LEGAL ISSUES ARISING ON THE ELECTRONIC HIGHWAY:
AN INTERNATIONAL SURVEY OF SIX AREAS

MINISTERIE VAN JUSTITIE
Wetenschappelijk Onderzoek- en Documentatiecentrum
's-Gravenhage

RE-97.14
December 1997

Jonathan Cave
Erik Frinking
Lisa van Dorp
Agnes Lotstra
Caroline Wagner
PREFACE

The Netherlands Ministry of Justice asked RAND Europe to conduct an international comparison of major legal problems and issues arising in the context of the electronic superhighway. This study was conducted between 15 March and 15 September 1997. The present document is the final report of that study; it describes legal problems and issues regarding the electronic highway in four countries: France, Germany, the United Kingdom, and the United States, in order to answer the following research questions for each of the surveyed countries:

1. What legal problems (regarding certain areas) have been experienced because of the electronic highway, and by whom?
2. If any initiatives have been taken or are being taken to address these problems, what are they and who has initiated them?
3. If the problems have been or are being resolved by legislation, what are its rationale, objective and main elements? If any legislative initiatives have been withdrawn, which and why?
4. What are considered to be the most important legal obstacles for the development of the information society?


This report should be of interest to persons interested in legal, economic, and policy aspects of the development of the electronic highway, especially as it pertains to issues of encryption, digital signatures, personal data, telecommunications, harmful and illegal content, and copyright.

RAND Europe, located in Delft, the Netherlands, is an independent unit of RAND and is chartered in The Hague as a Dutch foundation (Stichting). For more information about this report or about RAND Europe, contact may be made with the Director of RAND Europe, Dr. Richard Fallon, or with the project leader, Prof. Dr. Jonathan A.K. Cave.

Dr. Richard Fallon
RAND Europe
Landbergstraat 6
2628 CE Delft
The Netherlands
Tel: +31-15-278.54.11
Fax: +31-15-278.17.88
# TABLE OF CONTENTS

1. INTRODUCTION
   1.1. BACKGROUND .................................................................................. 1
   1.2. METHOD .......................................................................................... 2
   1.3. OUTLINE OF THE REPORT .............................................................. 2
   1.4. PERSPECTIVE .................................................................................. 3

2. ENCRYPTION
   2.1. INTRODUCTION ............................................................................... 5
   2.1.1. Note on WWW Resources .............................................................. 5
   2.1.2. Technical Background ................................................................. 7
   2.2. LEGAL ISSUES ................................................................................. 8
   2.2.1. Use of Encryption ....................................................................... 8
   2.2.2. Trade in Encryption Software ...................................................... 9
   2.2.3. Protection of Encrypted Information .......................................... 10
   2.2.4. Principled Positions .................................................................... 10
   2.3. COUNTRY SUMMARIES ................................................................. 11
   2.3.1. International Arrangements ........................................................... 11
   2.3.2. France ......................................................................................... 14
   2.3.3. Germany ..................................................................................... 16
   2.3.4. United Kingdom ......................................................................... 19
   2.3.5. United States ............................................................................... 21
   2.4. SUMMARY AND COMPARISON ...................................................... 27
   2.4.1. Issues Arising ............................................................................. 27
   2.4.2. Initiatives .................................................................................... 28
   2.4.3. Comparison ................................................................................. 30

3. DIGITAL SIGNATURES
   3.1. INTRODUCTION .............................................................................. 31
   3.1.1. The Use and Nature of Digital Signatures ...................................... 31
   3.2. LEGAL ISSUES SURROUNDING ELECTRONIC AND DIGITAL SIGNATURES 34
   3.2.1. Uses and Verification of Digital Signatures .................................... 34
   3.2.2. Liability of Certification Authorities ............................................ 35
   3.2.3. Legal Relationships in Certification ............................................. 36
   3.3. ARGUMENTS FOR AND AGAINST LEGISLATIVE RESOLUTION .......... 38
   3.4. COUNTRY SUMMARIES ................................................................. 39
   3.4.1. France ......................................................................................... 39
   3.4.2. Germany ..................................................................................... 40
   3.4.3. United Kingdom ......................................................................... 42
   3.4.4. United States ............................................................................... 45
   3.5. SUMMARY AND COMPARISON ...................................................... 49
   3.5.1. Issues Arising ............................................................................. 49
   3.5.2. Initiatives .................................................................................... 50
   3.5.3. Comparison ................................................................................. 52

4. PERSONAL DATA
   4.1. INTRODUCTION .............................................................................. 55
   4.1.1. Background ................................................................................ 55
   4.2. LEGAL ISSUES .............................................................................. 56
   4.2.1. Principles .................................................................................... 56
   4.2.2. Subject Rights ............................................................................ 56
   4.2.3. Other Issues ............................................................................... 57
   4.3. COUNTRY SUMMARIES ................................................................. 58
   4.3.1. EU Personal Data Protection Directive ......................................... 58
   4.3.2. France ......................................................................................... 60
   4.3.3. Germany ..................................................................................... 62
   4.3.4. United Kingdom ......................................................................... 64
   4.3.5. United States ............................................................................... 68
4.4. SUMMARY AND COMPARISON

4.4.1. Issues Arising

4.4.2. Initiatives

4.4.3. Comparison

5. TELECOMMUNICATIONS

5.1. INTRODUCTION

5.1.1. Background—General Issues

5.2. LEGAL ISSUES

5.2.1. Classification and Convergence

5.2.2. Universal Service

5.2.3. Treatment of Service Providers

5.3. COUNTRY SUMMARIES

5.3.1. European Union

5.3.2. France

5.3.3. Germany

5.3.4. United Kingdom

5.3.5. United States

5.4. SUMMARY AND COMPARISON

5.4.1. Issues Arising

5.4.2. Initiatives

5.4.3. Comparison

6. HARMFUL AND ILLEGAL CONTENT

6.1. INTRODUCTION

6.2. LEGAL ISSUES

6.2.1. Defamation

6.2.2. Other Intrinsically Harmful Content

6.2.3. Other Content-Based Issues

6.3. COUNTRY SUMMARIES

6.3.1. International

6.3.2. France

6.3.3. Germany

6.3.4. United Kingdom

6.3.5. United States

6.4. SUMMARY AND COMPARISON

6.4.1. Issues Arising

6.4.2. Initiatives

6.4.3. Comparison

7. COPYRIGHT

7.1. INTRODUCTION

7.2. LEGAL ISSUES

7.2.1. Protection of Works and People: Actors and Acts

7.2.2. Type of Rights Protected and Infringement to the Rights

7.3. COUNTRY SUMMARIES

7.3.1. Multinational Agreements

7.3.2. France

7.3.3. Germany

7.3.4. United Kingdom

7.3.5. United States

7.4. SUMMARY AND COMPARISON

7.4.1. Issues Arising

7.4.2. Initiatives

7.4.3. Comparison

8. IMPORTANT OBSTACLES TO DEVELOPMENT OF AN INFORMATION SOCIETY AND CONCLUDING REMARKS

8.1. INTRODUCTION

8.2. OBSTACLES

8.3. IS LEGISLATION NEEDED?

8.4. STEP TOWARDS THE INFORMATION SOCIETY
9. BIBLIOGRAPHY .................................................................................................................. 149
  9.1. WRITTEN MATERIALS ................................................................................................. 149
  9.2. ON-LINE SOURCES .................................................................................................. 164
      9.2.1. By Organisation Type ....................................................................................... 165
      9.2.2. By Topic ............................................................................................................. 169
10. PERSONAL CONTACTS ................................................................................................... 177
| **BBS** | (Bulletin Board System) A computerised meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. There are many thousands (millions?) of BBS's around the world, most are very small, running on a single IBM clone PC with 1 or 2 phone lines. Some are very large and the line between a BBS and a system like CompuServe gets crossed at some point, but it is not clearly drawn. |
| **Binary** | Meaning two. The principle behind digital computers. All input to the computer is converted into binary numbers made up of the two digits 0 and 1 (bits). |
| **Cache memory** | A buffer, smaller and faster than main storage, used to hold a copy of instructions and data in main storage that are likely to be needed next by the processor and that have been obtained automatically from main storage. |
| **Certification Authority** | Trusted agent that issues digital certificates to principals. Certification authorities may themselves have a certificate that is issued to them by other certification authorities. The highest certification authority is called the root CA. |
| **Certification:** | The comprehensive evaluation of the technical and non-technical security features of an AIS [automated information system] and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. |
| **Common carrier** | In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. |
| **Cookie** | A set of data that provides a connection between transactions. |
| **Cookie file** | A file that contains information (cookies) created by Web sites that is stored on the user's hard disk. It provides a way for the Web server to keep track of a user's patterns and preferences and, with the co-operation of the Web browser, to store them on the user's own hard disk in the COOKIES.TXT file. The cookies contain a range of URLs (addresses) for which they are valid. When the browser encounters those URLs again, it sends those specific cookies to the Web server. |
| **Cryptography** | The conversion of data into a secret code for transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext. The encryption algorithm uses a key, which is a binary number that is typically from 40 to 128 bits in length. The data is "locked" for sending by combining the bits in the key mathematically with the data bits. At the receiving end, the key is used to "unlock" the code, restoring it to its original binary form. |
| **Digital certificate** | The digital equivalent to an ID card in the RSA public key encryption system. Also called digital IDs, digital certificates are issued by certification organisations such as VeriSign, Inc., Mountain View, CA, after verifying that a public key belongs to a certain owner. The certification process varies depending on the certification authority (CA) that issues the certificates and the level of certification. Drivers licenses, notarisation and fingerprints are examples of documentation used to authenticate the user. The digital certificate is actually the owner's public key that has been digitally signed by the certification authority (CA). The digital certificate is sent along with an encrypted message to verify that the sender is truly the entity identifying itself in the transmission. The recipient uses the public key of the CA, which is widely publicised, to decrypt the sender's public key attached to the message. Then the sender's public key is used to decrypt the actual message. |

