Journal of Information Law and Technology

The Law of Unintended Consequences – Embedded Business Models in IT Regulation

Chris Reed
Professor of Electronic Commerce Law,
Centre for Commercial Law Studies,
Queen Mary University of London

chris.reed@gmul.ac.uk

This is a **Refereed** Article published on **22nd November 2007**

Reed, C., "The Law of Unintended Consequences – embedded business models in IT regulation", JILT 2007 (2), <http://go.warwick.ac.uk/jilt/2007_2/reed/>

---

1 Introduction

During the last quarter of a century, information technology (IT) has permeated most aspects of our daily lives. At the beginning of that period possession of a computer was still a rarity[1]; today almost all businesses and the majority of UK homes[2] make extensive use of IT. The processing and communication of digital information is now so deeply entrenched in modern life that many of the things on which we rely, such as telecommunications and finance, would cease to operate without it.

As a consequence of this quiet revolution, legislators and regulators have made IT-specific provision in their laws and regulations.[3] This is both sensible and understandable. IT is now as fundamental to both commercial and non-commercial activity as, say, motor transport, and one need only imagine the chaos which would ensue if the uses of motoring technology were completely unregulated.

However, the experience of those who work with IT regulation on a daily basis is that it is often unsatisfactory in a number of respects. First, in spite of the best efforts of regulators, IT regulation has consistently failed to cope with the rapid changes in the technology and its uses which we have seen over that period. Second, sometimes as a consequence of technology change but on occasion from the outset, IT regulation has produced effects which were very different from those intended by the regulator, leading to a number of undesirable and unintended consequences.[4]

This article attempts to identify the structural defects in IT regulation which have produced these unintended consequences, and discusses how those defects might be remedied in future regulation. It concentrates on IT regulation at the European Union level, both because that regulation has wide geographical application and because it often serves as a model for other countries' regulation. It should be noted that the structural defects identified are not unique to EU regulation, and some examples from other jurisdictions are given to demonstrate this.

2 Futureproofing – technology-neutral regulation

Regulators have not been blind to the danger that rapid and unforeseeable advances in IT will render regulation unsuitable or ineffective, and have sought to prevent this occurring. Their primary tool for achieving this end has been to produce "technology-neutral" regulation, or at least to aim to do so.

> 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.[5]

The danger which technology-neutral regulation attempts to avoid is the embedding in the regulation of a particular model of how the technology works. Because IT changes so

rapidly, any regulation which is specific to a particular implementation of IT will inevitably fail to cope adequately with the technology which replaces it.[6]

The EU's 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*[7] sets out five principles with which IT regulation should comply. Such regulation should:

- Be based on clearly defined policy objectives;
- Be the minimum necessary to meet those objectives;
- Further enhance legal certainty in a dynamic market;
- Aim to be technologically neutral, and;
- Be enforced as closely as possible to the activities being regulated.

This is not the earliest use of the term "technology-neutral" in EU legislative documents.[8] It first appears in July 1998 in relation to the protection of minors from undesirable online content[9] and again in October in relation to e-money regulation[10], and has been used in almost all proposals to regulate IT since then.[11] The concept may have been applied as early as 1990 when the Directive on data protection was first proposed[12], as the European Commission's *First report on the implementation of the Data Protection Directive (95/46/EC)* in 2003[13] states:

> Despite the doubts raised during the negotiation of the Directive, Member States have thus reached the conclusion that the Directive's ambition to be technology-neutral is achieved, at least as regards the processing of sound and image data.

However, the concept of technology neutrality does not appear in the 1990 proposal, and the companion proposal for a Directive on telecommunications privacy[14] contains a number of provisions which are quite technology-specific.

It appears that the EU has been generally successful in achieving technology-neutral IT regulation in its most significant legal instruments in that area.[15] We can illustrate this by examining four legislative instruments which are representative of that body of regulation: Directive 95/46/EC on data protection[16] (the Data Protection Directive); Directive 96/9 on the legal protection of databases[17] (the Databases Directive); Directive 1999/93 on electronic signatures[18] (the e-Signatures Directive); and Directive 200/46/EC on electronic money[19] (the e-Money Directive).

The field of application of the Data Protection Directive is explained in art. 3(1), which provides:

> This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of

> personal data which form part of a filing system or are intended to form part of a filing system.

It is immediately apparent that all technologies which might be used to process data automatically, most obviously computers but extending to older technologies such as punched card readers[20] and new technologies not yet invented, are covered by this drafting. Similarly, the key terms used in the Directive are either defined in technology-neutral language[21] or are left undefined.[22] The obligations imposed upon controllers and processors are non-technological and focus on behaviours such as fair and lawful processing[23], taking reasonable security precautions[24], providing information to data subjects[25] and the like. Overall, it is not possible to identify any provision of the Directive which does not apply to current technologies for processing personal data, or which would not apply to any such technology whose future development can currently be envisaged.

The Databases Directive deals with the commercial aspects of data, harmonising copyright protection for databases within the EU and introducing an unauthorised extraction right to protect some aspects of databases which are not subject to copyright. Its core subject matter is defined in apparently technology-neutral terms:

> "Database" shall mean a collection of independent works, data or other materials arranged in a systematic or methodical way and capable of being individually accessed by electronic or other means.[26]

Initially this definition was criticised for restricting protection to databases which were arranged systematically or methodically, on the ground that it would exclude those technologies which used advanced software to make unstructured data accessible.[27] However, it seems probable that completely unstructured databases are unlikely to be commercially exploitable[28] and that the definition is thus, in practice, technology-neutral.

The owner of rights in a database is granted legal protection against infringing copying of those elements protected by copyright, and against extraction or re-utilisation of a substantial part of the non-copyright protected elements.[29] "Extraction" is "the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form", and "re-utilisation" occurs by "any form of making available to the public all or a substantial part of the contents of a database".[30] All of these are technology-neutral concepts.

Electronic signatures are by definition a creature of computing technology, and it might therefore be expected that their regulation could not be technology-neutral. However, the UK's law relating to signatures has always been based on their evidential functions rather than the means used to effect a signature[31], and the trend in e-signature regulation world-wide is to adopt a functional rather than a formal approach.[32]

The e-Signatures Directive is, of course, not completely technology-neutral because it applies only to electronic signatures. However, within that limitation the Directive is

remarkably successful in not mandating or excluding any particular e-signature technology.

Electronic signatures are defined by art 2 of the Directive as follows:

> 1. “electronic signature” means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;
>
> 2. “advanced electronic signature” means an electronic signature which meets the following requirements:
>
> (a) it is uniquely linked to the signatory;
>
> (b) it is capable of identifying the signatory;
>
> (c) it is created using means that the signatory can maintain under his sole control; and
>
> (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

This produces two types of electronic signature.

The first is simple electronic signatures, which have merely to meet the definition in art 2(1) and are not to be denied validity, enforceability and effectiveness solely on the grounds that they are in electronic form or are not certified.[33] This type potentially encompasses such matters as including a scanned image of a manuscript signature in a word-processing document or typing the sender's name in an email. Whether these would amount to a valid signature, electronic form or lack of certification apart, remains a matter for national law.[34]

The second is advanced electronic signatures where the identity of the signatory is confirmed by a certificate issued by an appropriate third party[35] and complying with other provisions of the Directive (a qualified certificate)[36] and the certificate is created by means of a secure-signature-creation device.[37] The Directive provides that advanced signatures of this type will satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data, and are admissible as evidence in legal proceedings.[38] The characteristics of qualified certificates and secure-signature-creation devices are set out in functional, rather than technological terms: as examples, a qualified certificate must identify the issuing certification-service-provider[39], who must “use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process”[40], and secure-signature-creation devices must use “appropriate technical and procedural means” to ensure the uniqueness and unalterability of the signature.[41] Thus although the predominate technology for creating such advanced e-signatures is via public-private key encryption[42], it is equally

feasible to implement other e-signature technologies, such as biometrics[43], so as to comply with the Directive.[44]

The e-Money Directive regulates the issuance[45] of electronic money, defined as:

> monetary value as represented by a claim on the issuer 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;
>
> (iii) accepted as means of payment by undertakings other than the issuer.[46]

The only technological element of this definition is the requirement for storage on an electronic device. The Directive makes provision for authorisation of issuers, the financial requirements for authorisation and operation, redeemability of e-money, and the sound and prudent operation of the issuer. It is possible for the national supervisor of an electronic money institution to impose technology-specific rules, but the general practice in financial supervision is for these regulations to be technology-neutral as well.[47]

If, then, the EU's regulation of IT has to a large extent succeeded in its aim of technological neutrality, we must look elsewhere for the reasons why it has failed to cope with technological change and has produced unintended consequences. Is there some other aspect of futureproofing which is not addressed by technology-neutral regulation?

3 Embedded business models

Although it is common to talk of IT regulation, this is of course no more than a shorthand expression. It would be nonsensical to speak of a computer itself as being in breach of some regulation. What we mean by IT regulation is regulation of the *users* of IT and the *uses* they make of the technology; in other words, regulation of human behaviour in relation to IT use.

