

SCRIPT-ed

Volume 4, Issue 3, September 2007

Taking Sides on Technology Neutrality

*Chris Reed**

Abstract

It has often been asserted that technology neutrality is the proper approach to ICT regulation, but those making this assertion use the concept in a number of divergent senses. This article analyses those different meanings and asks whether technology neutrality really is as desirable as motherhood and apple pie, and whether it does in fact achieve the goals desired by legislators.

DOI: 10.2966/scrip.040307.263

© Chris Reed 2007. This work is licensed through [SCRIPT-ed Open Licence \(SOL\)](#).

* Professor of Electronic Commerce Law, Centre for Commercial Law Studies, Queen Mary University of London.

1. *Motherhood and apple pie*

Technology neutrality has long been held up as a guiding principle for the proper regulation of technology, particularly the information and communications technologies. The liberalisation of the telecommunications market, first in the US and then in Europe, led to calls for the new regulatory regimes to be technology neutral¹, and technology neutrality has continued to be a pervasive concept in that field, influencing among others the debates on convergence with broadcasting², voice over IP³, universal service⁴, spectrum allocation⁵ and net neutrality.⁶

Rather than continuing those debates, this article examines how technology neutrality has been used in regulating the wider field of computing technology and online services. In this respect, the key factor in persuading legislators that technology neutrality should be adopted more widely was the advent of the internet for general public use.⁷ In July 1997 the US Government published its *Framework for Global Electronic Commerce*, which stated: “rules should be technology-neutral (i.e., the rules should neither require nor assume a particular technology) and forward looking (i.e., the rules should not hinder the use or development of technologies in the future)”.⁸ The following year the term was used in EU legislative proposals for the first time⁹ and has been adopted in relation to most EU technology legislation ever

¹ The earliest discoverable use of the term describes the aims of the US Electronic Communications Privacy Act 1986 – see John R Kresse, “Privacy of Conversations Over Cordless and Cellular Telephones: Federal protection under the Electronic Communications Privacy Act of 1986”, (1987) 9 Geo Mason UL Rev 335. See also Nicholas W Allard & Theresa Lauerhass, “Debalkanize the Telecommunications Marketplace”, (1991-2) Cal WL Rev 231 for an early use of the term.

² See e.g. Herbert Ungerer, “Access Issues Under EU Regulation and Anti-Trust Law: the case of telecommunications and internet markets” (2000) 5 International Journal of Communications Law and Policy <http://www.ijclp.org/>; Niloufer Selvadurai, “The Regulation Of The Information Society In The European Union” (2004) 10(6) CTLR 130.

³ See e.g. Shaun P. Montana, “An Approach to the International Regulatory Issues of IP Telephony” (2002) 8 BUJ Sci & Tech L 682, 704; James B. Speta, “Deregulating Telecommunications in Internet Time” (2004) 61 Wash & Lee L Rev 1063.

⁴ See e.g. Allen S. Hammond IV, “Universal Service: Problems, Solutions, and Responsive Policies” (2005) 57 Fed Comm L. 187; Thomas Roukens, “What Are We Carrying Across the EU These Days? Comments on the Interpretation and Practical Implementation of Article 31 of the Universal Service Directive” (2006) 15-SPG Media Law & Policy 201.

⁵ See e.g. Patrick S. Ryan, “Wireless Communications and Computing at a Crossroads: new paradigms and their impact on theories governing the public's right to spectrum access” (2005) 3 J Telecomm & High Tech L 239.

⁶ See e.g. [Richard E. Wiley](#), “A New Telecom Act – Remarks” (2006) 31 S III U LJ 17.

⁷ Conventionally dated to the founding of the World Wide Web Consortium in September 1994.

⁸ 1 July 1997 <<http://www.technology.gov/digeconomy/framewrk.htm>>.

⁹ Opinion of the Economic and Social Committee on the “Proposal for a Council Recommendation concerning the protection of minors and human dignity in audiovisual and information services”, OJ C 214 10 July 1998 p. 25 para. 3.2.5: “Regulation should be ‘technology-neutral’: as few as possible new regulations, policies and procedures should be specific to the new services.”; Recitals to the Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions, COM (1998) 0461 final, OJ C317, 15 October 1998 p. 7: “... this Directive introduces a technology-neutral legal framework that harmonises

since.¹⁰ Technology neutrality has also been espoused extensively by national legislators and international organisations.¹¹ The desirability of technology neutral regulation has become part of the general wisdom, and is rarely questioned.¹²

Alarming, this consensus among legislators seems to have developed in an almost complete absence of any clear understanding what the term “technology neutrality” might actually mean. It was only in 2006 that Professor Bert-Jaap Koops published his masterly essay on the subject¹³, the first proper analysis of the use of the concept outside the telecommunications sector. Although there are numerous references to the desirability of technology neutrality in earlier writings¹⁴, these do no more than attempt a brief definition of that concept without seeking to explore its deeper meaning and implications.

Koops examines technology neutrality as a starting point for legislators, and asks (and answers) three questions¹⁵:

- Why might a legislator take the principle of technology neutrality as a starting point when legislating?
- How might that legislator use the principle in formulating legislation?
- In what circumstances would it be appropriate for a legislator to take the principle as a starting point?

the prudential supervision of electronic money institutions to the extent necessary for ensuring their sound and prudent operation and their financial integrity in particular”.

¹⁰ See e.g. Amended proposal for a European Parliament and Council Directive on a common framework for electronic signatures, COM (99) 195 final; Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM (2000) 0385 final, OJ C 365 E, 19 December 2000 p. 223; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Electronic Communications: the Road to the Knowledge Economy, COM (2003) 65 final; Proposal for a Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the Internet and new online technologies, COM (2004) 91 final.

¹¹ Bert-Jaap Koops, “Should ICT Regulation be Technology-Neutral” in Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens, *Starting Points for ICT Regulation: deconstructing prevalent policy one-liners* (The Hague: TMC Asser Press 2006) p. 77, 77-9.

¹² There is, of course, a small number of dissenting voices, which are examined more closely in part 3.

¹³ Koops, *op cit* note 11.

¹⁴ See e.g. Erik S Knutsen, “Techno-Neutrality of Freedom of Expression in New Media Beyond the Internet: solutions for the United States and Canada” (2001) 8 *UCLA Ent L Rev* 87, 95 ff; Joanna Gray, “Draft Secondary Legislation on Financial Promotion: A Technology-Neutral Investment Marketing Regime” (2001) 22 *Comp Law* 150; Tapio Puurunen, “The Judicial Jurisdiction of States Over International Business-to-Consumer Electronic Commerce from the Perspective of Legal Certainty” (2002) 8 *U.C. Davis J Int'l L & Pol'y* 133, 174; Richard W Downing, “Shoring Up the Weakest Link: What Lawmakers Around The World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime” (2005) 43 *Colum J Transnat'l L* 705; Laura Hildner, “Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level” (2006) 41 *Harv CR-CL L Rev* 133; Chad A Kirby, “Defining Abusive Software to Protect Computer Users from the Threat of Spyware” (2006) 10 *Computer L Rev & Tech J* 287, 303 ff.