<p>| <strong>Digital signature</strong> | An electronic signature that cannot be forged. It is a computed digest of the text that is encrypted and sent with the text message. The recipient decrypts the signature and recompiles the digest from the received text. If the digests match, the message is authenticated and proved intact from the sender. |
| <strong>DNS</strong> | Domain Name System (DNS): The online distributed database system that (a) is used to map human-readable addresses into Internet Protocol (IP) addresses, (b) has servers throughout the Internet to implement hierarchical addressing that allows a site administrator to assign machine names and addresses, (c) supports separate mappings between mail destinations and IP addresses, and (d) uses domain names that (i) consist of a sequence of names, i.e., labels, separated by periods, i.e., dots, (ii) usually are used to name Internet host computers uniquely, (iii) are hierarchical, and (iv) are processed from right to left |
| <strong>Electronic commerce</strong> | Doing business online. It includes purchasing products via online services and the Internet as well as electronic data interchange (EDI), in which one company’s computer queries and transmits purchase orders to another company’s computer. |
| <strong>Email address</strong> | The domain-based or UUCP address that is used to send electronic mail to a specified destination. |
| <strong>Encryption</strong> | Encryption is the manipulation of a packet’s data in order to prevent any but the intended recipient from reading that data. There are many types of data encryption, and they are the basis of network security. |
| <strong>FTP</strong> | (File Transfer Protocol) A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). It includes functions to log onto the network, list directories and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. Unlike e-mail programs in which graphics and program files have to be “attached,” FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data. |
| <strong>FTP site</strong> | A computer system on the Internet that maintains files for downloading. |
| <strong>Header</strong> | The portion of a packet, preceding the actual data, containing source and destination addresses, and error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time. |
| <strong>Home page</strong> | The first page retrieved when accessing a Web site. It serves as a table of contents to the rest of the pages on the site or to other Web sites. |
| <strong>HTTP</strong> | (HyperText Transport Protocol) The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser. |
| <strong>Interconnection</strong> | 1. The linking together of interoperable systems. 2. The linkage used to join two or more communications units, such as systems, networks, links, nodes, equipment, circuits, and devices. |
| <strong>Internet service provider</strong> | An organisation that provides access to the Internet. Small Internet service providers (ISPs) provide service via modem and ISDN while the larger ones also offer private line hook-ups (T1, fractional T1, etc.). Customers are generally billed a fixed rate per month, but other charges may apply. For a fee, a Web site can be created and maintained on the ISP’s server, allowing the smaller organisation to have a presence on the Web with its own domain name. |
| <strong>IP</strong> | (1) (Internet Protocol) The IP part of the TCP/IP communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or sub-network. TCP provides the transport layer (layer 4), which ensures complete delivery of the entire message or file. |
| <strong>IP address</strong> | (Internet Protocol address) The physical address of a computer attached to a TCP/IP network. Every client and server station must have a unique IP address. Client workstations have either a permanent address or one that is dynamically assigned for each dial-up session (see DNS). IP addresses are written as four sets of numbers separated by periods; for example, 204.171.64.2. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network operating system (NOS)</td>
<td>Software that (a) controls a network and its message (e.g., packet) traffic, and queues, (b) controls access by multiple users to network resources such as files, and (c) provides for certain administrative functions, including security</td>
</tr>
<tr>
<td>Newsgroup</td>
<td>A discussion group on the Internet. It is an on-going collection of messages about a particular subject.</td>
</tr>
<tr>
<td>PGP</td>
<td>(Pretty Good Privacy) Public key cryptography software from Pretty Good Privacy, Inc., San Mateo, CA, (<a href="http://www.pgp.com">www.pgp.com</a>). It was developed by Phil Zimmermann, founder of the company, and it is based on the RSA cryptographic method.</td>
</tr>
<tr>
<td>Server</td>
<td>A computer in a network shared by multiple users. The term may refer to both the hardware and software or just the software that performs the service.</td>
</tr>
<tr>
<td>Spam</td>
<td>Sending copies of the same message to large numbers of newsgroups or users on the Internet. People spam the Internet to advertise products as well as to broadcast some political or social commentary.</td>
</tr>
<tr>
<td>TTP</td>
<td>The trusted third party shares a secret (password) with each principal. It uses a key derived from the password to issue tickets to these principals.</td>
</tr>
<tr>
<td>Universal service</td>
<td>The concept of making basic local telephone service (and, in some cases, certain other telecommunications and information services) available at an affordable price to all people within a country or specified jurisdictional area.</td>
</tr>
<tr>
<td>URL</td>
<td>(Uniform Resource Locator) The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages. The URL contains the protocol prefix, port address, domain name, subdirectory names and file name. Port addresses are generally defaults and are rarely specified. To access a home page on a Web site, only the protocol and domain name are required.</td>
</tr>
<tr>
<td>Usenet</td>
<td>(USEr NETwork) A public access network on the Internet that provides user news and e-mail. It is a giant, dispersed bulletin board that is maintained by volunteers who provide news and mail feeds to other nodes. All the news that travels over the Internet is called NetNews, and a newsgroup is a running collection of messages about a particular subject. Usenet began in 1979 as a bulletin board between two universities in North Carolina. Today, there are some 10,000 newsgroups. News can be read with a Web browser or via newsreaders such as nn, rn, trn and tin.</td>
</tr>
<tr>
<td>Web site</td>
<td>A server that contains Web pages and other files which is online to the Internet 24 hours a day.</td>
</tr>
<tr>
<td>World wide web</td>
<td>An Internet facility that links documents locally and remotely. The Web document is called a Web page, and links in the page let users jump from page to page (hypertext) whether the pages are stored on the same server or on servers around the world.</td>
</tr>
</tbody>
</table>
1. INTRODUCTION

1.1. BACKGROUND

Technological developments, particularly those occurring on the "electronic superhighway," are affecting social, personal, academic and business interactions throughout the world. These increasing and increasingly effective contacts between far-flung individuals place severe strains on the mechanisms and institutions they have devised to protect their mutual interests. Almost every nation has been affected by these developments, but no nation can respond to the resulting problems in a vacuum; the responses of other individual nations and multinational initiatives (whether \textit{ad hoc} or through supranational organisations) need to be considered. Cross-border interactions and the complexity of information and communication technologies can only be effectively understood and dealt with if developments are seen from a transnational point of view.

Discussions and initiatives in other nations can provide useful background for the discussion of parallel issues and the framing of national legislation. New or modified legislation, conscious decision to await further developments, work towards a supranational solution or simple reliance on self-regulation can draw on these experiences. Of course, different nations may experience problems in different ways and at different times, as a combined result of different pace and direction of technological developments or uptake, evolution of service infrastructure, and the pre-existing nature of the formal and informal legal system. This is particularly true for areas in which policy and legal problems are combined.

The Netherlands Ministry of Justice asked RAND Europe to conduct an international comparison of major legal problems and issues arising in the context of the electronic superhighway. This study was conducted between 15 March and 1 September 1997. The present document is the final report of that study; it describes legal problems and issues regarding the electronic highway in four countries: France, Germany, the United Kingdom, and the United States, in order to answer the following research questions for each of the surveyed countries:

1. What legal problems (regarding certain areas) have been experienced because of the electronic highway, and by whom?
2. If any initiatives have been taken or are being taken to address these problems, what are they and who has initiated them?
3. If the problems have been or are being resolved by legislation, what are its rationale, objective and main elements? If any legislative initiatives have been withdrawn, which and why?
4. What are considered to be the most important legal obstacles for the development of the information society?

