piece on the right to privacy it was a right that was yet to be recognised, let alone constitutionally.[46] Today, however, privacy in the United States can be seen, to an extent, as a constitutional right, despite no express reference to it within the Constitution itself.[47] In addition to this, there is a mass of federal and state level legislation, which has been likened to an ill-fitting jigsaw.[48] With much of the legislation responding to gaps in the law that the courts have refused to fill, there appears to be an absence of an overall privacy framework in the US. Privacy laws in the US often target certain sectors, be it health details, financial details or attempts to protect the privacy of children on the Internet. Laws aimed at the latter have encountered difficulties when placed against the First Amendments right to free speech, with the most recent attempt, the Child Online Protection Act, being sent by the Supreme Court for trial to determine whether the First Amendment would be infringed should the Act enter into force, with the majority remarking that a violation was "likely".[49] Data privacy within the commercial sphere in the US is most often regulated by contract law, via privacy policies. It is the Federal Trade Commission that is responsible for ensuring that these policies are agreed with and had been quiet enthusiastic in prosecuting breaches by a company of their privacy policy. While this lack of an overall framework may be levelled as a criticism, all that stops the UK reaching such a position is Parliament's refusal to take repeated judicial prompts to legislate in this field. Indeed, is an ill

---

[44] Article 25(4)DPD

[45] A full list can be found in Article 26(1)DPD

[46] Warren and Brandeis, *The Right to Privacy: The implicit made explicit* (1890) 4 Harvard Law Review 193

[47] Charlesworth, above, p. 90. On the US Constitution as a source of the right to privacy generally, see Ferrera et al., *Cyberlaw: Text and cases* (2nd Ed.), chapter 9, especially pp. 258-260. (Hereinafter "*Cyberlaw*")

[48] Alderman and Kennedy, *The Right to Privacy* (New York: Random House, 1997) pp. 330-1, quoted by Charlesworth, above, p. 93

[49] *Ashcroft v ACLU*, US Supreme Court, 29 June 2004, case no. 03-0218. For a comment on the case, see: http://edition.cnn.com/2004/LAW/06/29/scotus.web.indecency/index.html (sourced: 30 June 2004)

fitting jigsaw worse than being saddled with a Parliament that turns its back on this thorny issue while the judiciary insist it is outwith their realm?

The US approach to data privacy has the same objective as the EU – to avoid unnecessary interference with commerce. While the US government is subject to data privacy laws,[50] it is the absence of any concerted regulation of the private sector that ensures that the Commission will not recognise the US as a 'safe' country. With the US remaining the sole economic superpower, along with their dominance of the Internet, it was unreasonable for the EU to maintain a stance that prohibited its Members from allowing any data transfer from within the borders of the EU to the US. It was equally unrealistic to expect the US to yield and reform its data privacy laws so as to comply with the European approach. Consequently, a compromise had to be reached that was mutually satisfactory. After years of negotiations, such an agreement was finally found – the 'Safe Harbour' agreement.

November 30, 2000 finally saw the 'Safe Harbour' Principles[51] enter into force. These principles allow US companies that comply with them to lawfully receive personal data from the EU. EU organisations benefit from these principles by not having to continually review contractual terms with US organisations so as to ensure that they fall within the exception to the export ban.[52] Enforcement of the principles will in the main take place in the US and will be primarily a system of self-regulation. It is this enforcement mechanism that is the primary criticism to be levelled at the 'Safe Harbour' agreement. By ceding the enforcement of the agreement to the US authorities, the EU has lost control of the level of protection that data transferred under the agreement will attain. It is unrealistic and naïve to expect the US authorities to adopt the same approach to data privacy as prevails in Europe, when they live and have been trained in a culture that affords so little protection to data privacy. Furthermore, primary enforcement is to be private sector self-regulation. It is unrealistic to expect private firms, with no prior experience of any form of data privacy regime to be expected to enforce the agreement to the level the EU would otherwise demand. Dispute resolution is in the hands of private sector organisations in a considerable number of cases which must also be of concern. Furthermore, the 'Safe Harbour' agreement is overseen by the Department of Commerce, whereas commercial data privacy within the US is within the realm of the Federal Trade Commission. The latter body believes that on- and off-line standards of data privacy should be equal, whereas the former is willing to afford 'Safe Harbour' status on the basis of only one. These internal disputes further undermine European confidence in the United States ability and willingness to effectively enforce the agreement. Failing to do so could undermine the efforts being made in Europe to afford a degree of data protection to individuals.