¹⁵ This description grossly over-simplifies Koops’ detailed and complex analysis, and readers are exhorted to read his essay for themselves.

The answers to these questions demonstrate that technology neutrality is a more complex concept than previous commentators have realised, and that different aspects of the concept need to be addressed for different legislative purposes.

The aim of this article is to extend Koops' work in two respects. First, it sets out a simplified classification of the different meanings of technology neutrality, with the aim that legislators and regulators should understand more precisely what their espousal of the principle might be likely to achieve. Second, it attempts to analyse whether the general wisdom, that technology neutrality is unquestioningly as good a thing as motherhood and apple pie, is correct.

2. *Types of technology neutrality*

The first discoverable extension of this term from telecommunications regulation to the wider field of ICT regulation appears to be in the US Government's *Framework for Global Electronic Commerce*, quoted above. Here, technology neutrality is used to mean that "the rules should neither require nor assume a particular technology".

Only a few days later, the Bonn Ministerial Conference Declaration of 6-8 July 1997 used the term in a different way, declaring in its principle 22: "Ministers stress that the general legal frameworks should be applied on-line as they are off-line. In view of the speed at which new technologies are developing, they will strive to frame regulations which are technology-neutral, whilst bearing in mind the need to avoid unnecessary regulation."¹⁶

From these statements it is possible to deduce two main elements of technology neutrality:

- The fundamental rules should be the same online as off-line (or more broadly, the same for an online technology activity as for the equivalent off-line technology activity)¹⁷; and
- Legal rules should not favour or discriminate against a particular technology.¹⁸

However, a closer examination of these two elements reveals that each is distinctly ambiguous.

Applying identical rules to different technologies (e.g. online and offline communications technologies) can be done in two ways. The first of these is for there to be a single rule, or for the equivalent rules in sectoral regulation to be identically worded. This creates the risk that differences between the technologies will mean that

¹⁶ <http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html>.

¹⁷ See e.g. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, *Principles and guidelines for the Community's audiovisual policy in the digital age* COM (1999) 0657 final, note 17: "identical services should in principle be regulated in the same way, regardless of their means of transmission."

¹⁸ See e.g. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review* COM (1999) 539 final, 10 November 1999 p. 14: "Technological neutrality means that legislation should define the objectives to be achieved and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives."

the effect of the rules is different as between them. As an example, the rule in defamation law that a publisher is liable in addition to the author can mean that the host of an internet resource such as a website or newsgroup can be made liable for defamatory content of which the host had no knowledge and could not discover without taking unusual precautions.¹⁹ The rule applies very differently to an offline publisher, where the content will invariably have been seen by representatives of the publisher such as editors. Alternatively, the rules may be worded differently so as to achieve functionally equivalent treatment for each technology, as is now the case for defamation in many jurisdictions. Interestingly, in defamation the online rules attempt to achieve equivalence by conferring some degree of immunity on the host²⁰ or by redefining the term publisher.²¹ In either case, the result may be to favour online publishing over offline in some circumstances.²² Given the substantial operating differences between online hosting and offline publishing, it is far from clear what equivalence of treatment between them might be.

As the expressed aim behind this element of technology neutrality is to ensure equivalent treatment between different technologies, the first potential meaning can be discarded. We need therefore to recognise that technologically neutral rules addressing the same issue may well differ in their wording and content, in order to achieve the same (or at least broadly equivalent) *effects* when applied to these technologies.²³

The principle that regulation should neither favour nor discriminate against a particular technology is also potentially ambiguous. Clearly, a rule which states that only technology A can be used to comply with it²⁴ favours that technology and discriminates against all others. What, though, of a rule with which technology A can comply without modification, whereas technology B can only comply if feasible, but

¹⁹ For an example from the UK, see *Godfrey v Demon Internet Ltd* [1999] 4 All ER 342.

²⁰ See e.g. Directive 2000/31/EC on electronic commerce OJ L 178 p. 1, 17 July 2000 art. 14.

²¹ See e.g. US Communications Decency Act 1996, 47 USC § 230.

²² For example, a host does not lose its US Communications Decency Act immunity even when it knows the nature of the content - *Zeran v. America Online Inc.* 129 F.3d 327 (4th Cir. 1997) at 330-31; [Barrett v. Rosenthal](#) 146 P.3d 510 (Cal Supr Ct 2006) at 514, 525.

²³ The UK Financial Services Authority has recognised this distinction:

“... the fundamental principles of regulation remain the same whatever the medium (principle of technological neutrality). This policy means that the FSA will not discriminate in its approach on the basis of delivery channel alone, unless the risks to the statutory objectives justify it. Nevertheless, non-discrimination does not suggest the imposition of the same requirements on all delivery channels, since the risk may differ but it does require the FSA to be able to justify any differences by reference to the features of the specific medium.”

Apostolos Gkoutzinis, “The Prudential Supervision of Internet Banking in the United Kingdom - is the ‘Basel Approach’ Finding its Way Through National Regulations” (2002) 17 *JIBL* 249, 254 (discussing the FSA’s policy document “New Regulator for a New Millennium” (London, January 2000)).

²⁴ For example, the those elements of English law which require personal signatures for a limited class of transactions, and which limit personal signatures to those written by hand – see *Goodman v. J. Eban Ltd.* [1954] 1 QB 550.

expensive, modifications are made? Such a rule does not favour technology A directly but it does *indirectly* discriminate against technology B.²⁵

This ambiguity should again focus our attention on the aims of the legislator. If the aim is to regulate the activities of users of already existing technologies which are used for similar ends then technology neutral regulation will adopt the first of these approaches, treating use of each type of technology in equivalent ways. Thus the EU regulation of commercial communications imposes restrictions whose stringency increases with the intrusiveness, cost to the recipient and potential deceptiveness of the communication, rather than allowing the use of some communications technologies and forbidding or restricting others.²⁶ If, however, the aim is define the legal consequences which arise from the use of technology, such as whether a valid signature has been made²⁷ or when and where a communication has been received²⁸, then the legislative solution must necessarily concentrate on the characteristics which are required to achieve that legal consequence. Some existing technologies may already possess those characteristics, whereas others do not. In these circumstances, a technologically neutral solution will not prevent the latter type from being modified to achieve those characteristics, but will inevitably favour technologies which do not need such modification.²⁹

To complete our understanding of the concept of technology neutrality, it is clear that we must identify what further aims are intended to be achieved by use of the concept. Koops has undertaken this analysis and identifies four main legislative purposes³⁰:

1. The achievement of particular effects, in terms of peoples' behaviour or the outcomes of activities;
2. Functional equivalence between different modes of activity, in particular offline and online;
3. Non-discrimination between technologies with equivalent effects; and
4. Futureproofing of the law in two senses:
 - drafting of laws in a way which is flexible enough not to hinder the future development of technology; and
 - achieving sustainability in the sense that the law should not require over-frequent revision to cope with technological change.

²⁵ See further part 2.3 below.

²⁶ Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37, 31 July 2002 art. 13 and recitals 40-45.