This report seeks to answer these questions by giving an assessment of the current situation in the surveyed countries in terms of the electronic superhighway. Such aspects as particular legal strategies, the drafting of specific provisions, scope of legislative proposals and even the way the issue is perceived necessarily relate to deeper differences between these nations. It is beyond the scope of this report to summarise or analyse these broader legal, social and economic differences. The report provides information on the way the issues are discussed and the steps taken to address them, but should not be seen as a normative evaluation or explanation of those initiatives. To make the best use of the results, they should be seen as:
a set of possibly different perspectives on a set of electronic superhighway issues and their interaction;

• a comparative description of the 'state of play' in different countries whose experiences may prove influential in a supranational context; and

• a source of ideas for initiatives and approaches that may be worth considering, together with pointers to the ongoing 'natural experiments' being conducted in the surveyed nations.

1.2. METHOD

In order to develop answers to these questions, we began by identifying, collecting and reviewing data on many different legal initiatives pertaining to the Internet and, in a broader sense, to the electronic highway. We used peer-reviewed, journalistic and on-line written sources as well as interviews and discussions with government officials, legal academic experts, and people working in Internet-related business (see Appendix for references). This exercise produced an extensive inventory of laws, regulations, law proposals and policy papers. From this inventory were developed ten subject areas, which can be viewed as coherent fields likely to be controlled by a single body of law or at least by laws closely related to each other. At the same time, they might be issues for national and international discussion.

Grouping possible legal initiatives by subject areas facilitates comparison, assists in highlighting specific national approaches to perceived problems, and helps to focus the overall assessment. The subject areas selected for further investigation were:

• Encryption
• Digital Signatures
• Personal Data
• Telecommunications Infrastructure and Broadcasting
• Harmful and Illegal Content
• Intellectual Property Rights
• Contract
• Antitrust
• Tax
• Computer Crime.

After an initial investigation of the legal issues in each of the subject areas, it was agreed to focus the remainder of the research on and answer research questions 2 and 3 for six subject areas. These are the first six of the list of subject areas above. This refinement was necessitated by the enormous wealth of available information and the need for a well-structured and deliberated approach. Together, these six areas were perceived as involving some of the most important issues and the most interesting legal initiatives across the surveyed countries. Question 4 frames a summary of the investigation.

1.3. OUTLINE OF THE REPORT

Chapters 2 through 7 answer research questions 1, 2 and 3 by providing a discussion of specific legal issues occurring in each of the six major subject areas. Each chapter starts with an introductory section, containing a brief general introduction to the area, any technical background necessary to understanding of the legal issues, and a more detailed discussion of the issues in terms not specific to
particular countries. In view of the complexity and global scope of the issues, these discussions are sometimes quite substantial. This is followed by a survey of developments, initiatives and laws in each country surveyed. Where overarching international agreements or position papers contribute to or affect the discussions, they are referenced at the beginning of the country surveys. To the greatest extent possible, the country reports follow a parallel structure in order to facilitate comparisons. They conclude with a brief summary of the situation in that country if the presented material requires this. The chapter itself concludes with a comparative summary across the countries, together with an indicative table based on the material in the country reports.

Chapter 8 answers research question 4 by integrating the information provided in the earlier chapters. It provides a list of what we perceived to be “the most important legal obstacles to the developments of an information society”, thus addressing the last research question. We should stress that this is our perception, based on the materials we have reviewed and the interviews and discussions in which we have participated. It does not represent either the results of a scientific survey or the consensus judgement of authorities. In our view, this would be difficult to achieve and of dubious value.

1.4. PERSPECTIVE

We conclude this introductory chapter with some remarks on the perspective taken in performing this study, in order to place our research in its appropriate context. It is our objective to have the material in this report considered of value to legal, economic and policy analysts. From the outset, we concentrated on issues arising on the electronic highway. This is a rapidly-expanding and inherently international arena for human interaction; moreover, it is one where people with varying disciplinary perspectives and policy interests vie to be heard on matters of law, policy and practice. It is characterised by an uneven development, as different countries proceed at different paces in divergent directions, driven both by their own particular legal, social and economic structures and by international developments. In order to understand legal issues, we must understand the technological, economic and social developments that frame these issues. These observations and their resulting perspective have certain specific implications.

It is premature to regard any major issue as concluded. New developments are occurring all the time, and issues which have been quiescent in one nation may awaken (often in different forms) as a result of developments in other national or multinational spheres.

Our analysis touches on relatively small parts of large areas of law. Our conclusions should not be used outside the context of the Internet and the electronic highway.

Our analysis deals only with the surface of legal issues. The careful description, weighing and reconciliation of competing arguments that can be found in judicial opinions is rarely present in either public or political debate over pending legislation, making it difficult to infer the underlying arguments. A full legal investigation of any of the subject areas covered in this report was beyond the constraints posed by the time and budget for this study.

Our analysis is of the legal issues in their economic, policy and technological context. Even the most legal of issues must sometimes be approached from a political, policy or (increasingly) economic perspective; it is necessary to take those perspectives seriously, if only because they address the reasons why legislation is developed and the reactions of private parties to changes in law.

The report addresses the differences in perspectives across all the countries surveyed. Different weights are attached to legal, economic, and policy perspectives in the different countries we surveyed. However, it is important to note that because many of the technological advances and uses pertaining to the Internet first surfaced in the United States, we found a broader set of material on the
issues under study originating from that country. Nevertheless, many of these issues, as our survey shows, have arisen across all the countries. This report strives to depict each country’s approach to these complicated set of issues in order to help the Netherlands draw lessons from the range of experiences and perspectives.
2. ENCRYPTION

2.1. INTRODUCTION

More than other means of communication, electronic message traffic is notoriously vulnerable to interception and forgery. These problems may be addressed by encryption: the transformation of electronic messages and documents in ways that make them inaccessible to persons not in possession of a decryption "key." In the electronic communications world, the term refers to the hardware and software techniques used to pass between the original text and the encrypted message. Recent developments have brought virtually unbreakable encryption within easy reach of vast numbers of people. Encryption is used in many contexts and for many purposes.

The transformation (in either direction) between open text and some form of confidential code can have a number of overlapping purposes. In this report, we have divided these two purposes into two general classes: (1) those having to do with maintaining confidentiality of materials transmitted via the electronic highway and (2) those having to do with verifying the authenticity of senders and text. In this chapter, our focus is on the first of those purposes, while in the next chapter on digital signatures, we focus on the second.

Our research identified three aspects of encryption as particular subjects for policy debate and legal investigation: use of encryption; trade (international import and export) in encryption products; and legal treatment of encrypted information.

The following part of this introduction gives a short technical background. Without some understanding of the technological and organisational basis for encryption, the legal and policy issues, discussed below in general terms, cannot be grasped. Readers already well-acquainted with modern encryption may wish to skip to the next section, in which the legal issues and the principled positions in the emerging debate are described. Following these introductory materials, we will present the country-by-country descriptions, organised by the three aspects of encryption given in the paragraph above.

2.1.1. Note on WWW Resources

The related areas of encryption and privacy are extensively documented in both published and on-line materials. In preparing this section, we drew extensively on the contents of various on-line archives of cryptography policy, technology and legislative materials. The bibliography of this report contains a collection of electronic materials used in the study as a whole. In view of the extensive use made of on-line materials in preparing this section, we feel it advisable to highlight the main resources. They are listed in Table 2.1 below, and a more detailed listing is provided in Section 9.2.2.8. Readers are urged to consult these sites for up-to-date information. Many of these sites contained written interpretations or summary materials as well as links to other resources. Due to the extensive overlap between the sites, it is difficult to identify single sources for each piece of information. However, a few sites were particularly influential—these include Koops' "Crypto Law Survey" site, Akdeniz' "Cyber-Rights and Cyber-Liberties" site, the "lambda" newsletter, the Electronic Frontier Foundation, and

---

3 http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm
4 http://www.leeds.ac.uk/law/pgs/yaman
5 http://www.freenix.fr/netizen/212-e.html
6 http://www.eff.org
the Electronic Privacy Information Center. The organisation and substance of the following material is largely based on material in those sites, though the sites' authors bear no responsibility for any misstatements, errors or omissions.