Regulators cannot undertake this task purely in the abstract. They need to develop an understanding of how IT is actually being used, or how it is expected to be used, in order to identify the behaviours which the regulation should attempt to influence. Thus IT regulation will always be based on some model of technology use, a *business model*. "Business" is used here in the wider sense of activity[48], rather than as a limitation to commercial uses of IT, though of course the majority of IT regulation is found in the commercial sphere and applies predominantly to commercial actors.

Are these business models relevant to the problem of futureproofing? The answer must surely be, "yes". If the business model is used not merely to identify the behaviours which should be regulated but is in addition embedded in the regulation, then the regulation will often mandate IT users to adopt that business model. It is well-known that business models in the IT arena change almost as fast as the technology itself changes, particularly where there is some element of online activity, and that predictions of the

ultimate business model or models which will be adopted are rarely accurate. Thus regulation which contains an embedded business model is at risk of exhibiting the same defects, so far as futureproofing is concerned, as regulation which embeds a particular technology and is thus not technology-neutral.

Outside the field of IT regulation it is common to find business models embedded in regulation. Thus, for example, the UK Partnership Act 1890 s. 1(1) provides:

> Partnership is the relation which subsists between persons carrying on a business in common with a view of profit.

and the remainder of the Act sets out the consequences of establishing such a relationship, as between the partners themselves[49] and in relation to persons dealing with the partnership. The modern shape of UK companies regulation, which was established in the second half of the nineteenth century[50], is based on an embedded business model under which the company has a discrete legal identity, is owned by its shareholders and is controlled in its day-to-day operations by its directors.

However, these are both examples are of regulation which was devised long after their respective business models became established by use. By the time the regulation was enacted the evolution of these business models had stabilised to such an extent that embedding them in the regulation did not cause major difficulties. It is instructive that the pre-1862 companies legislation, which was largely reactive to the problems which emerged as new uses of the corporate structure and new structures themselves were adopted, was amended constantly without much real success in achieving an effective system for their regulation.[51]

In the IT field it has been commonplace to regulate as soon as the potential implications of a new technology are noticed, and well before the business models under which that technology will be used are established. Such attempts to regulate a future which, it is clear, will contain a substantial degree of change can only be successful if the regulation is both technology-neutral *and* is capable of regulating the new business models which will inevitably emerge. Unfortunately, none of the regulation examined in part 2 above has succeeded in achieving this second requirement; in each case because elements of an inappropriate business model are unconsciously embedded in the regulation.[52]

3.1 EU IT regulation

It is perhaps unsurprising to find this defect in the Data Protection Directive, given the historical origins of data protection law. The Directive is based on the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[53], which itself has its origins in the Swedish Data Act of 1973[54] and the German Lande of Hesse's Data Protection Act 1970.[55] At that time, computers were rarely found outside universities, central and local government departments and large corporations. Although there were signs that the use of computing technology might become more widespread[56], the business model on which these early laws were based

was dictated by the limitations of the current technology.[57] Thus these laws assumed an organisation which:

- Operated a limited number of computers, usually only one, which had limited or no connectivity to other computers;
- Held each of its working[58] datasets in a single physical location and in most cases as a single set of punched cards or magnetic tapes or disks; and
- Allowed direct access to the computer and datasets only to a small core of technical staff.

This business model explains why the 1981 Council of Europe Convention concentrates its provisions primarily on the "automated data file" and the "controller of the file".[59] Article 3, which sets out the scope of the Convention, contains seven references to files and only one reference to the processing of personal data. The data security obligations of art. 7 apply only to the file, and the subject access provisions of art. 8(a) and (b) similarly apply only to files. It is clear that the drafters of the Convention had the business model set out above very much in mind, and to some extent embedded that model implicitly in the Convention.

By 1995 when the Data Protection Directive was enacted, it was clear that the processing of personal data was being undertaken very differently from the 1970s model. Many businesses were operating networks of personal computers, allowing staff to store data locally as well as to access central data files, and a rapidly increasing proportion of the population had access to a personal computer at home.[60] This was also the year when the internet is thought to have entered the consciousness of the general public[61], but although this development must have been known to the European Commission it was too late for the Directive to be amended to take account of the new possibilities for processing personal data online.

The legislative history of the Directive shows a recognition that the underlying business model for personal data processing was changing. The original 1990 proposal followed the Council of Europe Convention by drafting in terms of the file[62], but the importance of this concept was reduced in the Commission's modified proposal of 1992[63] and eliminated in the final text.[64] In spite of these amendments, however, three elements of the 1970s business model remain embedded in the Directive:

- The concept that an organisation, rather than its individual staff, determines whether personal data will be collected and for what purposes. This is seen most clearly in the notification provisions of arts. 18 and 19, which require a controller to notify the relevant national authority of a number of matters, including types of data to be collected and the purposes for which they will be processed, and not to commence processing prior to such notification. In the modern, distributed processing model these matters can be initiated by individual staff, and it is not feasible for an organisation to prevent decisions to collect and process data

being made, or to require them to be reported so that notification can be made. In practice this problem is largely overcome by notifying very wide and general categories of data and processing, but it is almost certain that every large organisation is still in breach of these articles because of the activities of some of its staff.

- The concept of controller itself is also an echo of the 1970s, containing an implicit assumption that there is central control of personal data processing and that the organisation's staff merely undertake that processing in accordance with central instructions. Under art. 2(d) the controller is defined as "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". If this were applied strictly to, say, a modern university, it is clear that almost every member of academic staff, and a large proportion of non-academic staff, will be controllers because they act autonomously in determining the purposes and means of processing personal data.[65] This would mean that each of these staff would have obligations to notify, to provide information to data subjects, to receive and act on subject access requests etc.

- The assumption that data can only be accessed via possession of a physical copy of the dataset is implicit in art. 25, which provides:

  > … the transfer[66] to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if … the third country in question ensures an adequate level of protection.

  It is clear that if a copy of a dataset[67] containing personal data is given to a person in a third country, a transfer will have taken place. However, it was only in 2003 in the case of *Lindqvist*[68] that the ECJ determined whether permitting remote access from a third country to personal data held on a server in the controller's country would infringe art. 25. The court decided that including personal data in a web page amounted to "processing", but that its availability world-wide via the internet was not a transfer of that data to persons accessing the website. Unfortunately the court did not give reasons for this decision, which nonetheless appears to confirm that art. 25 is not applicable to remote access to data and thus that the 1970s business model is firmly embedded in this part of the Directive.

The Databases Directive was enacted only a year after the Data Protection Directive, but even by the date of its original proposal in 1992[69] database technology was comparatively well-advanced and, in particular, the commercial methods of exploiting databases had largely ceased to evolve. Databases were then, and still are, exploited in one of two ways: by providing online access on a subscription basis (usually via dial-up in 1996 rather than online, as today); or by supplying a copy of the database to be installed on the user's

computing equipment in return for a licence fee. Although the business models were stable, however, the Databases Directive unintentionally embedded in its drafting the concept that the business of database makers was to seek out and make available third party data, rather than exploiting their own data.

Under art. 7(1) the Directive 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 …

Until 2004, the general consensus was that these words covered databases both of content originating from third parties, and content originating from the maker of the database.[70] Organisations which generate data, such as stock exchanges and market research companies, spend large amounts of money and effort in collecting, checking and storing their data, and there seemed no doubt that this would amount to a "substantial investment" for the purposes of art. 7(1). In that year, however, the ECJ decided the case of *British Horseracing Board Ltd and Others v William Hill Organization Ltd.*[71] The claimant (BHB) maintained a large database of information relating to horse racing, and the defendant had copied parts of it indirectly from sources published under licence from BHB, for use in the defendant's betting business. Initially in the UK the case proceeded on the assumption that the BHB database was protected by the sui generis right[72], and concentrated on whether William Hill's use infringed that right. Various questions about the proper interpretation of the Directive were referred to the European Court of Justice[73], including two which asked for a ruling on the proper interpretation of "obtaining" and "verification" in art. 7(1). In its judgment, the ECJ concentrated on these two questions. It made a distinction between *creating* and *obtaining* data, and held 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. When the UK Court of Appeal applied this ruling to the facts[74], the outcome was that the investment in the BHB database was almost all in its creation, and that therefore the database received no protection via the sui generis right.[75]

The effect of this decision is that most databases which consist of data generated by their maker will fall entirely outside the Directive's sui generis protection. The implicit and clearly unintended[76] assumption of the drafters, that the database industry's role was to collect and make available third party data rather than to generate such data itself, was found by the ECJ to be reflected in the language of art. 7(1) and the recitals, and thus to limit the scope of the sui generis right.