²⁷ Directive 1999/93/EC on a Community framework for electronic signatures OJ L13/12, 19 January 2000.

²⁸ Australian Electronic Transactions Act 1999 s.14; US Uniform Electronic Transactions Act 1999 § 15(b) & (d).

²⁹ See the discussion at part 2.3 below.

³⁰ Koops, *op cit* note 11 at pp 83-90. This summary does not match Koops' analysis precisely but is, the author hopes, conceptually equivalent.

The first three of these are implicit in the two elements of the concept discussed above. The fourth is commonly cited as a reason why legislation should be technologically neutral, though there is as yet little evidence that such legislation has thereby been future proofed successfully.

Assuming (at least until part 3 of this article has been reached) that technology neutrality is worth attempting, we must now examine the three main legislative techniques which can be adopted.

2.1 Technology indifference

Some laws and regulations apply in identical ways, whatever the technology. The law of murder is an obvious example. Professor Plum's liability is unaffected by her choice between strangling the victim with the rope in the conservatory or bludgeoning him with the lead pipe in the drawing room. Such laws are *indifferent* to the technology involved, because they apply to behaviour of the actors involved and the effects of that behaviour³¹ and not to the means through which the actors behave or by which those effects come about.

In the information and communications technology field, one of the most clearly technology indifferent legal provisions is the right to authorise communication of a work to the public³², granted to authors by copyright law.³³ The reason for the introduction of this right in 1996 was the increasing quantity of online information provision³⁴, but the right is by no means limited to online communication. If the works of Shakespeare were still in copyright I could infringe his rights in *Hamlet* in numerous offline ways, for example via the use of technologies such as semaphore flag communication.³⁵

³¹ Koops, *op cit* note 11 at pp 83-6.

³² WIPO Copyright Treaty 1996 art. 8: "... authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them."

It is worth noting that the Berne Convention of 1979 is not technology indifferent on this point, in most cases limiting the right to "communication to the public by wire" – see arts 10, 11bis(1), 14(1). Only the rights to prevent the communication of performances (art. 11(1)) or recitations (art. 11ter(1)) are technology indifferent.

³³ Copyright law is often said to be generally technology neutral, using that term in the sense of technology indifference. "Copyright law has by and large been formulated according to principles of 'technological neutrality.' It has focused on the nature of the use of the work, rather than the medium by which the use is accomplished, or the physical facilities or equipment involved. Thus, the law has granted to authors the rights to reproduce the work, to adapt it, to perform it publicly, and to communicate it to the public. The primary exception to this technological neutrality has been the separation of a broadcasting right from the general right of communication to the public." [Shira Perlmutter](#), "Convergence and the Future of Copyright" (2001) 24 Colum-VLA J.L. & Arts 163.

³⁴ See *Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society* COM(97) 628 final, 10 December 2007 p. 20: "Technological developments have made it possible to make protected works and other subject matter available in new ways which differ significantly from traditional methods of exploitation. This is particularly true with respect to the exploitation of intellectual property on-line over the networks, and notably 'on demand'."

³⁵ Images from <<http://www.inter.scoutnet.org>>, reproduced by kind permission of D Jansen.



At first sight, technology indifferent laws appear to exhibit technology neutrality in all the senses analysed above. Further thought reveals, however, that the internet communications technologies are different in kind from offline communications methods like semaphore. The involvement of intermediaries whose role is to store, copy and/or forward all the information they receive, without examining its semantic content, has already raised the question whether “copying” for the purposes of copyright law is a factual description or an intentional activity³⁶, and similar questions will need to be answered for the right to control communication to the public. As Perlmutter has written:

To put it bluntly, this approach no longer works. Even rights deliberately written to be technologically neutral are quickly called into question by the rapidity of today's technological developments. There ensues a tremendous diversion of time and energy in debating the precise borders of each right. Which rights are implicated by a particular type of dissemination – for example, “making available” online? Reproduction? Distribution? Rental? Communication?³⁷

Technology indifferent drafting may be an effective technique where the behaviour to be controlled, or the effects to be mandated or prohibited, are not made different in kind by the means adopted by the regulated actor. Where, though, the use of technology fundamentally changes the nature of the behaviour, or means that the effects of that behaviour are different or have different consequences, alternative mechanisms for achieving technology neutrality are required.

2.2 Implementation neutrality

If it is desired only to regulate the uses of a particular technology, the regulation must by definition be specific to that technology. However, it is often possible to frame that regulation in such a way that it does not favour one or more *implementations* of that technology over others. This type of technology neutrality has been described as “implementation neutrality”.³⁸

³⁶ See *Religious Technology Centre v Netcom On-Line Communications Services Inc.* 907 F Supp 1361, 1374 (ND Cal, 1995) and the extensive jurisprudence and legislation, in the US and elsewhere, addressing this issue, discussed in Chris Reed, *Internet Law: text and materials* (2nd edition, Cambridge: Cambridge University Press 2004) Ch 4.

³⁷ [Shira Perlmutter](#), “Convergence and the Future of Copyright” (2001) 24 Colum-VLA J.L. & Arts 163, 173.

³⁸ This terminology seems first to have been recorded by Professor Amelia Boss; see Amelia Boss, “Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform” (1998) 72 TLNLR 1931, 1971; “Searching for Security in the Law of Electronic Commerce”, (1999) 23 Nova L Rev 585.

The implementation neutral approach to regulation is illustrated most clearly in relation to the signature of electronic documents. There are, at the time of writing, four main ways in which such a signature might be attempted³⁹:

- by typing the signatory's name into the electronic document;
- by adding a scanned image of the signatory's manuscript signature to the document;
- by encrypting the document (or more normally, a mathematical message digest of the document) with the signatory's secret key, using an encryption method which enables the recipient to validate the signature by decrypting with the sender's public key; or
- to capture some biometric characteristic of the signatory, such as his signature metrics, iris print or voice print, and encrypt that biometric data with the message digest of the document.

Most jurisdictions have decided to pass laws which enable electronic signatures to be treated as legally valid forms of signing a document, and many of those have chosen to do so in a way which does not exclude any of these signature methods from being valid. This is comparatively easy in common law jurisdictions because case law has established over the years that the precise form a signature takes is not decisive.⁴⁰ A signature is any process which, when applied to a document, produces sufficient⁴¹ evidence: (a) of the identity of the signatory; (b) that the signatory intended to sign the document; and (c) that the signatory adopts the contents of the document.⁴² Any e-signature law which imposes as the sole requirement for validity that evidence of these matters must be produced is implementation neutral as between the available e-signature methods.

Thus the UNCITRAL Model Law on Electronic Signatures 2001, art 2(a) states:

“Electronic signature” means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate

³⁹ See further Chris Reed, *Internet Law: text and materials* (2nd ed. Cambridge University Press 2004) Chapter 6.1.2.

⁴⁰ Thus in English law, for example, valid signatures have been made by initialling a contract (*Hill v. Hill* [1947] Ch 231), making a mark on a will (*in re Clarke* 27 LJPM&A 18), printing a name on a letter (*Schneider v. Norris* 2 M&S 286) or using a rubber stamp facsimile of a manuscript signature (*Goodman v. J. Eban Ltd.* [1954] 1 QB 550).