Table 2.1. Selected On-line Encryption Resources

<table>
<thead>
<tr>
<th>Country</th>
<th>Site</th>
<th>Site URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finland</td>
<td>European Cryptography Resources</td>
<td><a href="http://www.modeemi.cs.tut.fi/~avs/eu-crypto.html">http://www.modeemi.cs.tut.fi/~avs/eu-crypto.html</a></td>
</tr>
<tr>
<td>France</td>
<td>Data Encryption and the Law(s)</td>
<td><a href="http://web.cnam.fr/Network/Crypto/survey.html">http://web.cnam.fr/Network/Crypto/survey.html</a></td>
</tr>
<tr>
<td>France</td>
<td>lambda 2.12 - Crypto : French TTPs</td>
<td><a href="http://www.freenix.fr/netizen/212-e.html">http://www.freenix.fr/netizen/212-e.html</a></td>
</tr>
<tr>
<td>France</td>
<td>Spécial chiffrement - Crypto Archives</td>
<td><a href="http://www.freenix.fr/netizen">http://www.freenix.fr/netizen</a></td>
</tr>
<tr>
<td>Germany</td>
<td>Aktuelles zur Kryptokontroverse</td>
<td><a href="http://www.provet.org/kk/kkindex.htm">http://www.provet.org/kk/kkindex.htm</a></td>
</tr>
<tr>
<td>Germany</td>
<td>German Cryptography law &amp; policy</td>
<td><a href="http://www.thur.de/ulf/krypto/verbot.html">http://www.thur.de/ulf/krypto/verbot.html</a></td>
</tr>
<tr>
<td>Germany</td>
<td>Public Key Infrastructure (PKI) links</td>
<td><a href="http://www.pca.dfn.de/eng/team/ske/pem-dok.html#CA">http://www.pca.dfn.de/eng/team/ske/pem-dok.html#CA</a></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Anonymity: Index</td>
<td><a href="http://www.stack.nl/~galactus/remailers/index-anon.html">http://www.stack.nl/~galactus/remailers/index-anon.html</a></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Crypto Law Survey</td>
<td><a href="http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm">http://cwis.kub.nl/~frw/people/koops/lawsurvey.htm</a></td>
</tr>
<tr>
<td>UK</td>
<td>Cyber Rights and Cyber Liberties</td>
<td><a href="http://www.leeds.ac.uk/law/pgs/yaman">http://www.leeds.ac.uk/law/pgs/yaman</a></td>
</tr>
<tr>
<td>UK</td>
<td>UKERNA Secure Email Project</td>
<td><a href="http://tech.ukerna.ac.uk/secemail/">http://tech.ukerna.ac.uk/secemail/</a></td>
</tr>
<tr>
<td>UK</td>
<td>University of Exeter UK Export Controls &amp; GAK Crypto Politics</td>
<td><a href="http://www.dcs.ex.ac.uk/~aba/ukcrypto">http://www.dcs.ex.ac.uk/~aba/ukcrypto</a></td>
</tr>
<tr>
<td>USA</td>
<td>Center for Democracy and Technology Crypto Page</td>
<td><a href="http://www.cdt.org/crypto.html">http://www.cdt.org/crypto.html</a></td>
</tr>
<tr>
<td>USA</td>
<td>Crypto.com home page</td>
<td><a href="http://www.crypto.com/">http://www.crypto.com/</a></td>
</tr>
<tr>
<td>USA</td>
<td>Electronic Frontier Foundation</td>
<td><a href="http://www.eff.org">http://www.eff.org</a></td>
</tr>
<tr>
<td>USA</td>
<td>Electronic Privacy Information Center</td>
<td><a href="http://www.epic.org/crypto/">http://www.epic.org/crypto/</a></td>
</tr>
<tr>
<td>USA</td>
<td>Internet Privacy Coalition</td>
<td><a href="http://www.privacy.org/ipc">http://www.privacy.org/ipc</a></td>
</tr>
<tr>
<td>USA</td>
<td>Northern Illinois University Crop</td>
<td><a href="http://sun.soci.niu.edu/~crypt/">http://sun.soci.niu.edu/~crypt/</a></td>
</tr>
<tr>
<td>USA</td>
<td>Newsletter</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>PERKINS COIE:</td>
<td><a href="http://www.perkinsoic.com/resource/ecom/crypto/crypto.htm">http://www.perkinsoic.com/resource/ecom/crypto/crypto.htm</a></td>
</tr>
<tr>
<td>USA</td>
<td>Encryption/Cryptography</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>PGP Software</td>
<td><a href="http://www.pgp.com">http://www.pgp.com</a></td>
</tr>
<tr>
<td>USA</td>
<td>Privacy, International</td>
<td><a href="http://www.privacy.org/pi">http://www.privacy.org/pi</a></td>
</tr>
<tr>
<td>USA</td>
<td>SOFTWAR Information Security</td>
<td><a href="http://www.us.net/softwar/">http://www.us.net/softwar/</a></td>
</tr>
</tbody>
</table>

7 http://www.epic.org/crypto
8 Most sites contain material for more than one nation.
2.1.2. Technical Background

Encryption\(^9\) is a means of putting data or messages (called "plaintext") into a form that cannot be understood without additional, secret information. This is accomplished by applying a mathematical algorithm that combines the plaintext with a user-selected "key." Decryption is accomplished via the same algorithm. Many of the perceived problems with encryption reflect the development of "strong" encryption systems. The length of the "key" used to encrypt the message determines the difficulty of decryption; strong encryption systems use long keys that are unbreakable to all intents and purposes.

Encryption algorithms can use secret or public keys. A secret key system uses the same key for encoding and decoding. Providing the key is kept secret, this can provide good security and rapid encryption and decryption. The main drawback is that the sender and the recipient must agree on and share the key. This is clearly impossible between strangers. In a "public key" system different keys are used for encoding and decoding the same message - individuals publish one key, retaining the other key as private information. In such a system messages encrypted with a public key can only be decoded with the corresponding private key; conversely, messages encrypted with the private key can be decoded by anyone using the corresponding public key, proving that the message originated with the holder of the private key. In practical terms, a user publishes his public key so that anyone can use it to send a message that only he can read.

More subtly, individuals can use public key systems to verify both ends of a communication and the authenticity and integrity of the message with the same system. If A sends B a message encrypted with both A's private key and B's public key:

- B's private key is required for decryption, so B (and only B) can read it;
- A's public key is also required to decrypt the message, so B knows that it could only have come from A, and further that it has not been altered.

This clearly facilitates secure person-to-person communication between strangers, including protection against later repudiation. It can also be used to provide selective anonymity. This is not a panacea, since it is still necessary to establish legal connections between public keys and their owners. This can be accomplished by the use of certification authorities (CAs). These are a special type of trusted third party (TTP) that maintains a list of individuals' public keys. We should note that these developments are not specific to the electronic highway.

Another technical development critically connected to the electronic highway is the emergence of applications software with integral encryption capabilities. Encryption and decryption are cumbersome matters, and would not be used in ordinary commerce without a compelling reason. New software products bring encryption within reach of everyone and allow them to do those things (electronic commerce, for example) that they would not do without the security that encryption offers.

To enhance the utility of encryption to the private parties and preserve legitimate access by the government, a process called "key escrow" can be established whereby a third party (possibly a certification authority or government agency) holds all private keys, supplying them to their owners in case of loss or destruction. If the government\(^{10}\) can obtain the key from the escrow agent, the system is referred to as a "key recovery" system - this is more intrusive than a system where law enforcement agents can only require the agent to decrypt specific messages. Encryption applications also exert their force in other areas specifically treated in this document:\(^{11}\)

---

\(^9\) For a comprehensive discussion of encryption technology and its impacts, see Froomkin, M. *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow",* 1996 U. Chi. L. Forum 15

\(^{10}\) Or other parties with legitimate claims, like employers, spouses, etc.

\(^{11}\) In particular, in a commercial, consumer or contractual context cryptographic keys, electronic cash, digital signatures and digital certificates may need to be issued, validated, retained and/or redeemed by a third
2.2. LEGAL ISSUES

We discuss here three aspects of encryption: use of encryption; restrictions on the trade in encryption software; and legal treatment of encrypted information. The discussions are intended to lay out the main legal issues and the positions that have been taken with regard to them. Few of the issues are settled, but we do indicate major developments in actual or proposed legislation and related legal decisions.

2.2.1. Use of Encryption

The vague and uncertain nature of legal initiatives, the rapid evolution of encryption technology and practice and the unresolved state of many of the fundamental issues combine to make much of the public discussion fairly "generic." To facilitate an understanding of this discussion and the major pro- and anti-encryption restriction positions, we will first indicate how encryption and encryption techniques are used in a variety of activities. Individuals use encryption in order to:

- Establish their identity (see the discussion of digital signatures);
- Conceal their identity;
- Authenticate and ensure the integrity of documents (again, see the discussion of digital signatures);
- Control access to electronic documents and their contents (i.e. ensure confidentiality); and
- Conceal electronically-arranged or recorded activities from authorities.