In its efforts to achieve technology-neutrality, the e-Signatures Directive managed also to avoid embedding most aspects of the various e-signature business models which were then under development. However, its aim of legislating for a type of e-signature[77] which would be accepted in all Member States and beyond required it to include provisions relating to the liability of the entity (the certification-service-provider) which certifies the signatory's identity and other attributes.[78] By issuing such a certificate, the certification-

service-provider is subject to negligence-based liability to any person who relies on the following matters:

- The accuracy of the certificate's contents[79];
- That the person named in the certificate controlled the technology used to create the signature[80]; and
- That the certification-service-provider's register of revoked certificates is accurate.[81]

These liability provisions contain an implicit assumption that these matters are under the certification-service-provider's control, i.e. that it performs identity and attribute checks before issuing the certificate, verifies that the signatory controls the technology and operates the register of revoked certificates. These liability provisions derive from the ANSI X.509 standard[82], which assumed an open rather than a closed PKI model[83], and thus that the applicant for a certificate would provide proof of identity direct to a Certification Authority (a certification-service-provider in the Directive's terms). This assumption was based on an operational business model described in RFC 2527[84] which assumed that a signatory would purchase a single signature certificate from an independent Certification Authority and would use that certificate to validate all his e-signatures.

As e-signature schemes have been developed in recent years it has become clear that this model is not commercially viable. What happens in practice is that third parties, such as corporations or trade associations, identify a need for their employees or members to use electronic signature technology. In that case the third party enters into an agreement with a Certification Authority under which the third party will act as a Registration Authority. The Registration Authority, which already has a relationship with potential signatories, then identifies individuals and their attributes and provides the necessary identification information to the Certification Authority, using technology provided by the Certification Authority. The signature certificate issued by the Certification Authority thus certifies that the signatory has identified himself to the Registration Authority, and not directly to the Certification Authority.

This modern business model does not map accurately to the liability provisions of X.509-based legislation such as the Directive. As explained above, those laws place liability for inaccurate information in the certificate on the Certification Authority, whereas the body which has failed to take proper identification evidence is the Registration Authority. The consequences of this mismatch will be explored in part 4 below.

The Directive also provides in art. 6(3) and (4) that a certification-service-provider may establish use limitations and transaction limits[85] in the certificate. However, it does not explain the legal basis on which such limitations will be binding on the relying party, or even provide that they will be binding at all. This is also based on RFC 2527, whose description of the liability of Certification Authorities to relying parties assumes that limitations contained in a published certificate policy[86] will be binding, either in contract

or tort.[87] It is far from certain that this is a correct statement of the law, because it assumes that relying parties will receive from their software, or will seek out, information about these matters before relying on a certificate. Given that the appropriateness of the scheme of liability allocation in the Directive is based on the enforceability of these limitations, it is surprising that the UK implementing legislation[88] does not deal at all with the issue of use limitations and reliance limits, apparently sharing RFC 2527's presumption that these will be binding in contract or tort.

In the case of the e-Money Directive, there are two elements of embedded business model, one accidental, based on the anticipated way in which the technology would be used, and the other deliberate. The first element is the assumption that e-money would be used in a similar way to cash, and would therefore consist of an electronic equivalent of notes and coins which would be held in the possession of the customer, rather than merely recorded as accounting data as is the case for value held in bank accounts.[89] Thus recital 3 of the Directive states, "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", and the definition of electronic money in art. 1(3)(b) is:

> monetary value as represented by a claim on the issuer 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;
>
> (iii) accepted as means of payment by undertakings other than the issuer.

The rapid spread of internet access to consumers has meant that much simpler e-payment technologies have become workable – for example, the world's largest non-bank payment service, PayPal, holds funds on its internal accounting system and effects payments by simple book transfers. Only in the last two or three years have stored value e-money systems, the primary technology envisaged by the Directive, begun to achieve commercial significance.[90]

The deliberately embedded element was that issuers of e-money should be regulated as financial institutions, adopting the regulatory mechanisms which had been devised to ensure that custodians of financial assets would not put the value of those assets unreasonably at risk. Without considering whether this was the most appropriate way of regulating a pure payment technology with almost no custodianship element and which, at the time, had not been put into commercial operation to any appreciable extent[91], the Commission proposed a text under which e-money would be authorised and supervised by a national financial supervisor[92], meet minimum capital and liquidity requirements[93], limit investment of the float to specified, low-risk vehicles[94], and engage only in "the provision of closely related financial and non-financial services".[95]

The justification for these restrictions (most importantly the last, as we shall see in part 4 below) is to some extent for the protection of consumer holders of e-money, but primarily to "preserve a level playing field between electronic money institutions and other credit institutions issuing electronic money"[96] by limiting the ability of e-money issuers to compete with established financial institutions. For these policy reasons, therefore, the Directive embeds a business model under which e-money issuers are require to be regulated institutions, engaging solely[97] in the business of issuing and redeeming e-money. As explained below, recent developments in technology have led other types of business entity into the field of payment services, with the consequence that the Directive's provisions do not fit appropriately with their business practices.

3.2 Embedded business models in non-EU regulation

This examination of EU examples of IT regulation merely illustrates a phenomenon which can be observed world-wide. Business models are embedded in much of the world's IT regulation, perhaps to an even greater extent than that of the EU.[98] This is seen particularly clearly in the field of e-signatures, where early legislation was usually inspired by the ANSI X.509 business model and thus embedded many features of that model.[99]

One of the most troublesome business models which often attracts the attention of regulators is that of the offline publishing industry, in which those who make information available to the public, publishers, undertake a process of selecting the material which they will make available and exercise editorial control over its contents to ensure, amongst other things, that the published information complies with national controls on content such as defamation and indecency laws. Regulators have consistently failed to resist the temptation to apply this model to online intermediaries such as ISPs, based on the only similarity with publishers that each makes information accessible. Perhaps the most interesting examples of this phenomenon are the US Communications Decency Act 1996[100] and the Australian Broadcasting Services Amendment (Online Services) Act 1999.

The intention of the Communications Decency Act was to introduce new criminal offences of knowingly creating, sending, transmitting or displaying obscene or indecent materials to minors, or knowingly permitting the use of telecommunications systems for these purposes. As a counterbalancing element, the legislation provided protection for "Good Samaritan" activities on the part of ISPs. The aim was to overrule *Stratton Oakmont Inc v Prodigy Services Co*[101] and thus permit ISPs to introduce blocking or filtering technology without assuming the role of editor or publisher, which would otherwise make them responsible for the third party content.[102] However, the new criminal offences were struck down in *ACLU v Reno*[103] as infringing the First Amendment protection for freedom of speech, leaving the immunity provisions of § 230(c) to stand alone. The relevant part is sub-section (1) which provides, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The effect of this, discussed further in part 4 below, is to give a broad immunity from civil liability to ISPs and other intermediaries.

Australia's attempt to apply the publishing business model to ISPs took a different approach, trying to impose the same censorship regime as for films. The Broadcasting Services Amendment (Online Services) Act 1999 inserted a new Schedule 5 into the Broadcasting Services Act 1992, s. 10 of which defines "prohibited content"[104] which ISPs must not host. Content which has not yet been classified, including content hosted outside Australia, is "potential prohibited content".[105] On request from any person this must be classified by the Australian Broadcasting Authority (the ABA), using the same tests as for films and video games.[106] If a complaint is made that potentially prohibited content is being hosted in Australia or is accessible via an Australian ISP, and it is classified as prohibited content by the ABA, then the ABA can issue a take-down notice to the ISP[107] or, in the case of content hosted outside Australia, give notice requiring the ISP to prevent access to that content.[108] Failure to comply with such a notice by the end of the next business day is a criminal offence.

Both these laws were enacted on the assumption that, like offline publishers and film distributors, an ISP is capable of examining the content it makes available, accessing its compliance with legal standards and making the editorial decision whether to make that content available. This is so far from reality that it is unsurprising that neither law achieved its legislative aims.

3.3 Consequences of embedding

It would seem obvious that the presence of embedded business models will have the consequence that IT regulation is less futureproof than it might be. As new business models develop, compliance with regulation will inevitably become more difficult.

More serious, however, is the effect that these embedded business models have on the behaviour of those who are subject to the regulation. The next part of this article argues that the consequences of embedding have been largely unforeseen, and have been so different from what was expected by the regulators that, in some instances, the regulation produces effects which are very far from the original intention of its promoters.

4 Unintended consequences of embedded business models

Regulation aims to influence and control human behaviour, and the vast majority of businesses and private individuals want to act lawfully. It is therefore no surprise that IT users adopt behaviours which they believe will enable them to comply with IT regulation. If, though, we examine the behaviours which they have been constrained to adopt, it is often the case that these are very different from what the regulator originally intended. In many instances these unintended consequences of regulation are caused by those features which embed outdated or unworkable business models.

Part 3.1 above identified three embedded business model elements in the Data Protection Directive: that an organisation rather than its staff as individuals would determine the processing of personal data; that individuals would not exercise sufficient autonomous control over these matters to be data controllers themselves; and that access to and use of personal data required possession of a physical copy of the dataset. The consequences of

the mismatch between this model and reality, where possession and control of data is widely distributed and online access is, for most purposes, indistinguishable from use of a local copy of a dataset, has three main consequences.