To adequately protect the privacy of European citizens, it is essential that the EU, to some extent, retain control over the enforcement of the data protection rules. The 'Safe Harbour' agreement is a marriage of convenience between the EU and US to facilitate trade whilst the EU may maintain that the Directive is being complied with. Somewhat regrettably, in order to facilitate this marriage, the rights and interest of

---

[50] Privacy Act 1974

[51] Hereinafter "*the Principles*"; for further details, see: Carey, above, pp.116-123, Lloyd, above, pp.194-197, or for an American perspective, *Cyberlaw*, above, pp. 302-304

[52] Carey, above, p. 117

European citizens have seen pushed to one side. A final concern with the agreement, and perhaps one which makes the above concerns academic, is the poor take up of the 'Safe Harbour' agreement in the US. Whilst Europeans may worry over the enforcement of the agreement in the US, if only a few companies take part in the first place, even effective enforcement against that minority would prove meaningless in the grand scheme of things.

3.3 Data Protection – an untenable position

With the increasing importance of online data privacy, it is increasingly unacceptable that protection of data online is squeezed in to existing, ill-fitting laws. The Directive was not specifically designed to combat the ever increasing flows of data that the Internet facilitates. Rules on data exports, while a valiant attempt, are looking increasingly helpless and unenforceable. Just as in UK privacy law, where breach of confidence is finding it increasingly difficult to cope with a concept it was not designed to address (i.e., privacy), the Directive looks equally strained. Furthermore, the 'Safe Harbour' agreement with the US provides for enforcement of the agreement in the US, according to US law. Having ceded this, the EU has lost control of the level of protection online data transfers will have and is dependant upon the co-operation and support of the US courts and must trust the self-regulatory regime. As a result, the search should be well underway for alternative solutions to the increasingly pressing question of online data privacy. With it increasingly difficult to prevent privacy abuses in the online age, any solution must not aim to prevent privacy abuses, but must have an effective and enforceable remedy and sanction as its target.

4. A Proposed Solution

One such proposal came from Lilian Edwards and she suggested the use of a trust model.[53] Whilst an attractive solution to the problem of online privacy but with, by the authors own admission, "*many details still to be worked out*", there appears to be two fundamental flaws with the proposal. Firstly, the proposal likens online data protection to common law trust. As has already been noted, the inherent difficulty with the Internet is that of jurisdiction. A solution based upon the common law of a single jurisdiction will fail to leap that initial and substantial hurdle. Common law, by its definition, is common to a single jurisdiction and can differ significantly between jurisdictions. This problem is then compounded by jurisdictions that are not based upon the common law. How would such countries cope with regulating the Internet according to a very 'foreign' concept?

Secondly, it is proposed that any dividend is paid into a fund that could be used to fund some form of national enforcement agency, provide set levels of compensation and privacy-enhancing technologies to those who do not wish to give away personal data under any circumstances. This flaw is again tied to the trans-national nature of the Internet. To be fully effective, national enforcement agencies would have to be established in every country that had access to the Internet and these new bodies would have to co-operate fully with each other. An international body would need to

---

[53] Edwards, *The Problem with Privacy – A Modest Proposal* 2003 PDP 3.3(6). A fuller version of the "Modest Proposal" is forthcoming and the author is grateful to Ms Edwards for allowing him an advanced sighting of it. The following comments relate only to the published version noted above.

be established to manage the fund and distribute the monies. As with almost all international bodies, they lack authority to hold their main members to account and are without effective enforcement mechanisms.

Whilst the benefits that a trust model would bring appear beneficial, it appears difficult, if not impossible, to bring them to fruition. It is true that alternatives to the current position are required – European data protection law is unsatisfactory and the US attitude towards data privacy even less so. A solution must come from a multi-national body, with effective enforcement mechanisms and a recognised authority. One such body exists – the European Union.