These purposes may be loosely divided among electronic commerce, public speech, private speech and crime. The bulk of the legal issues stem from the fact that the same technology and activities support all of these activities, making it hard to establish "bright-line" standards for permitted conduct. Indeed, prohibitions are justified in terms of the content rather than the form of messages and encryption renders this content immune to scrutiny. More specifically, the legal issues derive from the policy issues, since encryption is primarily a means to an end rather than an end in itself.

The use restrictions that have been suggested include: prohibitions on the use of all encryption; limits on key length; limits on the type of use to which encryption may be devoted (identity is OK, confidentiality is not); limits on specific encryption products or algorithms; requirements that individuals store their private keys (key escrow), make them available to officials on production of a warrant (key recovery), or allow officials access to plaintext of specific documents. These are accompanied by different degrees of compulsion. Current legislation and proposals tend to conflate different uses of encryption in an attempt to marry two essentially disparate goals: provision of a secure communications infrastructure (primarily for commercial reasons); and preservation of legitimate government access.

Public key encryption systems provide integrated identification, authentication and confidentiality - these functions are difficult to separate in practical terms, though the parties need to establish that keys "belong" to the expected people. If they cannot exchange keys in person, it may be necessary to ensure that public keys are "certified" by a third party known to and trusted by both.

---

12 Third-party provision of identification and authentication services is treated under the digital signature/certification authority discussion in the following chapter.

13 The need of private individuals for secure or anonymous communication is rarely mentioned in official rationale for proposed use restrictions.

14 See page 8 supra.
For their part, governments need access to the contents of certain encrypted messages. The most powerful way is to obtain the senders' private keys - for this, they need key recovery agents or some other means of compelling disclosure of private keys. Alternatively, governments can seek to compel use of specific encryption products offering a government "trapdoor," to ensure access to the plaintext of specific encrypted messages, or to prevent the use of encryption.

The functions of commercial security and government access are very different. The former principally involves identification and authentication, while the latter is mainly concerned with confidentiality\textsuperscript{15}. Proposed legislation systematically attempts to connect them.

Few private parties are persuaded by this connection; this accounts for the generally hostile reception accorded key recovery proposals and the frequent changes to which they have been subject. In broad overview, private parties assert that:

- Third-party providers of encryption services \textit{may} be unnecessary for business (or personal) communication;
- There is no basis for compelling the use of specific organisations or products;
- Use of certification authorities can create significant additional risk, not least as they are likely targets for criminals who might benefit from fraudulent key certification;
- This risk is magnified in the case of key escrow agents;
- Compulsory key escrow is practically unenforceable - at best, individuals might have to resort to additional levels of encryption;
- Absent compulsion, criminals would certainly avoid using escrow agents.

The conclusion of these assertions is that regulations seeking to serve both functions may reduce the security of private transactions without improving legitimate law enforcement access.

We are thus led to separate discussions of encryption used for confidentiality from encryption used for authentication or identification. This chapter deals with the former, while the next chapter deals with the latter. We further note that some current proposals attempt to distinguish the use of encryption from the provision of encryption services. This distinction is not highly regarded in the public debate\textsuperscript{16}. We therefore interpret use of encryption broadly to include provision of encryption services.

\subsection{2.2.2. Trade in Encryption Software}

Export restrictions are typically based on national security arguments, and opposed on the grounds of economic impact and unenforceability. Exports of specific encryption products to a limited set of countries deemed to support terrorism are restricted by various international agreements\textsuperscript{17}. Some countries have attempted to go beyond this. Such extended export controls are intended\textsuperscript{18} to serve two

\footnotesize{\textsuperscript{15} This is somewhat broad - there is certainly a commercial need for confidentiality, and the same infrastructure that supports secure commercial transactions may also be useful for ordinary communications that may benefit from confidentiality or even anonymity. On the other hand, simple access to plaintext without a solid link to the parties or a guarantee of integrity may be more helpful to investigation of wrongdoing than to prosecution.}


\footnotesize{\textsuperscript{17} e.g. COCOM and Wassenaar agreements and the EU Convention on Exports of Dual-Use Goods. For more details on international agreements, see section 0 and the Crypto Law Survey (footnote 3), EPIC (footnote 7), and EFF (footnote 6) archives.}

\footnotesize{\textsuperscript{18} cf. S. Baker, \textit{Decoding the OECD's Guidelines for Cryptography Policy}, \textit{International Lawyer}.}
functions. First, they are intended to discourage widespread foreign use of strong encryption, helping national security and the investigation of international crimes. Second, they are aimed at encouraging an international key recovery infrastructure standardised around encryption products that preserve government access. The first of these presupposes a dominant technical position on the part of the nation concerned. The second depends on international support and co-operation. Recent events (see discussion of the US in section 0 infra) have weakened these arguments for export controls.

Import controls have also been implemented, primarily in countries that have domestic controls on the use of strong encryption or those who wish to promote international standardisation on specific domestic products.

2.2.3. Protection of Encrypted Information

This is almost exclusively an area of UK and US concern, though the central issue is possibly of wider applicability. This issue is compulsory disclosure of decryption keys. The heart of the matter is that individuals have certain protections in terms of what they can be compelled to disclose in court. These protections were largely put in place before encryption was possible. Like silence in response to a question, the use of encryption may suggest that one has something to hide. Different societies will have to decide whether to reserve this freedom to the individual, comment on the suspicion it raises or compel revelation. The details are highly specific to the countries involved.

2.2.4. Principled Positions

The legal issues have evolved with the policy responses. In broad terms, most governments take the position that principles of free speech, privacy, economic interest combined with practical law enforcement difficulties prevent much interference with the use of encryption under ordinary circumstances. Third-party providers can, in principle, be regulated, and even compelled to co-operate with law enforcement enquiries (through grants of access to plaintext or decryption keys). National security concerns are used to justify restrictions on trade in strong encryption. Finally, the use of encrypted material in legal proceedings raises certain special issues that are only now beginning to be addressed.

The groups who most object to regulation of encryption use are businesses, network operators and citizen privacy rights organisations. They raise concerns that reflect the different uses of encryption and the different manifestations of encryption techniques.

Business parties maintain that encryption is an essential part of conducting business (electronic commerce over the Internet) as it protects

- the transmission of computerised data from third parties (security aspect);
- the authenticity and integrity of electronic communications; and
- the confidentiality of electronic documents in telecommunications.

Some of these functions (integrity, identification) are discussed under digital signatures. Others concern encryption per se. It is often claimed that transaction security and business confidentiality need technical protection in this area, because the legal safeguards available in non-electronic communication (e.g. protection of trade secrets) are unenforceable on the Internet. Pragmatic arguments are also advanced. A legal compulsion to use weaker forms of encryption places businesses at a competitive disadvantage with respect to foreign competitors with whom they are in head-to-head competition over the Internet. In addition, limits on encryption use create substantial contractual risk

that may, moreover, be difficult to mitigate or allocate efficiently\(^{19}\). Other alternatives (password-protection, mandatory use of licensed certification authorities, etc.) lack some capabilities of "decentralised" strong encryption and impose costs and delays. Finally, pragmatic law enforcement difficulties may produce inappropriate liability assignment.

For their part, network operators regard encryption as an essential tool for protecting both the security of their systems and the personal data they contain.

Citizen groups maintain that encryption can guarantee private communication in much the same fashion as postal confidentiality measures. In addition, they argue the importance of anonymous public speech and the protection from self-incrimination. Finally, they point out that encryption provides private parties with hedges against both government censorship and overweening collection of personally identifiable data.

For all these parties, the difficulties of applying or enforcing encryption restrictions are a source of considerable legal uncertainty.

Those who favour regulating encryption are primarily concerned with the fact that the same encryption which prevents illicit access also prevents licit access. They place particular emphasis on the informational needs of criminal enforcement agencies. Routine surveillance\(^{20}\), investigation, evidence-gathering and prosecution are all hampered by encryption. Initially, encryption policies were both justified and shaped by references to specific acts supposed to occur under its shelter. Crimes involving harmful or illegal content (especially pornography), illegal transactions (especially money-laundering) and acts of conspiracy to commit other crimes (especially drug trafficking, terrorism and hate crimes) were lumped together to justify restraints on the use of encryption, demands for access to encrypted messages, and or key recovery. Slowly -as the initiatives fail to be enacted, prove unenforceable or impose undue burdens on legitimate uses - this emphasis is being replaced by approaches focused on specific acts or strategies. Beyond legal restrictions on the traffic in and use of encryption, these policies include moves to encourage an accessible third-party encryption infrastructure, exploitation of market forces to spread encryption techniques that provide government access, and development of legal rules and doctrines regarding the treatment of encrypted material in court. Even nations that have had little activity to date are contemplating restrictions.