First, the requirement to notify to a controller's national authority the types of personal data which will be held and the purposes for which they will be processed has become almost meaningless. Organisations no longer have detailed knowledge of the personal data processing undertaken by their staff, and in some cases even their "big picture" understanding of that processing may be inaccurate. In order to permit theoretical compliance with the Directive notification is made using broad, uninformative categorisations of data types and processing purposes[109], which fail to achieve the Directive's aim that data subjects should easily be able to discover what kinds of data an organisation might hold about them and how the organisation intends to use that data.[110] Notification has become a purely internal compliance function, undertaken for its own sake rather than for any useful end.

The second consequence is that compliance with the letter of the Directive is in many respects impossible in practice for any but the smallest organisation. To take just two examples:

- Article 11 requires a controller who obtains personal data from a source other than the subject to inform the subject of various matters at the time of recording the data or disclosing it to a third party. In, say, a university it is highly likely that some academics will have produced their own databases of information about their students' academic progress. Whether those students are informed about this will depend entirely on that academic's knowledge of data protection law. It is not feasible to devise central systems or processes to ensure that the university as a whole complies with art. 11. All large organisations experience similar compliance problems.

- A subject access request under art. 12 will be met by disclosure of the relevant records from an organisation's central computer systems, but it is unlikely that the organisation will be able to identify whether individual members of staff hold further information on their own computers or, even if this is discoverable, to devise an effective system for disclosing that information. It is fortunate that in practice most data subjects are satisfied with disclosure of central records only.

This situation is not unworkable because organisations and their staff normally comply with the spirit of the law, to the extent that they are aware of it. However, a system of regulation with which full compliance is impossible is clearly undesirable.[111]

Thirdly, the concept of protecting data subjects against the transfer of their personal information to "data havens", based on controlling the possession of datasets, has become meaningless in the online age. *Lindqvist*[112], if it is correctly decided and not reversed by future legislation, means that the complex legal structures which have been developed to

make offshore outsourcing possible[113] will no longer be required if the dataset can be stored within the EU and simply accessed remotely by the outsourcing service provider. The aim of art. 25, that personal data held in the EU should not be processed in another country which does not provide an adequate level of protection for that data, has been defeated by a change in business model.

The Databases Directive embeds a simple business model concept, that databases are made by intermediaries who collect third party data and make it available rather than by those who collect or generate data themselves directly. The effect of art. 7(1), as explained in *British Horseracing Board Ltd and Others v William Hill Organization Ltd*[114], is to prevent most databases whose content was generated by their maker from benefiting from the sui generis right. This is exactly the opposite of the original intention of the legislator.[115]

It is not possible for the maker of an unprotected database to prevent indirect extraction or re-utilisation by limiting access to online customers and imposing contractual restrictions on them, as art. 8(1) provides:

> The maker of a database which is made available to the public in whatever manner may not prevent a lawful user of the database from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever.

The only option remaining is to create a special-purpose corporate vehicle, to which the data is licensed for a fee and which itself compiles the data into a database. Provided such a vehicle *makes* the database, rather than merely receiving a ready-made copy from the data creator, the licence fees will amount to a substantial investment in obtaining the data and should thus qualify the database for sui generis right under art. 7(1). Such a corporate vehicle serves no commercial purpose other than overcoming the defects in the Directive caused by the embedded business model.

The liability provisions of the e-Signatures Directive embed a certification model under which the certification-service-provider itself performs checks on the identity and other attributes of the signatory and also confirms that the signatory possesses the signature-creation key. The effect of this is that the person who actually performs these functions, the Registration Authority, has no direct liability to a relying party.[116] This mismatch of business models creates real uncertainty as to the certification-service-provider's liability. There are two possibilities:

- Because liability under the Directive is negligence-based[117], a certification-service-provider might be held to have no liability at all to a relying party. Both UK[118] and US[119] negligence cases have held that where a function is properly delegated to a third party it will not be negligent for the delegator to rely on the performance of that third party unless there are reasons to suspect improper performance. This interpretation, if correct, would mean that the Directive has in practice failed to achieve its aims so far as liability is concerned.

- If, however, the negligence liability imposed on certification-service-providers by the Directive is a non-delegable duty[120] then liability can be reallocated from the certification-service-provider to the Registration Authority by means of indemnity provisions in the contract between them. These will normally extend beyond relying party losses and encompass some of the certification-service-provider's own risks. To counterbalance the extra risks which a Registration Authority thereby accepts, it is likely to insist on use limitations which prevent the certificates being used outside the confines of the closed PKI for which the contract was negotiated. This need to allocate liability risks through contract, rather than imposing them by law on the party who can obviate the risks, makes it less likely that existing closed PKIs will be extended to create the form of open PKI for Europe envisaged in the Directive.

It is worth noting that the uncertainties as to the liability position are made worse by the Directive's failure to specify clearly whether, and on what legal basis, any use limitations and transaction limits are binding on relying parties. This failure derives from assumptions about the way in which certification-service-providers and relying parties will communicate during the signature verification process, and thus how the law of contract and tort will view these limitations, and is a further consequence of implicit business model embedding.

The two embedded business model features found in the e-Money Directive, that e-money would be held in the possession of the user and that issuers should be authorised financial institutions only, have combined to produce real uncertainty as to which electronic payment technologies fall under the Directive. The wording of art. 1(3)(b)(i) requires e-money to be a claim on the issuer which is "stored on an electronic device", and it is strongly arguable that online payment systems which operate by transferring account balances held with the service provider (accounted e-payments) do not fall within this definition. What is stored on the provider's accounting systems is not the value itself but instead a record of the provider's indebtedness to each customer.[121]

To avoid the risk of acting unlawfully, accounted payment services such as PayPal and Neteller have obtained UK authorisation as electronic money institutions. However, a number of other businesses which are already in possession of customer funds have recognised the value of providing a payment service as part of their business model. The most important of these are the mobile telephone companies whose customers pre-pay for airtime. From those prepayments the companies can offer the service of making payment to selected merchants by simple internal accounting transfers. This accounted e-payments business model does not map easily on to the regulatory regime of the Directive, and the UK FSA's attempt to treat such services as e-money[122] has foundered because, apparently unnoticed by the FSA, requiring mobile telephone companies to become authorised as electronic money institutions would prevent them from continuing to provide telecommunications services. It remains to be established whether such payment services will be treated as e-money or will fall under the far less onerous provisions of the proposed Payment Services Directive.[123]

It may also be worth noting here that the supervisory model for e-money issuers, based on the assumption that they act as custodians of assets, means that acting as an authorised e-money issuer can only be a low-margin activity, and is only likely to be profitable for large issuers. This is a substantial entry barrier to potential new e-money services. As pointed out in part 3.1, however, the embedding of this business model was intentional, and may thus in part have been designed to preserve existing financial institutions from competition in the payment services market.

Where regulation has been based on the liability model for offline publishers and broadcasters, as discussed in part 3.2 above, the unintended consequences have been far more striking. Because parts of the original US Communications Decency Act were unconstitutional, these were struck out by the Supreme Court leaving only the provisions granting immunity from civil suit. In subsequent litigation it has been held that the Act provides a complete immunity from civil actions for defamation,[124] even where the ISP pays the author for the right to provide access to the defamatory material,[125] and even from a civil action alleging negligence in failing to prevent continued solicitations to purchase child pornography made via the ISP's system.[126] The aim of the legislation was to make ISPs police the internet and reduce the volume of indecent material available; the outcome has been exactly the opposite, and ISPs do no policing at all.[127] Similarly, the Australian Broadcasting Services Amendment Act had been intended to apply cinema censorship rules to online content. However, ISPs have no obligation in respect of prohibited content if they operate a "restricted access system"[128], and have therefore universally adopted the simplest method of achieving this by supplying filtering software to their customers. Filtering software is notoriously ineffective, particularly as its filtering parameters can be adjusted by technically knowledgeable users such as children. So far as an outside observer can ascertain little or no censorship of online content occurs in Australia, but providers of filtering software have found an important and continuing market.

5 Business model-neutral regulation

If, then, embedding business models in IT regulation produces structural defects which have unintended and unfavourable consequences, it would seem obvious that we should aim to regulate IT in a way which is not only technology-neutral, but business model-neutral as well. Achieving this aim is, however, more difficult than stating it.

A counsel of perfection would be to abstain from regulation until the business models adopted for a new field of IT activity have become established, thus reducing substantially the danger of unintentionally embedding features of an incompatible business model. Such a policy of masterly inactivity[129] is difficult to sustain, however, in the face of the pressures on IT regulators. All the EU Directives discussed above were enacted to resolve the situation of differing and incompatible national laws, as was the US E-Sign Act. Masterly inactivity can be effective if these pressures are absent; the US took a policy decision in 1996 not to regulate e-money until it became a significant factor in the payment services market[130], and this has proved a wise decision as the current e-money business models are very different from those envisaged in 1996.