5. 'Regulating' Privacy on the Internet

Unlike almost any other multi-national body, the European Union has not only asserted its supremacy but this assertion has been accepted by its Member States.[54] This supremacy was not created in the founding Treaties, it was created by the Court of Justice. The doctrine of supremacy[55] and that of direct effect[56] have allowed the Union to develop the strength that it now possesses, with national courts being instructed to disapply any national law that conflicts with Community law, even where they would not normally be competent to do so.[57] Thus, when looking for a strong, multi-national body to protect data privacy online, it should first be asked whether the European Union is capable of fulfilling this task. With existing data protection laws being found to be inadequate, the answer may *prima facie* appear to be negative. There are two flaws with the Data Protection Directive as a suitable remedy however – it was not specifically designed to address the problem of online privacy and it did not fully harmonise the law within the European Union.

Directives are binding only "*as to the result to be achieved*" but leave open to the Member State the decision as to the "*form and method*" of implementation.[58] Consequently, implementation can take up to twenty-five different forms, which may be done at differing times prior to the deadline for implementation.[59] Despite data protection being a harmonised area, with different forms of implementation, there can still be choice of law and jurisdictional disputes, notwithstanding the best efforts of the Commission to ensure a degree of consistency. A further problem with directives is that they tend to be 'minimum harmonisation', that is to say, a Member State may afford a higher degree of protection than that offered by the directive if they so wish. The Data Protection Directive is one such directive. As such, laws are not truly harmonised and differing levels of protection are possible throughout the

---

[54] For an interesting discussion as to why this is the case, see: Alter, *Establishing the Supremacy of European Law: The making of an International Rule of Law in Europe*, (Oxford: 2001)

[55] C-6/64 *Costa v ENEL* [1964] ECR 585

[56] C-26/62 *van Gend en Loos* [1963] ECR 1

[57] C-106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* [1978] ECR 629

[58] Article 249 of the *Treaty Establishing the European Communities*

[59] For a summary on the implementation of the Data Protection Directive in the Member States, see *Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and third countries*, Part II, pp. 7-12

Community.[60] Such problems would be eradicated if European legislation were to take the form of a regulation.

5.1 'Regulating' on-line privacy

Regulations, on the other hand, "*shall be binding in* [their] *entirety and directly applicable in all Member States.*"[61] They cannot be implemented by Member States and any attempt to 'implement' a regulation is unlawful under Community law.[62] Consequently, they are the only true way of harmonising law throughout the Community and thus avoiding jurisdictional debates. A further benefit of a regulation is that should it be suitably drafted, that is to say it is clear, precise and unconditional, it will be afforded direct effect.[63] While it is true that directives can also be directly effective, in addition to meeting the above conditions, the time limit for implementation must have expired and a member state must have failed to, or erroneously, implemented the Directive. [64] Therefore, once implemented, so long as the desired result is achieved, it may be done in a variety of ways. Regulations provide absolute harmonisation and are capable of not only being directly effective between citizen and state – vertical direct effect – they are also capable of horizontal direct effect and thus being enforced by an individual against another individual.[65] Any new data privacy regulation could be adopted on the same legal basis as the Data Protection Directive and would comply with the proportionality requirement of Article 5EC, as the only way to effectively protect data privacy online is the complete approximation of laws.

Thus, a regulation specifically designed to address data privacy on the Internet would have three significant advantages over the existing framework. Firstly, online data privacy laws in each member state would be identical and people would be sure of their rights whether they are dealing with a British, a German or a Spanish website. This certainty and uniformity is essential when attempting to regulate the Internet. Secondly, through direct effect, a regulation could be enforced by citizens against their State, by citizens against each other, and by the European Commission. This would provide an effective army to ensure that privacy could be protected throughout the European Community. The Court of Justice could be called upon to interpret the regulation where necessary, while national courts would be available to enforce the regulation. A final benefit would be that online data privacy would be protected by a tailor made regulation, as opposed to being accommodated within existing, at times ill-fitting, laws.

---

[60] See further: Dougan, *Minimum Harmonization and the Internal Market* (2000) 37 CMLRev 853

[61] Article 249 of the *Treaty Establishing the European Communities*

[62] C-34/73 *Variola v Amministrazione delle Finanze* [1973] ECR 981

[63] For direct effect generally, see: C-26/62 *van Gend en Loos* [1963] ECR 1; for direct effect of regulations, see C-39/72 *Commission v Italy* [1973] ECR 101

[64] C-148/78 *Pubblico Ministero v Tullio Ratti* [1979] ECR 1629

[65] For the birth of horizontal direct effect, see: C-43/75 *Defrenne v SABENA* [1976] ECR 455

5.2 Preliminary obstacles

Before thought can be given to what sort of online privacy any regulation would provide, it is important to note the difficulty that could be faced by trying to reach agreement upon such a regulation. As Member States may not amend or alter the text of a regulation once it is adopted, gaining agreement upon the text will always prove difficult. This is especially so where individual rights are concerned, as in this case. The degree of protection afforded to them varies from country to country. The fundamental question is whether all Member States should be forced to raise their standards to that of the 'best' country, or whether those with the highest degree of protection must lower that protection. It is this conundrum that has led to the increased use of 'minimum harmonisation'.