2.3. COUNTRY SUMMARIES

In this section, we will discuss the three aspects of use of encryption, trade in encryption products and legal treatment of encrypted information in the four countries surveyed. Before passing on to consideration of individual countries, we will describe international arrangements, which touch on all three of these aspects.

2.3.1. International Arrangements\(^{21}\)

Various international arrangements have restricted exports of specific encryption products (broadly defined) to specific "pariah" destinations. The CoCom (Co-ordinating Committee for Multilateral Export Controls, dissolved in March 1994) organisation maintained an International Industrial List and an International Munitions List. After 1991, they allowed trade in public-domain and

\(^{19}\) Some have gone so far as to suggest that encryption restrictions might limit the ability of software manufacturers and electronic publishers to protect their intellectual property rights.

\(^{20}\) As implemented by e.g. artificial intelligence programs that monitor electronic message traffic for key words and phrases.

\(^{21}\) This discussion is based largely on material in Koops' Crypto Law survey (see footnote 3).
mass-market software. Most member countries followed this recommendation, but the United States maintained separate regulations. The main goal of CoCom regulations was to prevent exports of cryptography to countries regarded as friendly to terrorist organisations; such as Libya, Iraq, Iran, and North Korea.

In 1995, CoCom was succeeded by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The treaty was signed in July 1996. It controls exports of dual-use goods and technologies, including encryption. The provisions are largely the same as CoCom regulations. Initially, public-domain or mass-market software could be freely exported but this position may have changed. Significantly, export over the Internet does not seem to be covered, since the Arrangement concentrates on a list of specific physical products.

The EU has adopted a community-wide regulation on the export of dual-use goods (EC/837/95) to deal with the possible 'leakage' of such goods through the Single Market to member states that do not have specific export controls in place.

Recently, the Organisation for Economic Co-operation and Development (OECD) completed a Recommendation concerning Guidelines for Cryptography Policy. These do not have legal force, but do indicate a broad national consensus. The negotiations over these recommendations took place during 1996, and resulted in the enunciation of eight principles. The guidelines that embody these principles are intended to promote the use of cryptography to foster confidence in and data security and privacy on global networks without jeopardising public safety and national security. The wording is striking for its emphasis on public-private co-operation, international interoperability and standardisation and international policy co-ordination, all of which are mentioned more frequently than law enforcement and national security. The guidelines do not apply to classified information ('for national security or similar reasons'), and define cryptography very broadly. The principles, taken at face value, may be inconsistent\footnote{22 For instance, the privacy principle could conflict with the lawful access principle.}, but the "integration" section provides little concrete guidance.

The eight principles are:

1. **Cryptographic Methods Should Be Trustworthy in Order to Generate Confidence in the Use of Information and Communications Systems.** This is evidently intended to encourage governments to foster trust. The accompanying text calls for key management contracts to "specify the jurisdictions that apply." This could call for a choice of law clause which would certainly clarify consumer rights and thus enhance trust. It could also be a reference to forum choice (here, a listing of nations having the power to compel key disclosure). In practice, this may be very complex, as would the identification of those considered to be party to a key management contract.

2. **Users Should Have a Right to Choose Any Cryptographic Method, Subject to Applicable Law.** This seems to oppose restrictions on choice of cryptographic techniques. The explanatory text suggests further that 'data users' may be responsible for protecting their data by cryptographic means. On the other hand, the 'Applicable Law' phrase seems to envisage export, import or use controls on user choice, whether by prohibiting certain products or mandating others. Finally, the principle leaves open important aspects of user identity - for instance, whether firms or their employees are users of the corporation's computer system.

3. **Cryptographic Methods Should Be Developed in Response to the Needs, Demands and Responsibilities of Individuals, Businesses and Governments.** This calls for competitive market development of cryptographic products rather than government-sponsored ones.

4. **Technical Standards, Criteria and Protocols for Cryptographic Methods Should Be Developed and Promulgated at the National and International Level.** This emphasises the importance of standards to ensure interoperability (different products can 'talk to' each
other), portability (encryption applications can run on multiple computer platforms) and mobility (products can work in different countries and security infrastructures).

5. The Fundamental Rights of Individuals to Privacy, Including Secrecy of Communications and Protection of Personal Data, Should Be Respected in National Cryptographic Policies and in the Implementation and Use of Cryptographic Methods. This bears directly on privacy rights, leaving open the vexed difference between the US concept of citizens’ rights to privacy from government intrusion and the common European view of private citizens’ rights to privacy against corporate (and other private) intrusions. It does extend the 1980 OECD privacy guidelines to explicitly include secrecy of communications. However, the statement refers only to individual privacy and not to corporate communications or confidential business information.

6. National Cryptography Policies May Allow Lawful Access to Plaintext, or Cryptographic Keys, of Encrypted Data. These Policies Must Respect the Other Principles Contained in These Guidelines to the Greatest Extent Possible. This was reportedly the centrepiece of the talks. The initial impetus for the discussions came from US perceptions of the threat to law enforcement investigations posed by encryption, apparently shared by the UK and France. Other nations do not attach the same importance to it, as can be seen in the wording: policies “May” allow access, but “Must” respect the other principles. The explanatory text makes clear that “lawful access” is not limited to governments or police, and is deliberately vague as to the adequacy of plaintext as opposed to decrypt key access. Instances of “lawful access” should be recorded, be of limited duration, and their fruits must only used for lawful purposes. The supporting text also makes it clear that keys used only for identity or integrity “should not be made available” without the owner’s consent. This does not prevent access to private keys in a dual key system where the same key may be used to sign and encrypt; however, keys that “provide for” identity or integrity only (private keys) are protected while those that “verify” identity (public keys) are not.

7. Whether Established by Contract or Legislation, the Liability of Individuals and Entities That Offer Cryptographic Services or Hold or Access Cryptographic Keys Should be Clearly Stated. This was directed at the widespread fear of liability, to which can be attributed: the use of cryptography to protect confidential or personal data; the adoption of particular (government-endorsed) encryption standards or products; and provision or failure to provide key recovery. It is worth noting that the language appears to favour contractual assignment of liability. This allows other principles (esp. 1, 2 and 3) to be fully realised. A single mandatory standard would reduce consumer choice and efficient liability assignment - in particular by matching liability assignments and service pricing to specific circumstances. The role for legislation suggested by the Principle is to enforce contractual assignments of liability (including third-party liability) and to deal with other specifics such as individuals’ misuse of their own keys, immunity for compliance with lawful access requests, or liability of government agents. Internationally, there may be scope for agreements on treating claims of negligent handling of keys, international key access, etc.

23 Baker, op. cit.
24 E.g. the widespread use of the US Digital Encryption Standard (DES) has been attributed (Baker, op. cit.) to the idea that one cannot be sued for flaws in an encryption system that the US Government has endorsed and used.
25 E.g. liability for inability to recover client data.
26 Hence the reluctance of large companies to enter the key recovery industry. In particular, they may fear retroactive liability arising long after the opportunity to take precautions has gone.
27 E.g. using a digital certificate to obtain goods or services and later repudiating it.
28 For instance, if a keyholder in Country A provides the keys used by a firm from country B doing business in A, it cannot usually be sued in A, but it may be liable in B. For instance, the recent US law against economic espionage could create liability for the keyholder if the government of A used the keys to conduct such espionage. In this case, the keyholder’s obedience to A’s laws violates B’s.
8. **Governments Should Co-operate to Co-ordinate Cryptography Policies. As Part of This Effort, Governments Should Remove, or Avoid Creating in the Name of Cryptography Policy, Unjustified Obstacles to Trade.** The first sentence encourages co-operation without mandating homogeneous or even harmonised policy. The second sentence suggests that cryptography policy should not be used as a pretext for discrimination against foreign goods or firms. This allows substantial room for manoeuvre; it allows the Wassenaar restrictions for one thing. By proscribing "Unjustified" obstacles, it calls for members to provide justifications for their policies. The supplementary text makes explicit reference to global electronic commerce and to the international availability of cryptographic products, requiring trade restrictions to be openly justified. Moreover, the text allows private party international access, recognises that market forces favour international use of cryptography and suggests that nations should not restrict the free flow of encrypted data.

2.3.2. **France**

2.3.2.1. **Use of Encryption**

France has been known for its restrictive policy regarding encryption. Cryptography methods were classified for the first time in the *decret* law of 18 April 1939 as army weapons in the second (of eight) most dangerous category of munitions. A legal definition of encryption was not given until the Law on Telecommunications n° 90-1170 of 29 December 1990 (modified by law 91-648 of 11 July 1991), in its article 28-I:

On entend par prestation de cryptologie toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens, matériels ou logiciels conçus à cet effet.