⁴¹ It is obvious that the electronic signature methods described above are not equivalent in terms of their evidential weight. The test for evidential sufficiency is not an absolute standard, however. The question is whether the signature method used provides sufficient evidence of these matters in the particular case. Thus an email on which I have typed my name, where I do not dispute that I typed it, is sufficient proof of all these matters and is thus signed by me. By contrast, if I deny sending the email, the fact that my name is typed on it is not, on its own sufficient evidence of identity, intent to sign and adoption of contents to constitute my signature. Were there additional evidence, e.g. from my service provider's records, that the email came from my computer and that the computer was under my control, this might be sufficient to validate the typed name as my signature.

⁴² Chris Reed, “What is a Signature” 2000(3) *The Journal of Information, Law and Technology (JILT)*. http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.

the signatory's approval of the information contained in the data message.

Similarly implementation neutral drafting can be found in the US Electronic Signatures in Global and National Commerce Act 2000 15 USC 7001 §106(5), the Singapore Electronic Transactions Act 1998 ss. 2 and 8, the Australian Electronic Transactions Act 1999 s. 10(1), the UK Electronic Communications Act 2000 s. 7, the EU e-Signatures Directive⁴³ arts 2(1) and 5, and numerous other laws.

It is perhaps worth noting here that implementation neutrality is very close to technology indifference – indeed, art. 2(a) of the UNCITRAL Model Law could easily be redrafted to apply to both electronic and non-electronic signatures.⁴⁴ In the case of signatures, a technology indifferent approach would require each legislature to consider whether any exceptions were required to preserve any differences from the evidential approach which existed for particular types or uses of manuscript signatures.⁴⁵ For this reason, no country has chosen to introduce new legislation which extends beyond signatures in electronic form, and thus a technology indifferent approach has been ruled out.

In other fields of activity it may only be possible to impose functionally equivalent obligations on users of different kinds of technology by regulating each type of technology specifically. In this case the closest equivalent approach to technology indifference is that of implementation neutrality. For example, the issuance of e-money is so fundamentally different an activity from the printing of banknotes and minting coins that it would clearly be difficult, if not impossible, to regulate both activities by means of the same legal rules. The EU e-Money Directive⁴⁶ aimed to be implementation neutral as between different e-money technologies⁴⁷, but failed to achieve this aim as we shall see in part 3.1 below.

It is worth noting that the extent of neutrality as between different technology implementations depends very much on the definition of the technology to be regulated. Thus a law which controls the carrying of weapons is likely to be neutral as between different types of armament, whereas a law which regulates the carrying of guns will necessarily favour those who prefer knives or bows and arrows. The choice in the e-Money Directive to regulate the issuance of e-money, rather than the

⁴³ Directive 1999/93/EC on a Community framework for electronic signatures, OJ L 13 19 January 2000 p 12.

⁴⁴ For example, “‘Signature’ means a process applied to, or information in, affixed to or logically associated with, a document, which may be used to identify the signatory in relation to the document and to indicate the signatory’s approval of the information contained in the document.”

⁴⁵ In English law, for example, a memorandum of a contract for the sale or disposition of interests in land under the Law of Property (Miscellaneous Provisions) Act 1989 s. 2 requires a personal (i.e. manuscript) signature - *Firstpost Homes Ltd. v. Johnson and others* [1995] 1 WLR 1567.

⁴⁶ Directive 2000/46/EC of the European Parliament and of the Council on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275, 27 October 2000 p. 39.

⁴⁷ Recitals to the Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions, COM (1998) 0461 final, OJ C317, 15 October 1998 p. 7: “... this Directive introduces a technology-neutral legal framework that harmonises the prudential supervision of electronic money institutions ...”. It is clear from the context that “technology-neutral” is used here in the sense of implementation neutrality.

provision of e-payment services, was one of the reasons why this legislation was not implementation neutral.

2.3 Potential neutrality

There will be circumstances when a regulator decides that a particular attribute of a technology, or method of its use, is essential to achieve the legal result which the regulator is aiming for. Unless all existing and potential implementations of the technology exhibit that characteristic or are used in that way, implementation neutrality will not be available as a legislative technique. In these circumstances, the regulator can achieve some level of neutrality between different technology implementations by drafting the legal requirements in such a way that non-compliant implementations can be modified to become compliant.

Again, e-signature law provides the clearest illustration of this approach. E-signatures are used primarily in online dealings, and the question of the identity of the online counterparty is a perennial issue.⁴⁸ A document may appear to be signed electronically by Alice, but how can the recipient be sure that Alice is really Alice? The answer to this conundrum is for a trusted third party to take evidence of Alice's identity (e.g. via a passport or some other official document) and then issue an electronic certificate which confirms her identity and links her with the e-signature mechanism. Identity certification was from an early stage built into digital signatures, i.e. those which rely on asymmetric public/private key encryption⁴⁹, but not into the other e-signature methods described at part 2.1 above.

As we have seen above, the common law jurisdictions have tended to favour a purely evidence-based approach which does not mandate identity certification.⁵⁰ However, Civil law countries have traditionally treated offline signatures as a requirement of form, rather than a matter of evidence, and therefore considered independent evidence of the identity of a signatory to be an important factor if electronic signatures were to be given legal validity.⁵¹ Thus the EU e-Signatures Directive art. 5(1) introduced a second level of e-signature⁵² based on identity certification. This type of e-signature “[satisfies] the legal requirements of a signature in relation to data in electronic form

⁴⁸ See Chris Reed, *Internet Law: text and materials* (2nd ed. Cambridge University Press 2004) Chapter 5.

⁴⁹ See RFC 2459 and 2527 (available via www.ietf.org/rfc.html) and ANSI X.509 for technical descriptions.

⁵⁰ Though the earliest e-signature laws required identity certification as a prerequisite for validity of the signature. See e.g. Utah Digital Signature Act 1996 (Utah Code § 46-3), German Digital Signature Act (Signaturgesetz) 1997 and Ordinance (Signaturverordnung) 1997.

⁵¹ See recital 20 of the Directive: “... national law lays down different requirements for the legal validity of handwritten signatures; whereas certificates can be used to confirm the identity of a person signing electronically; advanced electronic signatures ... can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled”.

⁵² The “advanced electronic signature” based on a “qualified certificate” and created by a “secure-signature-creation device” (all defined in art. 2). Theoretically there could be an advanced signature which is not based on a qualified certificate and creates securely, but the Directive gives no special status to such a signature.

in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data” and is admissible as evidence.⁵³

This provision enables digital signatures to comply with little or no modification, but the main competing technology, biometric signatures, was not designed to include third party identity certification. As a consequence, art. 5(1) of the Directive favours the former as against the latter. This apparent lack of technology neutrality has been noted⁵⁴, but is not the point. Once the legislators had decided that identity certification was necessary to achieve the formality necessary to grant e-signatures legal validity (at least in Civil law countries), that choice would necessarily discriminate against non-certified e-signature technology. The question is whether neutrality could potentially be restored by modifications to the technology discriminated against, and it is clear that there is no insuperable barrier to incorporating identity certification into biometric signature technologies.⁵⁵ The fact that this has not been undertaken is explainable by the lack of economic demand for e-signatures of either kind, and not because of the law’s discriminatory effect.