Where fundamental rights are concerned, the Community must tread very carefully. In Germany, the Constitutional Court has made it plain that it will not accept a Community law that lowers the level of protection that is offered to its citizens' fundamental rights by the German constitution.[66] The long and difficult discussions over the text of the 1995 Directive give further warning about the difficulty in securing an agreement by the Member States. Article 94EC would require the Council to be unanimous in agreeing the regulation. While agreement may be difficult to reach, a suitable regime can surely be found that would be acceptable to the Member States – after all, they all agree in principle that privacy on the Internet should be protected. Protecting these rights by a regulation would be an important step and an essential one if the Community sought to protect its citizens against foreign threats to their privacy.

5.3 Regulating Privacy and Extraterritoriality

Whilst it remains politically controversial, especially with the United States, and there would be problems with the enforceability of any decision, there is a precedent for the Court of Justice claiming extraterritoriality of Community law. This has been done for many years in the field of competition law. Competition law, however, is based upon Treaty articles, namely Articles 81 and 82. Individual privacy online does not have such a basis. Therefore, application of the extraterritorial jurisprudence of the Court of Justice would require some extension and it is not certain that the Court would be willing to do so without a clear mandate in the Treaty. European law, however, is littered with examples of the Court of Justice expanding the law without a mandate from the Treaties, where the objects of the Community demand it.[67] Existing data protection laws avoid the issue of extraterritoriality by prohibiting transfers of data out with the Community unless the third country "*ensures an adequate level of protection*."[68] At present, there are only five countries that are considered 'safe', although they are expected to be joined by another three in the near future.[69] If a new

---

[66] *Brunner v The European Union Treaty* [1994] 1 CMLR 57; for further details on the German approach to the supremacy of Community law, see: Alter, above, pp. 64-123

[67] For example, the introduction by the Court of Justice of the 'mandatory requirements' exceptions to Article 28EC: C-120/78 *Rewe-Zentrale AG v Bundesmonopolverwaltung fur Branntwein* (*Cassis de Dijon*) [1979] ECR 649 and Craig and de Burca pp. 659-668

[68] Article 25(1) of the Directive

[69] Carey, above, pp 106-107

regulation could be enforced extraterritorially, this prohibition would be redundant and would allow for the free transfer of data from the Community. It would also enable the enforcement of the new regulation to rest within Europe, whereas the EU is currently dependant upon the goodwill of the self-regulatory regime currently in place in the US.

5.3.1 'Single economic entity' doctrine

The issue of extraterritoriality was originally dealt with by the Court of Justice by developing a 'single economic entity' doctrine. This allowed to Court to avoid confronting the possible existence of an 'effects' doctrine. In the *Dyestuffs* case[70] the Commission had investigated a possible cartel and found that ICI, a company registered in the UK, which was not then a member of the Community, had, by instructions given to a Belgium subsidiary, engaged in concerted practices and fined them 50,000ECU. ICI appealed against the decision and the British government expressed its displeasure at the Commission exercising jurisdiction under the 'effects' doctrine.[71] The Court of Justice was urged by its Advocate General to uphold the decision of the Commission under the 'effects' doctrine.[72] In its judgement, the Court opted to use the 'single economic entity' doctrine to uphold the Commission decision.[73] This doctrine allows parent and subsidiary companies to be treated as a single entity for the purpose of competition law thus allowing companies established outwith the Community to be punished where they have subsidiaries within the Community. Despite initial opposition to the doctrine from the British government, it now finds itself in UK law.[74]

Applying such a doctrine to a new regulation to protect data privacy online would allow it to be enforced against any company that had offices, branches or subsidiaries within the European Union. Many major US firms have such links and as such the Community could enforce its privacy requirements against them. It appears entirely reasonable that a company that seeks to avail itself of the benefits of the internal market should find itself bound by the laws of that market. Admittedly, this doctrine alone could not catch all those that would collect data online, some such entities having no connection with the Community, other than that of the Internet. An 'effects' doctrine would remedy this problem and the Court of Justice was later forced to confront the possible existence of such a doctrine.