The French government limited encryption to military use, allowing practically no civilian applications. *Crypto-anarchists* (e.g., hostile governments, terrorist organisations and organised crime) could use the over-protection of information to hide subversive information, which was viewed as an intolerable interference with the application of the law in France.

Art. 28-I required requests for encryption import, export and use to be made to the prime minister:

a) à déclaration préalable lorsque ce moyen ou cette prestation ne peut avoir d'autre objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis

b) à autorisation préalable du Premier ministre dans les autres cas.

The government's rationale was described in the law (Art 28 alinéa 2 de la loi n° 90-1170) as "the preservation of the interests of national defence and the security of the State, both internal and external."

Permission could be granted only for uses aimed at authentication of a communication or assuring integrity of transmitted message. These "potentially permitted" functions are enumerated in Art. 2 of a regulation order of 28 December 1992 *relative aux disposition particulieres auxquelles sont soumises les prestations de cryptologie*. The order cites as examples protecting passwords, access and authentication codes. These are fundamental to electronic mail and commerce, are consistent with the OECD Principles and do not impede government access. The files of declarations and demands for authorisation are registered with *le Service Centrale de la Sécurité des Systemes d'Information*.

---

29 This discussion is based largely on material in the "lambda Newsletter (footnote 5)" and the Crypto Law Survey (footnote 3).

30 This law is, partly, still in force.
(SCSSI), a Prime Ministerial department under the authority of the SGDN, the Secrétaire Général de la Défense Nationale.

The French government became aware of ever-increasing public demand for securing information exchanges on the net (e.g. for electronic commerce). On the other hand, they were increasingly conscious of “info-wars” in which protection of the means and content of communication has strategic national security value. The development of complex computer networks went hand in hand with the need of French businesses and individuals for secure and confidential communication. As the responsible French Ministry (Post and Telecommunications) put it on its Web site, the restrictive policy on encryption had to be changed:

Les dispositions de la réglementation touchant à l’usage de la cryptologie doivent être assouplies. En effet, le développement des autoroutes de l’information va entraîner une augmentation considérable des transactions électroniques qui ont besoin d’être sécurisées afin de garantir leur fiabilité et leur confidentialité.  

These ideas resulted in the new encryption policy laid down in the Loi no. 96-659 de 26 Juillet 1996 sur la réglementation des télécommunications. Art. 17 of this law modifies article 28 of the 1990 law and adds to the definition of encryption the following:

La cryptologie, c’est donc l’arme moderne par excellence (...). Elle apparaît comme une facteur essentiel de développement des échanges sur Internet, largement utilisée par les protocoles de télépaiement, mais les États s’en défient car elle présente bien évidemment le risque de faire échapper à leur contrôle toutes sortes de trafics et de détournements.

This new law considerably relaxes and simplifies the legal framework regulating encryption. However, decrees implementing this law have yet to be published.

The new law permits unrestricted use of encryption methods to authenticate or guarantee the integrity of messages. In other words, when information is transmitted without encoding, the prior requirement of declaration has been annulled for encryption used only for electronic signatures or to guarantee authenticity. Encryption methods can also be used for confidentiality services managed by a trusted third party.

According to Art. 28-II of the 1990 law, non-compliance is punishable by a fine of 6,000 - 500,00 FF and/or 1 - 3 months imprisonment.

A 16 October 1995 press release specified that under the 1990 law use of cryptography for protecting passwords, access codes, subscriber numbers or bank card numbers for authentication purposes only required declaration by the provider when installing the service. It is unclear to what extent the 1990 law is enforced in practice; it is rumoured to be widely ignored. It seems impossible for individuals or enterprises to obtain authorisation for “strong” cryptography. Even for state-owned industry, cryptography that does not serve military or high-grade security purposes must be breakable. SCSSI, the office dealing with authorisation, renders decisions without explanation.

On 25 August 1997, Premier Minister Jospin, speaking at the University of Communication in Hourtin, described the government’s priorities in preparing France for the information society. One is the development of electronic commerce. For this reason, Jospin intends to accelerate publication of the decrees that liberalise cryptography. Particular effort will be made in favour of so called “weak” cryptography that has been heavily restricted till now.

2.3.2.2. Trade in Encryption Software

According to Art. 17 of the new Law on Telecommunications, import or export between France

---

32 Rojinsky, C. Internet, Support de vente, October 1996, Paris
33 This leaves open the possibility of 'stealth signatures' containing encrypted information.
and countries outside the European Union of encryption devices or services that perform restricted
certainty functions require authorisation from the Prime Minister. To obtain it the supplier may be
required to reveal the identity of the purchaser. Encryption resources performing other functions
(authentication, identification) are subject to declaration.

Until the decrees for the new law are implemented, the old restrictions remain in place. That is,
import, export and use of cryptography requires:

1) prior declaration if they can only be used to authenticate communications or assure
their integrity; and

2) prior authorisation by the Prime Minister in all other cases.

Simplified procedures exist for certain cryptography products or services or certain user
categories. For authorisation, a dossier containing technical details and administrative data must be
submitted. Authorisation can be subjected to certain additional conditions in order to reserve the use of
certain types of cryptography to defined user or application categories.

Some French organisations (l’Agence pour la Protection de Programmes (APP34) and the
Interdeposit group) accept signatures generated by the Pretty Good Privacy (PGP) program, arguing
that the law authorises the free use of encryption for authentication. This points up an ambiguity as to
whether products are restricted if they can be or are used only for authentication.

2.3.2.3. Protection of Encrypted Information

No apparent developments, in view of the sparse use of encryption.

2.3.3. Germany35

2.3.3.1. Use of Encryption

Germany has no laws regulating encryption use, and the Bundesamt für Sicherheit der
Informationstechnik (BSI) publicly declared in 1995 that the use of encryption techniques in sending
electronic documents in telecommunications was not regulated by any existing law or regulation. Since
then, no new laws or concrete proposals have been introduced, though there has been a lot of
discussion, debate and other government activity on this topic. Despite or because of this, there have
been persistent, if conflicting rumours regarding future regulation.

The December 1995 report on the Information Society by the German Council for Research,
Technology and Innovation recommends legal conditions for the decryption of documents by state
authorities. These conditions should specify criteria for decryption authority and unequivocally regulate
document seizure. The report states that cryptography products should be developed and implemented
in ways that make it possible to decrypt single documents for purposes of criminal law enforcement.
That same month, a conference of Justice Ministers expressed concern that law enforcement is not
keeping pace with technological developments. Federal Minister of Justice Schmidt-Jortzig
acknowledged the problem, but doubted that a prohibition could be enforced, and suggested that
German regulation would be inadequate to deal with global cryptography.

The following year, the magazine der Spiegel carried two articles on planned restrictions of
cryptography use. They reported on 8 January 1996 that the Ministry of the Interior was preparing a draft
law to prohibit (unescrowed?) cryptography. In December 1996, another article on impending

34 cf. section 0.
35 We would like to thank Christopher Kuner, attorney-at-law, for his very valuable comments on this
subject area. In addition, much of the material was drawn from Koops’ Crypto Law Survey (see footnote 3).
legislation suggested that it would pursue one of three courses: mandatory key escrow; license requirements for commercial encryption products; and a ban on use of unlicensed encryption, or encryption that did not provide key escrow. The Bundestag resolved on 20 June 1996 that effective encryption procedures may be freely chosen by participants within the scope of the constitutional right to confidential communication. However, this right may be abridged for internal or external security reasons. An interministerial Task Force on Encryption Policy (Kryptopolitik) was set up in October 1996 to develop concrete suggestions for an overall political strategy on IT security; whether and how legislation should be set up, potential legal issues produced by restrictions on use of encryption, and problems perceived by parts of the government due to the lack of regulation. The federal Minister of Economic Affairs (who heads the Task Force) stated on 7 October 1996 that a trade-off should be found between the equally important principles of freely choosing cryptography and preventing criminal encryption abuse. This group has not produced an official proposal for a Kryptogesetz. An Interior Ministry official responsible for national security appeared, in a November 1996 debate, to favour encryption legislation to protect law-enforcement and national security. He did not think criminals would use licensed (key-escrow) cryptography, but suggested that use of unlicensed encryption would give rise to criminal suspicion and would facilitate traffic analysis to discover criminal organisations. In December 1996, a meeting in camera between federal and state Secretaries of State was reported by der Spiegel to have reached an understanding favouring a proposal that only licensed encryption could be used, and licensure would require deposit of private encryption keys and encryption source code for law-enforcement and national security access. Distribution and use of unlicensed encryption would be banned. Rumours concerning the status of this proposal ranged from a trial balloon to a (preliminary) draft.