Had the Directive imposed a requirement to meet a technical standard in order for an e-signature to achieve legal validity⁵⁶ it would have not have been potentially technology neutral legislation. Because, however, its requirements are at least theoretically achievable for non-digital signature technologies, the Directive exhibits some minimum level of technology neutrality.

A similar approach was taken in those parts of the EU Electronic Commerce Directive⁵⁷ which regulate online contracting. For example, art. 11(2) provides:

Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

⁵³ It is noteworthy that the UK’s implementation of the Directive in the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002, SI 2002/318 does not enact art. 5(1) expressly, because as already explained, under English law *all* signature methods have equivalent legal effect except where a personal signature is required.

⁵⁴ See e.g. Susanna Frederick Fischer, “Saving Rosencrantz and Guildenstern in a Virtual World? a comparative look at recent global electronic signature legislation” (2001) 7 *BUJSTL* 229, 236; European Commission, *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures* COM(2006) 120 final 15 March 2006 section 2.3.2.

⁵⁵ It is even theoretically possible to produce a manually typed signature to an electronic document which complies with art. 5(1) – cameras could simultaneously record the typing and the face of the typist, and the output of those cameras could be encrypted with a message digest of the document and a third-party certified picture of the signatory in a way which meets the Directive’s other requirements. This would be a cumbersome and ultimately pointless exercise, as the encryption process would most easily be performed using digital signature technology, but the fact that it is technically achievable demonstrates the art. 5(1) is at least *potentially* technology neutral in the sense discussed in this part.

⁵⁶ As was the case for the German Digital Signature Act (*Signaturgesetz*) 1997 and Ordinance (*Signaturverordnung*) 1997.

⁵⁷ Directive 2000/31/EC on electronic commerce OJ L 178 p. 1, 17 July 2000.

At that time many e-commerce technology platforms did not provide this functionality, and art. 11(2) therefore discriminated against these implementation of the technology. In spite of this the Directive has not been criticised for its lack of technology neutrality. The legislative aim was to ensure that the technology was operated in the specified manner, and the offending platforms were modifiable, and have since been modified, to enable online sellers to comply with art. 11(2).

3. *Is technology neutrality always desirable?*

Whichever sense of the term “technology neutrality” is being used, it seems clear that legislators have consistently failed to ask themselves whether they were being sensible in adopting their particular flavour of technology neutrality when legislating. To remedy this omission we need to ask a number of questions:

- Are the aims implicit in the concept of technology neutrality achievable?
- Is technology neutral drafting possible?
- Are there undesirable consequences of adopting a technology neutral approach?

3.1 Achievable aims

Technology neutral regulation appears to have three main aims: futureproofing, online and offline equivalence, and encouraging the development and uptake of the regulated technology. The question is whether those aims are achievable.

Futureproofing means producing law and regulation which can continue to apply to new technological developments without constant amendment. “Regulation that is based on specific technology can quickly become outdated, and may lead to inefficient investment by market players.”⁵⁸ It should be clear that technology indifferent regulation avoids this trap, unless a technological advance is so disruptive that it effectively overturns the fundamental assumptions on which that regulation is based.⁵⁹ Doubts have been expressed, however, whether other techniques of technology neutrality are capable of sufficient foresight to achieve futureproofing:

... it has to be said that technological neutrality is not always desirable. Applied to a regulation, it means that the regulation will apply to new technologies, the invention or development of which cannot be foreseen. The pre-regulation of those technologies may

⁵⁸ Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Towards a new Framework for Electronic Communications Infrastructure and Associated Services: the 1999 Communications Review* COM (1999) 539 final, 10 November 1999 p. 14, note 6. See also Koops, op cit note 11 at pp 87-89, using the term “sustainability”.

⁵⁹ Satellite broadcasting might be an example, producing a complete disconnect between the geographical location of the broadcaster and recipient of the broadcast, which was resolved in the EU by applying the regulation of the country of uplink – Directive 89/552/EEC, now replaced by Directive 97/36/EC and to be replaced from 2008 by the Audiovisual Media Services Directive art. 2(4) (24 May 2007 draft).

*produce undesirable consequences and even prevent the deployment of new technologies.*⁶⁰

These doubts may not be well-founded. I have analysed elsewhere a sample of ICT laws and regulations in terms of their effectiveness at futureproofing through technology neutral drafting, and conclude that these laws are still capable of applying in spite of the changes in technology.⁶¹ Their failure to achieve the original legislative aims is caused primarily by changes in the underlying business models for use of these technologies, rather than by over-specific regulation of particular technologies. From this, one might conclude that if other aspects of the legislation are satisfactory, a technology neutral approach can provide a useful degree of futureproofing to the law.

Achieving equivalence of effect between laws regulating new technological activities and those which continue to apply to the predecessor activities has proved more difficult. For example, one of the stated aims of the e-Money Directive was:

*to preserve a level playing field between electronic money institutions and other credit institutions issuing electronic money and, thus, to ensure fair competition among a wider range of institutions to the benefit of bearers.*⁶²

This aim was to be achieved by imposing a lighter regulatory regime on e-money issuers compared with more traditional financial institutions such as banks, and balancing this by three restrictions on the activities of e-money issuers: a requirement to maintain capital and liquidity in excess of 100% of outstanding e-money obligations (the float)⁶³; a restriction on investing the float in any but the safest (and lowest returning) government-issued securities⁶⁴; and a restriction on undertaking any non-financial services business activities.⁶⁵ It is not possible to make a direct comparison of the impact of the different regulatory regimes, as there are few e-money issuers authorised under the Directive and their accounts are not generally published. The author's impression is that the combined effect of these restrictions is to make e-money issuance only marginally profitable. The single e-money issuer

⁶⁰ Daniel J Gervais, "Towards a New Core International Copyright Norm: the Reverse Three-StepTest" (2005) 9 Marq Intell Prop L Rev 1.

⁶¹ Though the effects of that application may not always be those originally intended. See Chris Reed, "The Law of Unintended Consequences – embedded business models in IT regulation" 2007 (1) The Journal of Information and Technology Law (JILT), part 2 <<http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/>>.

⁶² e-Money Directive recital 12.

⁶³ e-Money Directive art. 4. It is worth noting that under the Basel II accord, credit institutions would need to hold a capital reserve against obligations owed to those institutions by e-money issuers of only 16% of the amount owed (assuming the e-money issuer were unrated for credit purposes) – Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: a revised framework comprehensive version* (Basel June 2006) pp 12-23 (available from www.bis.org/publ/bcbs128.htm).

⁶⁴ e-Money Directive art. 5.

⁶⁵ e-Money Directive art. 1(5).

which has so far achieved any substantial EU-wide market is PayPal⁶⁶, and it is noteworthy that PayPal has recently been granted authorisation as a Luxembourg bank⁶⁷ and thus escaped the Directive's regulatory regime.