5.3.2 An 'effects' doctrine in European law

In *Wood Pulp I*[75] the Commission had investigated alleged price fixing. Fines were imposed upon thirty-six of the forty-three investigated, all of whom had their registered offices outside the Community. All had some form of establishment within the Community. Again the Court was encouraged by its Advocate General to adopt

---

[70] C-48/69 *ICI v Commission (Dyestuffs)* [1972] ECR 619

[71] Jones and Sufrin, *EC Competition Law: Text, cases and materials*, Oxford, Oxford University Press, 2001, p. 1049

[72] See Mayars AG Opinion in *Dyestuffs* case, [1972] ECR 619, 665-704, especially 687-697

[73] *Dyestuffs* case, above, [130]-[142]

[74] Competition Act 1998, s.60

[75] C-89, 104, 114, 116, 117 and 125-129/85 *A. Ahlström Oy v Commission* [1988] ECR 5193

an 'effects' doctrine to establish extraterritorial jurisdiction,[76] but yet again the Court avoided discussing 'effects' directly and considered 'implementation'. It was observed by the Court that an infringement of Article 81EC consisted of two elements: formation of the agreement and its implementation. The Court held in that regard:

> *"If the applicability of prohibitions laid down under competition law were made to depend on the place where the [agreement] was formed, the result would obviously be to give undertakings an easy means of evading those prohibitions. The decisive factor is therefore the place where it is implemented."*[77]

As a result, the Court found that the Community's jurisdiction was covered by the territorial principle, as recognised by international law.[78]

While the Court avoided creating an 'effects' doctrine, or at least calling it such, the approach taken could have some application to the protection of data privacy online. By collecting the data outside the Community, an easy way to circumvent the new protections would be opened. However, if the collection of the data was seen as the implementation of a decision to breach the privacy laws, and collection was deemed to take place when it was transferred, as opposed to being received, could the Community claim jurisdiction under the *Wood Pulp I* jurisprudence? In *Wood Pulp I* the Court emphasised the "*global dimensions*" of the wood pulp market[79] and that Article 81EC was aimed at practices that may affect trade or restrict competition within the Community.[80] Similar concerns arise in relation to the Internet and privacy in that it is both global and an inability to enforce data privacy laws may have a negative effect upon the Common Market. As such, the Community could claim jurisdiction over those that breached any online data privacy regulation on the same grounds as used in *Wood Pulp I*, whether it is called an 'effects' doctrine or not.

5.3.3 A few practical problems

In addition to the political problems noted above, any such regulation would encounter some additional, practical problems, mainly concerned with resources. With the Community having recently been joined by an additional ten members, it is questionable whether the Commission would have the time, resources or inclination to effectively enforce the regulation. Even if it were to do so, it already takes a considerable time for a case to be heard by the Court of Justice. It currently struggles to cope with its workload and will soon face a barrage of preliminary references from the new Member States, without the additional workload such a regulation would provide. Would the delays faced in the Court of Justice prevent any effective enforcement of any new regulation? The final practical difficulty that immediately springs to mind is the difficulty in bringing a defendant to Court. While large multi-national companies may not be able to hide so well, the bulk of enforcement

---

[76] See Darmon AG Opinion in *Wood Pulp I*, [1988] ECR 5193, 5214-5232, especially [47]-[59]

[77] *Wood Pulp I*, above, at [16]

[78] *ibid.* at [18]

[79] *ibid.* at [12]

[80] *ibid.* at [11]

proceedings will in all probability be against anonymous individuals hiding behind a computer screen in the far corners of the world.

Yet despite these and other difficulties, the law must not turn its back upon the problem simply because of the sheer size of the task. While many details need to be worked out, not least the text of any regulation, it is possible that with some good will and a lot of effort, a suitably worded regulation could have vertical and horizontal direct effect allowing for its enforcement in Member States and against individuals, as well as being capable of enforcement overseas. The obstacles in the way are substantial, but using existing bodies, with an established reputation and credibility, may offer us the best chance we have of retaining some degree of privacy online.