5.1 A three-step approach

It is unusual to find a business model embedded in regulation intentionally – the only example identified above is the restriction of e-money issuance to authorised institutions. More commonly the embedding is both implicit and unconscious. The first step towards business model-neutral regulation must therefore be for the regulator to articulate the business model which has inspired that regulation.

This will enable two important checks to be made:

- The business model can be compared with current uses of the technology to identify errors and omissions. As an example, although the internet had not entered the public consciousness during the period 1990-1995 when the Data Protection Directive was under discussion, it was well-known that organisations were sharing data cross-border via proprietary networks rather than transferring datasets between those countries. Articulating this fact would have raised the question whether such sharing amounted to a "transfer" of data, and thus avoided embedding in the Directive the assumption that physically transferring copies of datasets were the only way in which cross-border use would be undertaken.

- Predicted changes in the technology and its use can then be researched, and their effects on the underlying business model analysed. In relation to e-signatures the concept of involving a Registration Authority in the certification process had been identified by 1999[131], and even before that date experts were arguing that the closed PKI model would be more commercially successful than the open model.[132] Identifying this as a potential development in the e-signatures business model would have raised the question of what liability the e-Signatures Directive should impose on Registration Authorities. Similarly, the e-Money Directive's embedding of the stored value business model for e-money was based on the predominate technologies of the time, but accounted e-payment systems were already in operation[133] and the mass penetration of the internet to private users was clearly predictable.[134] This should have alerted the regulators to the possibility that the accounted e-payment model might soon become viable, and thus led them to consider whether such payment services should be encompassed by the Directive.

The second step is to avoid the temptations of analogy. The fact that an existing sphere of activity operates successfully under its current regulation does not mean that a new activity, whose anticipated business model has common features with that of the existing activity, can successfully be regulated in the same way. The US Communications Decency Act and the Australian Broadcasting Services Amendment Act provide striking examples of how spectacularly this approach can fail. The danger of regulating by analogy will be much reduced if the business model of the new activity is properly articulated, as suggested in step one, because if this is done the differences between the two business models should become apparent.

The final step which regulators need to take, once they have a clear (and ideally reasonably mature) business model in mind, is to ensure so far as is possible that the regulation does not either (a) mandate those subject to the regulation to adopt the particular business model, or (b) favour that model over alternative models which might later be developed. This is a similar approach to that which has been largely successful in achieving technology-neutral regulation[135], and is examined in detail in the next part.

5.2 Achieving business model-neutrality

Once a clear and accurate business model for the activity to be regulated has been developed, regulators will have sufficient information about that activity to attempt to draft it in business model-neutral terms. There are a number of techniques which would assist this process.

First, it is essential to identify and enunciate the regulatory objectives. It is surprising how seldom this is done in any depth, and how easy it is to assume that controlling some aspect of the business model will achieve the intended result without questioning that assumption. Two examples from the EU IT regulation discussed above illustrate this particularly clearly:

- The Data Protection Directive does not explain what it aims to achieve by the prohibition in art. 25 on transferring personal data outside the EU. Is it the transfer itself which is the problem, or is the aim to ensure that personal data originating within the EU does not lose the privacy protections set out in the Directive when it is processed in a third country?[136] Assuming the latter to have been the regulatory aim, then if this had been expressed it would have been clear that data whose storage remained within the EU, but was processed outside, presented a potential problem. The difficulty could have been resolved either by defining "transfer" to include such remote processing or by imposing an obligation on the controller to ensure that any processing outside the EU did not deprive the data of those protections unless the place of processing also provided adequate protection. The latter would have been preferable because it addresses the aim more directly, and should thus work for future technologies or business models which might fall outside a revised definition of "transfer".

- The regulatory objective of the liability regime set out in the e-Signatures Directive[137] appears to have been to give a remedy to a relying party who suffers loss as a consequence of inaccurate information in a signature certificate. However, this is not stated anywhere in the legislative history of the Directive, which simply and without comment sets out a minimum level of liability for certification-service-providers. Had the regulatory aim been enunciated, it should have alerted the legislators to the possibility that this information might in practice be verified by persons other than the certification-service-providers and a consequent recognition that the verifying person might more appropriately bear the liability. This would

> have been a more nearly optimum solution because (a) it is the person who verified the information who was negligent and is therefore responsible for the loss, and (b) this approach regulates the behaviour of the verifier rather than the person who merely has the status of certification-service-provider, the quality of whose processes may play no role in determining whether the verification is accurate..

This leads us to the second technique, which is for the regulation to address human behaviour directly, rather than indirectly by regulating institutions, structures or status. The latter approach contains an implicit assumption that the institution, structure or person of that status actually undertakes the behaviour in question, and thus embeds part of the underlying business model. As we have seen, this assumption is often falsified by changes in business model: Registration Authorities take over functions which in the e-signatures model were performed by certification-service-providers, individual staff members take decisions about personal data processing which the data protection model presumed would be the preserve of the employer, non-financial institutions identify a business case for providing ancillary e-payment services, and so on. Even when business models change the behaviours usually continue, and thus regulating behaviour alone tends towards business model-neutrality.

The third requires regulators to recognise that the behaviours addressed by the regulation may not always be carried out in the manner anticipated in their original business models. A failure to notice this can lead to the unintentional embedding of a business model by limiting the scope of the regulation to those behaviours envisaged in the model. The drafters of the Databases Directive defined "making" a database in terms of "obtaining, verification or presentation"[138] of its contents, and therefore granted sui generis protection where there had been a substantial investment in those activities. Had they resisted the temptation to explain "making" and merely required there to have been a substantial investment in that making, *British Horseracing Board Ltd and Others v William Hill Organization Ltd*[139] would have been decided differently and the original intention of the Directive would have been preserved.[140]

Finally, IT regulation should be undertaken at the most general level which is likely to achieve its objectives. The more detail included in regulation about the precise behaviours which are to be regulated, the more likely the regulation is to become outdated. For the same reasons, there is likely to be an inverse relationship between the volume of detail and the regulation's business model-neutrality. It is instructive to compare IT regulation with the regulation of banks and financial services; the latter has proved far more robust in coping with technology and business model change. The reason for this seems to be the de-centred regulatory system adopted for the financial industries[141], under which legislation sets out general principles[142], softer regulation is produced by an industry supervisor to explain these general principles in more detail and can be changed rapidly in response to new developments[143], and codes of practice are developed by the industry itself at the most detailed level.[144] This regulatory system permits, for example, primary legislation to impose obligations to act reasonably or fairly while leaving the detail of what is reasonable or fair to be determined at a lower regulatory level.[145]

6 The law of unintended consequences

Legislators have a touching faith that passing laws is an effective way to ensure that what they intend to happen will in fact happen. They therefore have a natural tendency, when devising legislation, to concentrate on their intended consequences. Unfortunately, these do not always come to pass.

The Databases Directive aimed to correct the "… very great imbalance in the level of investment in the database sector both as between the Member States and between the Community and the world's largest database-producing third countries …"[146] by creating a uniform protection regime for databases in the EU, but the level of EU database production has not increased over the pre-Directive level.[147] The e-Signatures Directive states confidently that "a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies"[148], but at the time of writing there is little or no use of e-signatures outside closed PKIs, and no sign of cross-border use within the EU. The e-Money Directive aimed "to provide a regulatory framework that assists electronic money in delivering its full potential benefits and that avoids hampering technological innovation in particular"[149], but the result has been that only a handful of electronic money institutions are authorised in the EU and e-money represents a tiny proportion of payment transactions.[150]

This tendency to concentrate on the intended consequences of regulation often means that its potential to produce *unintended* consequences is overlooked. As this article has explained, these unintended consequences are usually quite different from what was originally intended, and in some cases produce almost diametrically opposite effects.

One of the most important reasons why regulation has unintended consequences is that it embeds a business model in the regulation, usually unintentionally. IT users who operate under other business models need to modify their behaviours to become compliant with the regulation, and the mismatch between business models often results in those behaviours being very different from the regulator's expectations.

Embedded business models can be avoided by producing regulation which is both technology and business model-neutral. Business model-neutrality is a new concept for regulators[151], and it is suggested that it might be achieved via the three-step process outlined in part 5 of this article.

The alternative to business model-neutrality is that we will continue to see IT regulation which fails to achieve its aims and produces unintended consequences. That this provides much-needed work for both academic and practising lawyers is an additional unintended consequence; how far it is also undesirable must be left for the reader to judge.

[1] The IBM PC was introduced in 1981 with a base price of US$1,565, which purchased 16Kb of RAM and a 160Kb floppy disk drive. See <http://www-03.ibm.com/ibm/history/history/year_1981.html> and <http://inventors.about.com/library/weekly/aa031599.htm>. To put its affordability in context, in 1982 the author received a research grant to purchase an IBM PC for about 25% of a UK Lecturer's annual salary. A perfectly useful PC can be purchased today for about 1% of a Lecturer's salary.