A further problem in achieving online and offline equivalence arose when the UK mobile telecoms companies began using their customers' pre-pay float to allow those customers to pay for ringtones, software and other products. The UK Financial Services Authority (FSA) took the view that this amounted to e-money issuance and instructed those telcos to register as e-money issuers, not noticing that this would prevent them from continuing to provide mobile telephony because of the prohibition on non-financial services activities! The regulatory position was further complicated by the fact that some, but not all, of the payments which were enabled could be seen as payments for premium rate telephony services (such as ringtones downloaded to the mobile phone itself), and these were regulated by the telephony regulator and not the FSA. After a number of abortive attempts to define which payments would be considered as e-money⁶⁸ the FSA abandoned its assertion of regulatory authority over these payments on the ground that the proposed Payment Services Directive⁶⁹ was forthcoming. The most recent text of that proposal, as approved by the European Parliament 24 April 2007, introduces the new regulated entity of *payment institution*, which will operate under much reduced capital and liquidity requirements⁷⁰ and be permitted to engage in non-financial business activities provided the payment funds are appropriately safeguarded.⁷¹ In theory e-money institutions will still exist and remain regulated by the e-Money Directive, but in practice it seems unlikely that any new payment service provider would choose the e-money regulatory regime in preference to that covering payment institutions. It remains to be seen whether this new regulatory system will achieve online and offline equivalence in the payment services sector.

Online and offline equivalence may turn out to be an unrealistic aim. In many cases the offline position may be so complicated that it is not appropriate to attempt to produce full equivalence with new online technologies, as was the case for signatures.⁷² More commonly, online activities will be so different in kind from their

⁶⁶ And it seems probable that this was based largely on PayPal's role as effectively the captive payment system for eBay.

⁶⁷ Effective from 2 July 2007 – see PayPal press release, "Paypal Building the Foundations for European Growth" 15 May 2007 (www.pppress.co.uk).

⁶⁸ Notably FSA, *Electronic Money: perimeter guidance* (February 2003), though readers should not expect to understand the logic of the distinctions made therein, largely because the logic is, on the kindest interpretation, elusive.

⁶⁹ Proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 97/7/EC, 2000/12/EC and 2002/65/EC COM(2005)0603.

⁷⁰ Art. 5c(1) of the text adopted by the European Parliament 24 April 2007 sets out three methods of calculation between which Member States can choose. Method A sets the requirement at 10% of annual fixed overheads, and method B on a sliding scale from 4% of average monthly payment volume (below €5m) to 0.25% of volume above €250m. Method C is too complicated to summarise in a footnote, but is likely to produce a broadly similar amount to methods A and B. All of these are likely to be substantially less than 100% of float.

⁷¹ *Ibid* arts 10(1), 5d.

⁷² See e.g. UK Department for Trade and Industry consultation document, *Building Confidence in Electronic Commerce* URN 99/642 para. 17: "...the Government recognises that requirements for

offline counterparts that it is not possible to identify what equivalence might mean – see, for example, the discussion of online defamation at part 2 above. If online and offline equivalence is either undesirable or undefinable, it is unlikely that any attempts at technology neutral regulation will achieve it.

The third common aim of technology neutral regulation is to encourage the development and uptake of the regulated technology. In this respect legislators often exhibit a charming, if naive, idealism about what legislation can do which is not always identifiable in their other activities. Many of the legal instruments which attempt to regulate online activities specifically claim that they will encourage those activities.⁷³ It must, however, be doubted whether legislation on its own can ever achieve this aim. Some technologies, of which e-money is a prime example, have been solutions in search of a problem ever since their invention.⁷⁴ Others, such as e-signatures, have so far failed to find widespread acceptance because the cost of the technology infrastructure outweighs the potential benefits of its use, though in the case of e-signatures there are signs that this may change as the costs of identity theft continue to rise.⁷⁵ In neither case did regulation do much, if anything, to encourage use of the technology. By contrast, digital music downloading has flourished in spite of the fact that the vast proportion of downloads are in breach of the law. Technologies are adopted because of their perceived benefits, rather than because they are legally sanctioned.

signatures and writing have developed over many hundreds of years of custom and law. It would not be sensible to impose equivalence between traditional and electronic means of communication in one fell swoop. Such a move could have unforeseen consequences.” See also part 2.2 above, explaining why the e-Signatures Directive did not attempt to achieve such equivalence.

⁷³ Some of these claims are particularly extravagant, such as the assertion in the Proposal for a European Parliament and Council Directive on the taking up, the pursuit and the prudential supervision of the business of electronic money institutions, COM (1998) 0461 final, OJ C317, 15 October 1998 p. 7 that the proposed legislation:

... will create legal certainty, encourage new market entrants, encourage competition, and contribute generally to the development of electronic commerce.

Other examples might include the European Parliament resolution of 17 July 1998 (A4-0189/98) on the proposed e-Signatures Directive; Australian Broadcasting Services Act 1992 s. 4(3)(c) (as amended); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework* COM(2007)96 para. 3.5.

⁷⁴ The origins of the technological concept of stored value e-money lie in the late 1980s – see e.g. D. Chaum, A. Fiat, & M. Naor, “Untraceable Electronic Cash” in *Advances in Cryptology: Proceedings of CRYPTO '88*, S. Goldwasser (Ed.) (Springer-Verlag 1990) pp. 319-327 – and the first operational system, Mondex (www.mondex.com), was invented by Tim Jones and Graham Higgins in 1990 with in-house trials at NatWest in 1992. Initially stored value e-money was proclaimed to be a solution to the problem of low value payments where giving change was difficult, such as car parking, then as a solution to the problem of payment over the internet, and most recently as a technology for mobile telephony payments. In each case, simpler technologies have proved commercially more effective.

⁷⁵ UK Government estimates of this cost were £1.3 billion p.a. in 2002, rising to £1.7 billion in 2006 – see www.identity-theft.org.uk – though it is unclear what proportion of this is due to online activities.

3.2. Drafting problems

It is clearly only sensible to attempt to produce technology neutral regulation if it is possible to draft the regulation in technology neutral terms. Some authors doubt whether this is ever achievable:

Language cannot be completely technology-neutral; it is impossible to draft legislation with sufficient precision and clarity that addresses every possible future technical variation.⁷⁶

Others are more sanguine about the prospects of success:

Where regulation is drafted in technology neutral terms (for example, ‘any means of transport’, ‘any means of communication’, ‘any means of human reproduction’, or the like), a literal interpretation will keep the law connected to the technology.⁷⁷

One important factor in determining whether technology neutral drafting is possible is the extent to which the legislator understands the technology. For example, art. 7(1) of the Databases Directive⁷⁸ grants a sui generis right to prevent unauthorised extraction and/or reutilisation to:

... the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents ...