6. Conclusion

With increasing value and importance being attached to personal data by companies throughout the world, it is becoming increasingly urgent that effective protection is afforded to it. It is increasingly unacceptable that an issue of such importance is squeezed into existing, ill-fitting laws. Current data protection laws date from the pre-Internet era and although the Directive makes a valiant attempt to protect such privacy, it simply was not designed to cope with the sheer scale of the problem it now faces. Meanwhile, existing privacy laws, such as they are, in the UK are unreliable for this task, with the discussion above demonstrating the continuing uncertainty as to what exactly the law in this area is. It is thus necessary to seek a new solution, not based upon existing laws, that stems from a respected and authoritative multi-national body. The most notable omission from the discussion above is any suggestion of the type and degree of protection any tailor made online data privacy regulation would offer. This is perhaps due to the size of the task and in part due to the fact that this article hoped to provoke some debate as to the suitability of a European Regulation as a possible solution to the current data privacy problem. It is nevertheless an issue I would hope to return to. Seeking to protect online data privacy through means of a regulation in the now twenty-five member EU, it is contended, would be a positive step forward. It will be by no means an ideal solution although as the power and size of the Internet continues to grow, it is increasingly important that the law begins to think ‘outside the box’ if we are not to be drowned by a tidal wave that would make the ‘tide’ of Community law that Lord Denning complained of appear as no more than a ripple on the transatlantic pond in comparison.

BIBLIOGRAPHY

Textbooks

- Alter, *Establishing the Supremacy of European Law: The making of an International Rule of Law in Europe*, London: Oxford University Press, 2001
- Carey, *Data Protection: A practical guide to UK and EU law (2nd Ed.)*, Oxford: Oxford University Press, 2004
- Craig and De Burke, *EU Law: Text, cases and materials (3rd Ed.)*, Oxford: Oxford University Press, 2003
- Edwards and Waelde (Eds), *Law and the Internet*, Oxford: Hart Publishing, 2000
- Ferrera, Lichtenstein, Reder, Bird and Schina, *Cyberlaw: Text and Cases (2nd Ed.)*, West, 2004
- Jay and Hamilton, *Data Protection: Law and Practice*, London: Sweet and Maxwell, 2003
- Jones and Sufrin, *EC Competition Law: Text, cases and materials*, Oxford, Oxford University Press, 2001
- Keller and Murray, *IT Law in the European Union*, London: Sweet and Maxwell, 1999
- Lloyd, *Information Technology Law (3rd Ed.)*, London: Butterworth's, 2000
- Reed, *Internet Law: Text and Materials*, London, Butterworth's, 2000
- Whish, *Competition Law (4th Ed.)*, London: Butterworth's, 2001

Articles

- A Johnston, *Putting the cart before the horse? Privacy and the Wainwright's* [2004] CLJ 15
- Bhogal, *United Kingdom Privacy Update 2003* SCRIPT-ed, Issue 1, March 2004, available at: http://www.law.ed.ac.uk/ahrb/script-ed/docs/privacy_comment.asp
- Charlesworth, *Data Privacy in Cyberspace*, in Edwards and Waelde, above
- Dougan, *Minimum Harmonization and the Internal Market* (2000) 37 CMLRev 853

- Edwards, *The Problem with Privacy – A Modest Proposal* 2003 PDP 3.3(6)
- Morgan, *Privacy, Confidence and horizontal effect: 'Hello' trouble* [2003] CLJ 444
- Phillipson, *Transforming breach of confidence? Towards a common law right of privacy under the Human Rights Act* [2003] MLR 726
- Warren and Brandeis, *The Right to Privacy: the Implicit made Explicit* (1890) 4 HLR 193
- Wildish and Nissanka, *A deletion too far: Huntley, Soham and Data Protection*, Computers and the Law, Vol. 14, Issue 6 (Feb/Mar 2004), p. 28
- Wildish and Turle, *Naomi Campbell: drugs, distress and the Data Protection Act*, Computers and the Law, Vol. 13, Issue 2 (June/July 2002), p33

Other texts

- *Fifth Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and third countries*, Part II

Websites

- http://europa.eu.int/comm/internal_market/privacy/index_en.htm
- http://www.dataprotection.gov.uk
- http://www.bbc.co.uk
- http://www.thetimes.co.uk
- http://www.cnn.com/LAW
- http://www.coe.int/dataprotection
- http://www.export.gov/safeharbor/
- http://www.scl.org
- http://www.law.ed.ac.uk/ahrb