[2] A typical UK household might contain one or more personal computers, several mobile phones, various entertainment devices such as DVD players and digital music players, a broadband router, etc. All of these are more powerful computers than the 1981 IBM PC. National Statistics estimated in August 2006 that 57% of UK households had internet access, 69% of these being broadband <http://www.statistics.gov.uk>.

[3] For ease of reading, the terms "regulation" and "regulators" are used predominately henceforward to cover both legislation and non-statutory regulation and those who are responsible for its introduction.

[4] To avoid repetition, these assertions are not substantiated here but are, it is hoped, made good in part 4 below.

[5] 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. A further explanation is given in 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.".

[6] "Regulation that is based on specific technology can quickly become outdated, and may lead to inefficient investment by market players." Ibid p. 14.

[7] COM (1999) 539 final, 10 November 1999 p. 13-15.

[8] The origin of the term for IT regulation may be the US Government's *Framework for Global Electronic Commerce* of 1 July 1997, which states: "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)" <http://www.technology.gov/digeconomy/framewrk.htm>. Soon thereafter it began to appear in writings on IT regulation world-wide – see e.g. Aalberts & van der Hof, "Digital Signature Blindness: Analysis of legislative approaches toward electronic authentication", November 1999, http://rechten.uvt.nl/simone/Digsigbl.pdf pp. 14-18 and references therein.

[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."

[10] 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 to the extent necessary for ensuring their sound and prudent operation and their financial integrity in particular".

[11] 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.

[12] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (90) 314 final p. 1 ff.

[13] COM (2003) 265 final.

[14] Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network (ISDN) and public digital mobile networks, COM (90) 314 final p. 75 ff.

[15] My thanks are due to Holly Towle of K&L Gates and Christopher Millard of Linklaters for independently pointing out that a significant proportion of the EU legislation which regulates more detailed aspects of IT is very far from technology-neutral. See e.g. Towle, Dyer & Evans, "The European Union Directive on Waste Electrical and Electronic Equipment: a study in trans-Atlantic zealotry", " (2004) 31 Rutgers Computer & Tech. L.J. 49, 60-66.

[16] 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.

[17] OJ L77, 27 March 1996 p. 20.

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

[19] 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 200 p. 39.

[20] One of the earliest automated searching technologies was the Hollerith Tabulator, invented to process punched cards for the 1890 US census and which laid down the foundation of the IBM corporation – see <http://www.columbia.edu/acis/history/tabulator.html>.

[21] Data Protection Directive Art. 2:

> (a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject") …
>
> (b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means …
>
> (c) "personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) “controller” shall mean 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 …

[22] Most notably, “collection” and “transfer” of personal data.

[23] Data Protection Directive art. 6.

[24] Data Protection Directive art. 17.

[25] Data Protection Directive arts 10-12.

[26] Databases Directive art. 1(2).

[27] See e.g. Pattinson, “The European Commission's Proposal On The Protection Of Computer Databases” (1992) 14 EIPR 113, 116; Chalton, “Property in Databases”, Chapter 7 in Reed & Angel (eds), *Computer Law* (4th ed. Oxford University Press, Oxford 2000) 232.

[28] See Reed, “Database Protection” in Reed & Angel (eds), *Computer Law* (6th ed. Oxford University Press, Oxford 2007) Chapter 8.5.

[29] Databases Directive art. 7(1).

[30] Databases Directive art. 7(2).

[31] See 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/>.

[32] See e.g. UNCITRAL Model Law on Electronic Commerce 1996 art. 7(1), UNCITRAL Model Law on Electronic Signatures 2001 art. 2(a); Australian Electronic Transactions Act 1999, s 10(1); US Federal Electronic Signatures in Global and National Commerce Act 2000, 15 USC 7001 §106(5).

Some early e-signature laws, e.g. the German Digital Signature Act (Signaturgesetz) and Digital Signature Ordinance (Signaturverordnung) 1997, mandated particular e-signature technologies. The potential incompatibility between EU Member State laws which such an approach would produce was an important reasons for adopting the e-Signatures Directive.

[33] e-Signatures Directive art. 5(2).

[34] Thus in the UK, for example, the court would need to be convinced that the purported signatory intended to sign and to adopt the contents of the document as his own – see Reed, “What *is* a signature” 2000(3) *The Journal of Information, Law and Technology (JILT)* part 3.1 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/.

[35] A “certification service provider”, defined in e-Signatures Directive art.2(11).

[36] e-Signatures Directive art. 2(10). The certificate must fulfil the requirements of Annex I, and it must be issued by a certification-service-provider who meets the requirements of Annex II.

[37] Under e-Signatures Directive art. 2(6) such a device must meet the requirements of Annex III.

[38] e-Signatures Directive art. 5(1)

[39] Annex I (d) and (h).

[40] Annex II (f).

[41] Annex III (1).

[42] See Rivest RL, Shamir A and Adleman L, "A method of obtaining digital signatures and public key cryptosystems" 21 *Communications of the ACM* 120 (1978), the starting point for the development of this technology.

[43] See Phillips, Martin, Wilson and Przybocki, "An introduction evaluating biometric systems" (2000) 33(2) *Computer* 56.

[44] See contra Towle, "E-Signatures – Basics of the US Structure", (2001) 38 Hous. L. Rev. 921, 947: "… there is concern that this approach will not recognize non-certificate based electronic signatures, such as those based on biometric technologies." However, it is important to note that third party certification could be included in the implementation of biometric technologies, and to this extent the Directive is technologically neutral as between those technologies and e-signatures based on public/private key encryption. Indeed, public/private key e-signatures were originally proposed without the additional feature of third party certification – see Rivest, Shamir and Adleman, "A method of obtaining digital signatures and public key cryptosystems" 21 *Communications of the ACM* 120 (1978) – and such e-signatures would equally be excluded from equivalence to hand-written signatures under the Directive.

[45] The supply, use, acceptance and settlement of e-money is not regulated by the Directive, though these matters might be subject to national regulation on e.g. the provision of payment services.

[46] e-Money Directive art. 1(3)(b).

[47] See e.g. UK FSA Handbook, ELM 5.4 and SYSC 3.

[48] See *Shorter Oxford English Dictionary* definition 9: "That about which one is busy; function, occupation".

[49] However, s. 19 permits the partners to agree on different relations between themselves than those set out in the Act, thus providing a high degree of flexibility and futureproofing.

[50] The UK Companies Act 1862 is generally seen as the starting point for the modern corporation. See Davenport, "What did *Russell v Northern Bank Development Corporation Ltd* decide" (1993) LQR 553, 557-8; Lobban, "Nineteenth Century Frauds in Company Formation: *Derry v Peek* in context" (1996) LQR 287, 288:

> … in the mid-century, the courts … had seen all those who signed a deed of settlement as partners with liability to creditors. After 1862, they took a different approach, seeing the company more as an abstract entity. On the one hand, shareholders were no longer seen as partners who had pledged their credit to the world at large. With the vague definition of the company member given in the 1862 Companies Act, it was no longer possible simply to see allottees whose names were on the register as partners. On the other hand, directors were increasingly seen as agents of the company (but not of the individual shareholders) …

[51] See Lobban, "Nineteenth Century Frauds in Company Formation: *Derry v Peek* in context" (1996) LQR 287, 289-317.

[52] The harmful consequences of intentionally favouring a particular business model have been recognised by Amelia Boss, initially in relation to e-signature legislation, where she states that the goals of such laws should be to "remove the barriers to electronic commerce, treat electronic communications on a par with paper communications, and not to favor one technology over another (technology neutrality) nor one business model over another (implementation neutrality)." Boss, "Searching for Security in the Law of Electronic Commerce", (1999) 23 Nova L Rev 585; see also Boss, "The Uniform Electronic Transactions Act in a Global Environment" (2001) 37 Idaho L Rev 275, 292.

The concept of implementation neutrality may have originated in the US contributions to the discussions on the UNCITRAL Model Law on Electronic Commerce, which proposed inclusion of the concept in the Model law - "Implementation Neutrality - Any rules should neither require nor hinder the use or development of new or innovative business applications or implementation models." *US Proposal for "International Convention On Electronic Transactions"* A/CN.9/WG.IV/WP.77, 25 May 1998 Chapter II – and influenced US policy on e-commerce law development:

> The market is very much in the early stages of experimentation with respect to business models for electronic commerce. The United States believes it is not wise at this time to attempt to identify a single model that these transactions will use or to develop a legal environment using a single model. Indeed, such an approach would prevent the market from testing different possible approaches and prematurely impose a particular model on all electronic commerce, inevitably limiting its growth. Therefore, at the current state of development, the legal framework should support a variety of business models so that the market is able to experiment and select the models that best fit particular types of electronic commerce. (U.S Government Working Group on Electronic Commerce, *First Annual Report* (Nov. 1998) p 14)

See also HR Subcommittee on Cts. and Intell. Prop., Hearing on H.R. 1714, Electronic Signatures in Global and National Commerce Act, 106th Cong. P 5 (Sept. 30, 1999), Testimony of Pamela Meade Sargent, Commissioner for the NCCUSL p. 5.