The aim of the drafters was to protect databases both of content originating from third parties, and content originating from the maker of the database.⁷⁹ However, in *British Horseracing Board Ltd and Others v William Hill Organization Ltd*.⁸⁰ the ECJ held that the drafting of art. 7(1) made a distinction between creating and obtaining data, and required that any investment in the *creation* of data should not be taken into account in deciding whether the investment in making a database was substantial. The effect was to remove protection from most databases which consist only of data generated by their maker, a result which “...[goes] against the Commission’s original intention of protecting ‘non-original’ databases in a wide sense”.⁸¹

This problem arose because the drafters of the Databases Directive wrongly thought that they understood the technology and how databases would be generated and used in the future. Had they resisted the temptation to define “making” a database in terms

⁷⁶ Lyria Bennett Moses, “Understanding Legal Responses to Technological Change: the Example of In Vitro Fertilization” (2005) 6 *Minn J L Sci & Tech* 505, 578.

⁷⁷ Roger Brownsword, “Regulating Human Genetics: New Dilemmas for a New Millennium” (2004) 12 *Med L Rev* 14, 31 (footnotes omitted).

⁷⁸ Directive 96/9 on the legal protection of databases OJ L77, 27 March 1996 p. 20.

⁷⁹ Explanatory memorandum to the 1992 proposal, COM(92)24 final paras 3.2.7 and 3.2.8 p. 25.

⁸⁰ Case C-203/02 9th November 2004. See also *Fixtures Marketing Ltd v Oy Veikkaus Ab*, Case C-46/02 9th November 2004; *Fixtures Marketing Ltd v Svenska Spel Ab*, Case C-338/02 9th November 2004; *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)*, Case C-444/02 9th November 2004.

⁸¹ DG Internal Market And Services Working Paper, “First evaluation of Directive 96/9/EC on the legal protection of databases”, Brussels 12 December 2005 p. 13.

of “obtaining, verification or presentation”⁸² and merely required there to have been a substantial investment in that making, *British Horseracing Board Ltd and Others v William Hill Organization Ltd* would have been decided differently and the original intention of the Directive would have been preserved.

Even if the technology is understood, no drafting can be proof against unanticipated changes to that technology. The e-Signatures Directive assumed that certification-service-providers would themselves take evidence of a signatory’s identity, and thus contains no provisions on the liability of those who actually take such evidence, registration authorities, while the e-Money Directive was drafted on the assumption that e-money value would be stored on a device in the holder’s possession, rather than on the central servers used by (for example) mobile telephony providers. For these, among other reasons, neither Directive is a close match to the current state of the technology.⁸³

3.3. Undesirable consequences

By definition, technology neutral regulation cannot be very specific about the subject matter which it regulates. This can produce the undesirable consequence that the law, or its application in practice, is insufficiently clear. As Escudero-Pascual and Hosein have demonstrated clearly in respect of the interception of communications data⁸⁴, an unsuccessful attempt to achieve technology neutrality has resulted in regulation whose meaning is so vague that its application to the technology is often a matter of guesswork.⁸⁵

As a further example, the e-Money Directive defines electronic money as value which is:

- (i) stored on an electronic device;
- (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; and
- (iii) accepted as means of payment by undertakings other than the issuer.⁸⁶

The drafting of point (i) is clearly an attempt to be implementation neutral.

⁸² Interestingly, the original Proposal for a Council directive on the legal protection of databases, COM(92)24 final, OJ C 156 23 June 1992 p. 4 did not explain “making” at all. All database makers were to receive protection from “unfair extraction” for commercial purposes (art. 2(5)), thus leaving it to the courts to decide whether the extraction was unfair.

⁸³ These aspects of the two Directives are analysed in more detail in Chris Reed, “The Law of Unintended Consequences – embedded business models in IT regulation” 2007 (1) *The Journal of Information and Technology Law (JILT)*, part 3.1 <<http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/>>.

⁸⁴ Alberto Escudero-Pascual and Ian Hosein, *The Hazards of Technology-Neutral Policy: Questioning Lawful Access to Traffic Data*, (2004) 47 *Communications of the ACM* 77.

⁸⁵ In the House of Lords debate on the UK Regulation of Investigatory Powers Bill 2000, the Earl of Northesk was provoked to remark: “One of the many difficulties I have with the Bill is that, in its strident efforts to be technology neutral, it often conveys the impression that either it is ignorant of the way in which current technology operates, or pretends that there is no technology at all.” Hansard, House of Lords 28th June, 2000 (Committee Stage), Column 1012.

⁸⁶ *Ibid* art 1(3)(b).

At that time, the proposed implementations of e-money all envisaged that the holder of this value would store it either on a smart card or in a software wallet on the holder's own PC. The physical world analogy was with notes and coins, where payment is achieved by transferring physical possession of the money.⁸⁷ Soon, however, the mass-market connectivity provided by the internet and mobile telephony made it possible for service providers to offer online payment services based on holding customers' money and making payments via internal accounting transfers to accounts held for merchants. The question then arose whether such payment services were dealing in value "stored on an electronic device", in which case they would fall within the ambit of the Directive. As explained in part 3.1 above, this gave rise to a long-running dispute between the UK FSA and mobile telecoms providers which has never been resolved.

If the Payment Services Directive is implemented in its current form, almost all EU-located services which transfer funds to a third party will be regulated under one of three regimes:

- Traditional "credit institutions", defined in the Consolidated Banking Directive in technology indifferent terms: "an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account".⁸⁸
- Payment institutions, which are any provider of payment services which is not a traditional credit institution or an electronic money institution.⁸⁹ This definition is based on the functions provided by the institution, not the means of effecting those functions, and is therefore also technology indifferent.
- Electronic money institutions, which issue e-money.⁹⁰ As we have just seen, "electronic money" is defined in implementation neutral language that does not provide enough detail to distinguish which uses of computing technology amount to e-money issuance and which are non-e-money payment services. It is unlikely in the modern world that many payment institutions will work purely on paper, and so the dividing line between the two regulatory regimes cannot be drawn clearly. The distinction is vital, however, because as we have already noted payment institutions are allowed to carry out non-financial business whereas electronic money institutions cannot.

⁸⁷ See D. Chaum, A. Fiat, & M. Naor, "Untraceable Electronic Cash" in *Advances in Cryptology: Proceedings of CRYPTO '88*, S. Goldwasser (Ed.) (Springer-Verlag 1990) pp. 319-32; recital 3 e-Money Directive: "electronic money can be considered an electronic surrogate for coins and banknotes, which is stored on an electronic device such as a chip card or computer memory and which is generally intended for the purpose of effecting electronic payments of limited amounts".

⁸⁸ Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions, OJ L177/1 30 June 2006 art. 4(1)(a). Art. 4(1)(b) now brings electronic money institutions within the definition.

⁸⁹ Proposed Payment Services Directive (24 April 2007 text) arts 1, 4(2a) and 2b), Annex.

⁹⁰ e-Money Directive art. 1(3)(a).