These discussions of the concept appear to have focused on laws which intentionally favour a particular business model, and thus to have overlooked the possibility of unintentional embedding. It has not been possible to find an express recognition of the need for business model-neutrality, intentional or unintentional, outside the US literature.

[53] ETS no. 108, Strasbourg, 28 January 1981.

[54] Datalagen, 1973:289.

[55] Hessisches Datenschutzgesetz, Gesetz und Verordungsblatt I (1970), 625.

[56] The first commercial microprocessor, Intel's 4004, was launched in 1971 and the Apple II, the first genuinely mass-market personal computer, came on to the market in 1977. ARPANET, the defence research project which grew into the internet, started in 1969 but did not lose its military research basis until the early 1980s.

[57] As an example, the author studied computer programming at the University of Keele in 1975, working on an Elliott 803 computer – see <http://bil.members.beeb.net/elliott.html>. This was the Department of Computer Science's primary machine. It had only 8Kb of RAM and no possibility of network connectivity, as the sole I/O mechanisms were punched card/tape or magnetic tape. Only trained technicians were permitted to operate it directly. My thanks are due to Colin Reeves, former Head of Department at the University of Keele, for correcting my memories of this system.

[58] Backup datasets would most likely be held in a different location, but could only be accessed by physically bringing them to a suitable computer.

[59] Both defined in art. 2.

[60] US home computer access rose from 8% in 1984 to 24% in 1994 – National Science Foundation, *The Application and Implications of Information Technologies in the Home: Where Are the Data and What Do They Say?* (February 2001) p. 11, citing US Bureau of the Census data.

[61] Probably based on the founding of the World Wide Web Consortium in September 1994. General public use of the internet was made possible by the 30 April 1993 announcement by CERN that it was placing the basic World Wide Web technology into the public domain and the launch of the Mosaic graphical browser by the National Center for Supercomputing Applications in the same year.

[62] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (90) 314 final art. 1(1): "The Member States shall ensure, in accordance with this Directive, the protection of the privacy of individuals in relation to the processing of personal data contained in data files." The concept of "data file" is used throughout this draft.

[63] The concept of "personal data file" was retained primarily in relation to manual processing - COM(1992)0422 15 October 1992, Explanatory Memorandum p. 2.

[64] Except for manual data, to which the Directive applies only if that data forms part of a "filing system" – arts 2(c), 3(1).

[65] The university itself may also be a controller of that personal data, on the basis that it acts through its staff and thus their decisions are also its own decisions.

[66] Although the term "transfer" is used 29 times in the recitals and articles of the Directive, it is never defined.

[67] Or a part of a dataset – Data Protection Directive recital 58.

[68] Case C-101/01 6 November 2003, OJ C7 10 January 2004 p. 3.

[69] Proposal for a Council directive on the legal protection of databases, COM(92)24 final, OJ C 156 23 June 1992 p. 4.

[70] This was clearly the original aim of the legislator. The explanatory memorandum to the 1992 proposal, COM(92)24 final paras 3.2.7 and 3.2.8 p. 25, makes it clear that the Directive was intended to protect *all* databases against parasitic competition. Specific provisions were included to require the maker of a database who was also the only source of that data to grant compulsory licences (art. 8(1)-(3) thus confirming that those "single source" databases were to be covered by the sui generis sight. The later deletion of these compulsory licensing provisions, coupled with the insertion of the "investment" requirement as a way of distinguishing valuable from trivial databases, produced the unintended business model embedding identified here.

Certainly the European Commission held this view of the Directive's intended scope throughout: "databases which qualified for copyright protection under the 'sweat of the brow' regime would no longer be protected. In exchange, and in order to compensate for the loss of the 'sweat of the brow' protection, the 'sui generis' form of protection for 'non-original' databases was introduced as an entirely novel form of

intellectual property." 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. 8.

[71] 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.

[72] [2001] EWHC 516 (Pat.) para. 21.

[73] Set out at Case C-203/02 9th November 2004 para. 22.

[74] [2005] EWCA Civ 863 (CA).

[75] For a more detailed discussion of this judgment see Reed, "Database Protection" in Reed & Angel (eds), *Computer Law* (6th, OUP 2007) Ch. 8 pp. 415-420.

[76] 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, states that the effect of the decisions in *British Horseracing Board Ltd v William Hill* and the *Fixtures Marketing* cases (Cases C-46/02, C-338/02 and C-444/02, all of 9th November 2004): "…[goes] against the Commission's original intention of protecting 'non-original' databases in a wide sense".

[77] The advanced electronic signature meeting the Directive's other requirements and certified by an appropriate person – see part 2 above.

[78] e-Signatures Directive art. 6. These attributes might include the signatory's employment or professional status, the extent of his authority to bind his employer, etc.

[79] e-Signatures Directive art. 6(1)(a).

[80] e-Signatures Directive art. 6(1)(b) & (c).

[81] e-Signatures Directive art. 6(2).

[82] See Housley, Ford, Polk and Solo *Internet X.509 Public Key Infrastructure – Certificate and CRL Profile* RFC 2459, January 1999, available from <http://www.ietf.org/rfc.html>.

[83] An open PKI (public key infrastructure) is where the signatory obtains a certificate from a Certification Authority and uses that single certificate for all his communications. In a closed PKI, all signatories are members of the same organisation, company or group, and certificates are issued only for the purpose of signing communications within the group.

[84] Chokhani & Ford, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* RFC 2527, March 1999, available from <http://www.ietf.org/rfc.html>.

[85] Thus, for example, the certificate might be usable only to sign purchase orders for the signatory's employer (a use limitation) up to a maximum value of X (the transaction limit).

[86] The normal practice would be for the signature certificate to contain a link to the certificate policy, thus enabling the relying party to investigate the limitations and, possibly, enabling his signature-checking technology to discover and flag these limitations.

[87] RFC 2527 is an operational description, not a legal analysis, and thus these points are presumed but not explained.

The contractual analysis would be that the relying party has received notice of the limitations, via the link in the certificate to the certificate policy, and that the issue of the certificate is a unilateral offer by the Certification Authority to be liable to relying parties on the terms of the certificate policy. That offer is accepted by the act of reliance, forming a contract between the Certification Authority and the relying party. Given the high degree of automation in e-signature validation, it is by no means clear that a court would find accept this analysis.

The tortious analysis would be that the Certification Authority is liable to relying parties for fraud or negligent misrepresentation (see American Bar Association *Digital Signature Guidelines* (Chicago: ABA, 1996) p. 22), and in either case will only be liable to the extent that it was reasonable to rely on the certificate in those circumstances. Reliance outside the terms of the certificate policy, assuming the relying party has sufficient notice of it, would be unreasonable under English and most US State laws.

[88] UK Electronic Signatures Regulations 2002, SI 2002 no. 318.

[89] The origins of the technological concept 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, was invented by Tim Jones and Graham Higgins in 1990 with in-house trials at NatWest in 1992 (see the Mondex timeline, <https://mbe2stl101.mastercard.net/public/login/ebusiness/smart_cards/mondex/about/Visio-history.pdf>).

[90] A small number of increasingly active stored value e-money businesses is now visible. Hong Kong's Octopus Card has more holders than the population of Kong Kong, and its success has inspired Transport for London to begin a project to introduce e-money functionality to the Oyster Card. The Proton stored value card is widely used in Belgium, and the Chipknip card appears to be taking off in the Netherlands.

[91] "At the present juncture, electronic money is not a widespread phenomenon." Opinion of the EMI Council on the issuance of electronic money, 2 March 1998 para. 1. See also ECB, *Report on Electronic Money* (August 1998) pp. 9-10.

[92] Authorisation is required by e-Money Directive art. 1(4) and the supervision provisions are contained in arts 4-6.

[93] e-Money Directive art. 4.

[94] e-Money Directive art. 5.

[95] e-Money Directive art. 1(5).

[96] e-Money Directive recital 12.

[97] With the exception of related minor technical activities which could not be a significant source of income – see e-Money Directive art. 1(5).

[98] Whatever its other flaws, the EU's technocratic legislative process, which often bases first drafts of directives on theoretical research and allows a period of years for consultation and amendment, tends to eliminate the most egregious flaws in legislative proposals unless they are the subject of political disagreement and subsequent compromise.

[99] In the late 1990s the majority of US States adopted or proposed e-signature laws, many of which were X.509-based. The danger of embedding this particular business model, particularly in relation to liability, was recognised in a number of articles – see e.g. Biddle, "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace" (1997) 34 San Diego L. Rev. 1225, 1226; Smedinghoff & Bro, "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce" (1999) 17 J Marshall J Computer & Info. L 723, 752. This legislation is now pre-empted by the US Federal Electronic Signatures in Global and National Commerce Act 2000 (usually known as 'E-Sign') which is not based on the X.509 model.