Further examples of uncertainty caused by attempts at technology neutrality are not hard to find. Readers might, for example, ask themselves how many “controllers” of personal data⁹¹ are to be found in the average university, and precisely what they need to do, or not to do, to export personal data from the EEA to a third country.⁹²

A further effect of technology neutrality is that it can tempt legislators into regulating prospectively, before it is properly understood how a new technology will be used and what problems the regulation will actually need to solve. One of the assumptions underlying the technology neutral approach is that such regulation will always be flexible enough to deal with the technology as it develops, but this has not always proved to be true in practice. ICT is not an end in itself but is used to achieve commercial and social ends, and it is these that may be changed by technology development in a way which outdates the regulation:

In the mid-90s, and still oft quoted today, technological neutrality is preached as a standard by which regulation in this field should be measured. Yet, technology is not neutral, ICTs are fundamentally altering the landscape and creating unique issues that policy-makers have to be prepared to address. One principle that would seem to stand the test of time, however, is that of allowing law to lag behind developments, rather than try to anticipate markets. The focus of the Electronic Signatures Directive on certification services, as the basis of a trust industry perceived critical to the mass take-up of electronic commerce, seems, to date, to be an example of how policy-makers can effectively regulate a market to a standstill.⁹³

4. Taking sides

When regulating new developments in ICT, lawmakers have to make a choice between technology neutral and technology specific approaches. How should they decide which side to take?

First, the lawmaker needs to be certain that both the technology and also, in particular, the ways in which it will be implemented and operated, are well understood. If the technology is so new that the ways in which it will be used are uncertain, technology neutral regulation is likely to result in one or more of the undesirable consequences explained in part 3.3 above. ICT is never regulated purely for its own sake, but aims to control the *users* of that technology and the *uses* they make of it. If that human behaviour is not properly understood, regulation is unlikely to be successful.

⁹¹ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995 p. 31 art. 2(d): “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”.

⁹² Compare the drafting of art. 25 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995 p. 31 with the ECJ decision in *Lindqvist*, Case C-101/01 6 November 2003, OJ C7 10 January 2004 p. 3.

⁹³ Ian Walden, “Regulating Electronic Commerce: Europe in the global e-economy” (2001) *EL Rev* 26(6) 529, 546

Second, a choice needs to be made between the different flavours of technology neutrality analysed in part 2 of this article. A technology indifferent approach should be adopted if the lawmaker is certain that the behaviour to be regulated is not made different in kind because of the use of different technologies. If, however, it is not clear precisely what those behaviours amount to when effected via the new technology⁹⁴ then technology indifference should be rejected.

Where the regulation will need to be applied to technology users alone, the choice lies between implementation neutrality and potential neutrality. Implementation neutrality is practicable if all known and anticipated implementations of the technology are capable of being used in compliance with the regulation. If, however, achievement of the regulatory aims requires that particular behaviours or effects must be mandated, and those behaviours or effects are only achievable via some of the technology implementations, then a potentially neutral approach can be used to permit the non-compliant technology to be modified so that compliance is possible.

Finally, the lawmaker ought to consider whether a *technology specific* approach would produce better regulation. Specificity is often rejected at the outset because technology neutrality has been hailed so loudly as the only correct way to proceed in the ICT arena, but it has a number of advantages. It creates substantial certainty as to the scope of the regulation and what needs to be done in or to comply with it.⁹⁵ As a consequence, the level of regulatory compliance is likely to be high, and the compliance costs lower than would be the case if advice were needed as to the meaning and application of the regulation. A further benefit of technology specific regulation is that its effects will not spill over into other fields of activity, forcing unwanted behavioural change in those fields.⁹⁶ Finally, specificity forces the lawmaker to reconsider the regulation at regular intervals⁹⁷, thus ensuring that the regulation keeps pace with technological and other changes.

⁹⁴ For example, “copying” or “publishing”.

⁹⁵ As an example from a different field of technology, the UK Road Vehicles (Construction and Use) Regulations 1986 SI 1986/1078 appear to be so clear in their application that there are no reported cases since 2000 which turned on the interpretation of those Regulations.

⁹⁶ “The experience of the 1870s may, however, remind us that technology-specific laws can be valuable, particularly where the goal is not outright prohibition. As we have seen, the goal of the prohibition on copying news was to facilitate the organization of economic relationships for dissemination and, in turn, to provide a legal mechanism for cost sharing. There was no need to extend the laws beyond news sent by telegraphy, nor necessarily to anticipate that later technologies of transmission would involve the same problems. Moreover, the importance of limiting the telegraphic property laws to news sent by electronic telegraph was to enable existing journalistic practices of appropriation, typically with attribution, to continue unaffected. The telegraphic property laws were formulated narrowly to meet the particular problem with a corresponding solution and to leave others alone.

Today, the drive for ‘technologically neutral’ laws, such as those that would broaden the notion of ‘reproduction,’ comes equally with the danger of bringing perfectly acceptable social practices into the realm of law, unintentionally replacing traditions with negotiations, and unnecessarily juridifying life worlds. A review of the story of the telegraphic property laws reminds us that technological neutrality is not always ideal.”

Lionel Bently, “Copyright and the Victorian Internet: Telegraphic Property Laws in Colonial Australia” (2004) 38 *Loy. L.A. L. Rev.* 71, 176.

⁹⁷ The Road Vehicles (Construction and Use) Regulations 1986 have been amended more than 20 times since their enactment.

Technology specificity does, of course, have a cost. It is immediately apparent that technological change will challenge such regulation, and that it is very likely that the regulation will not cope adequately with that change. This may not be so great a disadvantage as it might at first appear – as we have seen, purportedly technology neutral regulation is not necessarily good at coping with change either.⁹⁸

More important is the cost in legislative time and effort required to keep technology specific regulation up to date. Perhaps, though, this is an inevitable consequence of a world in which technological change occurs rapidly and in a seemingly unpredictable direction.⁹⁹ As Brownsword has noted in relation to the equally problematic technology of genetics:

*[If] there is a genuine question about whether (and, if so, where) the new technology falls within the spirit and intent of the regulatory scheme ... it is entirely appropriate that regulatory resource should be committed to further debate and decision concerning the new technology.*¹⁰⁰

The problem, of course, is that legislators are reluctant to re-examine issues which they believe they have already solved. In this regard, technology neutral regulation could be seen as a substitute for investing the effort necessary to decide whether regulatory objectives have been achieved and to remedy the law's inevitable defects.

⁹⁸ "... a good technology-neutral solution of today is not guaranteed to make sense in relation to a future technology simply because it is technology-neutral." Dan Jerker B. Svantesson, "The Characteristics Making Internet Communication Challenge Traditional Models of Regulation – what every international jurist should know about the internet" (2005) 13 *Int'l J.L. & Info. Tech.* 39, 64.

⁹⁹ "Our perspective of the sustainability of laws is influenced greatly by the past, and law-making processes are still largely the same as they were in the pre-ICT era. But time is a relative matter. The rate of change in current society is much higher than it used to be, and it might therefore be necessary to adapt our requirements of sustainability accordingly. In the industrial era, there may have been a requirement that laws should be sustainable for a period of, say, twenty or thirty years, but such a period seems much too long in the ICT era. ... It seems pointless these days to require telecommunications laws to last for decades, and the same holds for many other ICT laws." Koops, *op cit* note 11 p. 89.

¹⁰⁰ Roger Brownsword, "Regulating Human Genetics: New Dilemmas for a New Millennium" (2004) 12 *Med L Rev* 14, 32.