[100] 47 USC § 230.

[101] 23 Media L Rep 1794 (NY Sup Ct, May 25 1995) – see 4.2.3.1 above.

[102] The Senate conference report on § 230 states:

> 'This section provides "Good Samaritan" protections from civil liability for providers or users of an interactive computer service for actions to restrict or to enable restriction of access to objectionable online material. One of the specific purposes of this section is to overrule *Stratton-Oakmont v Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.' S Conf Rep No 104-230, at 435 (1996).

[103] 929 F Supp 824, 830–838 (ED Pa, 1996), *affirmed* 117 S Ct 2329 (1997).

[104] "Internet content" is defined in the Australian Broadcasting Services Act 1992, Sch 5, s 3 as information that:

> (a) is kept on a data storage device; and
>
> (b) is accessed, or available for access, using an Internet carriage service;
>
> but does not include:
>
> (c) ordinary electronic mail; or
>
> (d) information that is transmitted in the form of a broadcasting service.

This is prohibited content under s. 10 if it has been classified by the Australian Broadcasting Authority (ABA) as X or RC (refused classification), in essence films which depict sexual content in a way which is unsuitable for minors, or has been classified with an R classification (otherwise unsuitable for minors), if the material is made available other than by a "restricted access scheme", essentially a control method which restricts children from obtaining access such as filtering software.

[105] Australian Broadcasting Services Act 1992, Sch 5, s 11.

[106] Australian Broadcasting Services Act 1992, Sch 5, s 13.

[107] Australian Broadcasting Services Act 1992, Sch 5, ss 30–39, 82–3.

[108] Australian Broadcasting Services Act 1992, Sch 5, ss 40–51, 82–3.

[109] See e.g. the UK Information Commissioner's *Notification Handbook* pp. 12-14, <http://www.ico.gov.uk/upload/documents/library/data_protection/forms/notification_handbook_-_complete_guide.pdf>.

[110] Compare, for example, the Barclays Bank UK notification (available via <http://www.esd.informationcommissioner.gov.uk/esd/search.asp>) with the bank's privacy policy for personal customers at <http://www.barclays.com/privacy/per_info.html>. The former is a multi-page document containing uninformative terms of art; the latter is a single page which explains in clear language what the bank will do with the customer's data.

[111] There is even, in the longer term, the danger that those subject to the regulation will cease to recognise its normative effect – see Fuller, *The Morality of Law* (Yale University Press 1964) Chapter II.

[112] Case C-101/01 6 November 2003, OJ C7 10 January 2004 p. 3, discussed at part 3.1 above.

[113] See e.g. Baker, "Offshore IT Outsourcing and the 8th Data Protection Principle – legal and regulatory requirements with reference to financial services" (2006) 14 Int J L & Info Tech p. 1.

[114] [2001] EWHC 516 (Pat.) (High Court); [2001] EWCA Civ 1268 (CA); Case C-203/02 9th November 2004 (ECJ).

[115] See 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. 8.

[116] At least under the Directive and its national implementing legislation, though of course there might be residual liability under general principles of tort law in some jurisdictions.

[117] The actual standard under e-Signatures Directive art. 6 is that the certification-service-provider has a defence if he proves he did not act negligently; this is still a negligence standard, but with reversed burden of proof.

[118] See e.g. *Prendergast v. Sam & Dee Ltd* (1988) *The Times*, 24 March 1988.

[119] See e.g. *Independent School District No. 454, Fairmont, Minnesota v. Statistical Tabulating Corporation* 359 F Supp 1095 (ND Ill, 1973).

[120] See for UK law the principles set out in *Wilsons and Clyde Coal Ltd v English* [1938] AC 57.

[121] Certainly, at the time the Directive was proposed the main available technologies all envisaged that such a device would be in the possession of the user. This interpretation is supported by the original drafting of art. 1(3)(b) in the 1996 proposal, which defined e-money a being "(i) stored electronically on an electronic device such as a chip card or a computer memory" and (iii) generated in order to be put at the disposal of users to serve as an electronic surrogate for coins and banknotes" (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).

[122] See UK FSA, *Electronic Money: perimeter guidance* (February 2003). The methodology proposed for distinguishing between payment transactions (to be regulated by the FSA) and premium rate telephony services (to be regulated by Ofcom, the UK telecoms regulator) exhibits a remarkable lack of understanding of both the technology and the telecoms industry, together with some notable leaps of logic.

[123] Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market, COM(2005) 603 final, 1 December 2005. Payment service providers which fall under this regime will have no minimum funds requirement or restrictions on investment or non-financial business activities.

[124] *Zeran v America Online, Inc* 129 F 3d 327 (4th Cir, 1997), 1998 US 4047 (cert Denied).

[125] *Blumenthal v. Drudge and America Online Inc.* 992 F Supp. 44 (DDC 1998).

[126] *Doe v America Online Inc* 718 So 2d 385 (4th Cir, 1999).

[127] "While it appears to this Court that AOL in this case has taken advantage of all the benefits conferred by Congress in the Communications Decency Act, and then some, without accepting any of the burdens that Congress intended, the statutory language is clear: AOL is immune from suit …" *Blumenthal v. Drudge and America Online Inc.* 992 F Supp 44, 52 (DDC 1998).

[128] Defined in Australian Broadcasting Services Act 1992, Sch 5, s 4.

[129] A term originally used to describe British foreign policy in the mid-nineteenth Century, particularly in relation to Afghanistan – see Wyllie, "Masterful Inactivity", XII *Fortnightly Review* July-December 1869 p. 596 – but which has proved invaluable ever since to justify policy decisions not to act.

[130] Federal Reserve Bank Governor Kelly, "Developments in electronic money and banking", Cyberpayments '96 Conference, Dallas 1996

[131] See Chokhani & Ford, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* RFC 2527, March 1999, available from <http.www.ietf.org/rfc.html>, although the role of Registration Authorities is not fully articulated.

[132] See Biddle, "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace" (1997) 34 San Diego L. Rev. 1225, although Biddle does not separate the functions of Certification Authority and Registration Authority.

[133] PayPal was founded in 1998, and previous though unsuccessful attempts to commercialise accounted e-payments had been made - see e.g. First Virtual, which was founded in 1994 but ceased to provide e-payments in 1998, <http://computing-dictionary.thefreedictionary.com/First+Virtual>. Also in 1998 the distinction between stored value e-money and accounted e-payments was explained in ECB, *Report on Electronic Money* (August 1998) p.7 (using the term "access product).

[134] US home internet penetration had risen from 2% in 1994 to 26% in 1998 – National Science Foundation, *The Application and Implications of Information Technologies in the Home: Where Are the Data and What Do They Say?* (February 2001) p. 11, citing US Bureau of the Census data for 1998 and Clemente, *State of the Net: The New Frontier* (1998 McGraw-Hill, New York) for 1994. The possibility that accounted e-payments might eclipse stored value e-money was recognized in ECB, *Report on Electronic Money* (August 1998) p. 9: "However, it is possible that advances in the technology used for access products may reduce the comparative advantages of electronic money products and, consequently, their growth rate."

[135] See part 2 above.

[136] The closest to an explanation which can be found in recitals 56-60 of the Directive is in recital 59: "… particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards …", which suggests the second rather than the first.

[137] e-Signatures Directive art. 6.

[138] Databases Directive art. 7(1).

[139] Case C-203/02 9th November 2004.

[140] 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 contain any investment requirement to qualify for protection. 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, taking into account the exceptions to art. 2(1) set out in art. 8, the extraction was unfair. Making was not explained anywhere.

[141] See Black, "Enrolling Actors in Regulatory Systems: examples from UK financial services regulation" (2003) PL 6.

[142] See e.g. UK Financial Services & Markets Act 2000.

[143] See e.g. the UK FSA Handbook, <http://www.fsa.gov.uk/Pages/handbook/>, which is updated at least monthly.

[144] See e.g. the UK Banking Code, <http://www.bankingcode.org.uk/pdfdocs/BANKING%20CODE.pdf>.

[145] Thus in deciding whether a particular bank account term was unfair under Directive 93/13/EEC on unfair terms in consumer contracts (OJ L095 21 April 1993 p. 29), the UK courts would examine how far those terms complied with the Banking Code.

[146] Databases Directive recital 11.

[147] 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. 4.

[148] e-Signatures Directive recital 4.

[149] e-Money Directive recital 5.

[150] In Belgium, which appears to have the highest European level of e-money usage, 2.5 million users spent less than US$1.8 million daily, and the figures for Germany (US$0.2 million) and the Netherlands (US$0.65 million) are proportionately lower per user – BIS Committee on Payment and Settlement Systems, *Survey of developments in electronic money and internet and mobile payments* (March 2004) Table B p. 197 ff.

[151] See note 52.