In 1997, a hearing of various legal scholars, and governmental officials in the Bundestag indicated, however, little support for the need of new legislation. Approval was limited to the BSI, which was in favour of regulation to be able to obtain information on criminal behaviour. On one point in the discussion, there seems to be agreement. If any regulation should be considered, the location of private keys should be restricted to German territory. The Bavarian Secretary of Internal Affairs demanded federal telecommunications law sanctions against use of encryption by conspirators. Contrary to law-enforcement and national security officials, however, state Ministers of Economic Affairs and federal Minister of Economic Affairs Rexrodt stated early March 1997 their opposition to restrictions on encryption use. The position of the Ministry of the Interior has been clarified by a series of statements by Minister Kanther. On 28 April 1997 he stated that he wants to allow only technologies whose manufacturers agree to provide keys to law enforcement. In June 1997 the Interior Ministry seemed to favour a voluntary approach, in which the government would certify cryptography products which incorporate key-escrow. Use of certified products would be voluntary. Most recently, on 22 July 1997 Minister Kanther stated that there will be no encryption law until the government has investigated what is technically feasible and useful. Summarising, it appears that The main impetus for restrictions comes from the Interior Ministries (especially at the state level), with the Ministries of Economic Affairs, Justice and Science, Research, and Technology taking various, but mainly negative positions.

The main political parties show a similar range of negative-leaning positions. In particular, the FDP explicitly spoke out against encryption regulation during the April 1997 parliamentary debate on the Information and Communication Services Law. CDU/CSU-MP Marschewski called for a Europe-wide licensing regime. The political party Bündnis 90/Die Grünen opposes cryptography prohibitions or restrictive (e.g., key-escrow) regulations. Finally, Federal Minister of Justice Schmidt-Jortzig, speaking at a March 1997 conference of his FDP party, called demands to ban cryptography "deeply illiberal."

Since no actual detailed proposals have surfaced, the debate is divided along traditional lines:
pro-privacy, pro-commerce arguments set against crime fighting and national security concerns.

The business sector is rather unanimous in rejecting any attempt to restrict the use of encryption. The fundamental argument is that encryption is an essential part of conducting business (esp. electronic commerce over the Internet) as it protects: transmission of computerised data from third parties; authenticity and integrity of electronic communications; and confidentiality of electronic documents in telecommunications. It is further argued that use restrictions would violate:

- Civil rights of economic development (Article 12, par. 1 and Art. 2, par. 1 of the German Constitution)
- Confidentiality of communications (Article 10 of the German Constitution), and
- Informational self-determination (Article 2, par. 1, Art 1, par. 1 of the German Constitution).

Beyond this, there has been some discussion of the conditions and type of encryption to be used in transmitting state secrets.

The emerging positions reflect a mix of economic, constitutional and pragmatic legal concerns. With the exception of provisions in the new Digital Signature Act and anticipated clarification of the status of encrypted communications as regards wiretap in an amendment to the Telecommunications Act of 1996, no new legislative initiatives are anticipated before the next election. The most likely future option at this stage appears to be a voluntary system: encryption users can attain a security certification by, among other conditions, complying with key escrow/key recovery conditions. There is already an informal analogue of this process; BSI conducts voluntary evaluation of cryptographic products, though there is as yet no key recovery attached to this evaluation. While the new Digital Signature Act does not allow certification authorities to hold private keys, people favouring more restricted use hope for the take-off of a CA network as a first step towards a future Trusted Third Party network/infrastructure.

2.3.3.2. Trade in Encryption Software

Encryption is one of the items included in the more comprehensive Aussenwirtschaftsgesetz (AWG) that regulates the export of certain goods and technologies which can be used for both civilian and military purposes. Anlage AL of the accompanying ordinance, the Aussenwirtschaftsverordnung (AWV) contains the export control list including encryption products. This law almost strictly follows European Union regulation of the export of dual-use goods (EC/3381/94).

2.3.3.3. Protection of Encrypted Information

There has been some discussion of whether wiretap laws would be applicable to Internet communications. No apparent use has been made of this discussion, and there is no uniform opinion within the Justice Ministry as to whether this is allowed under current Telecommunication Law. A new Telecommunications ordinance (not yet published) is expected to replace the existing ordinance of 1996; this could clarify the issue.

---

36 See section 0.
37 This is distinct from encryption per se: wiretap laws may authorise government access to channels of communication but to date they do not guarantee that the government can make sense of the intercepted communication. See further discussion in Section 8.4.
2.3.4. United Kingdom

2.3.4.1. Use of Encryption

The United Kingdom places no formal restrictions on the use or trade in encryption by UK citizens or businesses. Almost the entire elaboration and discussion of legal issues in the encryption area takes place in the arenas of TTP and legal treatment of encrypted data. The only exception of which we are aware surfaced in an internal National Health Service memorandum last year concerning measures to safeguard patient information on the "NHSNet." That memorandum revealed the existence of a block encryption program ("Red Pike") that the Government-commissioned from a private software manufacturer. The program has a "back door" feature that allows Government access, and further offers modular choice of encryption levels. The Memorandum strongly urged the use of this program by both NHS and fundholding practices and suggested that it might eventually become part of the NHS electronic document interchange requirement. There was vigorous and largely negative reaction by the affected parties, and it is believed (by an official of the British Medical Association whom we contacted) that the memorandum was not being enforced and would be withdrawn by the new government.

The most important development is found in the Department of Trade and Industry (DTI) proposals for establishing a TTP structure. These allow users to choose whether or not to avail themselves of third party encryption service providers, who would be compelled to offer key recovery. In other words, while TTP use is voluntary, TTPs face mandatory licensure by a centralised authority, mandatory key escrow/key recovery requirements, and strict liability. The central control aspect has been attacked as inconsistent with the private nature of most regulated cryptography, a source of economic distortion and a potential risk with regard to industrial espionage and government abuse. It has also been mentioned that the proposals for licensing do not provide incentives to seek licensing or a clear delineation of individuals (such as those generally receiving common law evidentiary privileges - doctors, clergy, attorneys) who might be exempt. The strict liability conditions are regarded as a strong disincentive to entry and a source of 'moral hazard' for users (who would be less likely to take their own precautions). Privacy advocates have pointed out that the proposals further stipulate that clients are not to be notified of searches. This is broadly consistent with the provisions of the

2.3.4.2. Trade in Encryption Software

The UK has no export restrictions beyond those implied by the CoCom/Wassenaar agreements and the EU regulation of dual-use exports. The DTI proposals would require licensing of software imported into the UK; this may impose costs and risks that reduce inward high-tech investment and

---

38 On-line sources for material used in this discussion include the Cyber-Rights and Cyber-Liberties page (footnote 4) as well as the EFF archives (footnote 6), the EPIC pages (footnote 7) and the Crypto Law Survey (footnote 3).

39 For further information, see United Kingdom Department of Trade and Industry, Licencing of Trusted Third Parties for the Provision of Encryption Services, March 1997, available at http://www.dti.gov.uk/pubs/. See also the discussion in section 0.


41 Analogous to the 'safe harbour' provided in the Utah Digital Signature Act - see section 0.
economic development.

2.3.4.3. Protection of Encrypted Information

As mentioned in section 0, the central issue is the compelled production of decryption keys or plaintext. To understand the issue, it is necessary to briefly review the right to silence in general terms. Until 1994, this right consisted of a conglomerate of different ideas:

- A caution - given initially when the investigating officer had grounds for suspecting that that person had committed an offence and the purpose of the questions was to obtain evidence to use in court. A caution had to be given on arrest. If the person was then interviewed at a police station, the interviewer had to remind the interviewee at the start and after every break that he or she was still under caution. The caution was repeated at formal charge.

- A presumption of innocence;

- Police and prosecution were not permitted to comment on the defendant's silence in the police station or in court. There were limited exceptions - the prosecution could adduce evidence of silence when accusation was made by victim or parent or where the accused was on 'level terms' with police. The judge could comment, but only in measured terms, with a warning to the jury not to assume guilt from the defendant's silence.

- Privilege against self-incrimination

As a result of sections 34-35 of the Criminal Justice and Public Order Act 1994, the first and third paragraphs above require reconsideration. A Royal Commission on Criminal Justice in 1993, suggested that the defence should be under an obligation to disclose aspects of its case but stood firm against the wholesale abolition of the right to silence. Despite this, the Criminal Justice and Public Order Act 1994 now allows juries to use silence as evidence against the accused.

Article 3 and section 34 are aimed at 'ambush defences' and at forcing disclosure of the defence, by allowing a court to 'draw such inferences as appear proper' from a failure to mention a relevant fact. A jury would thus be told to attach less weight to a defence, which has only been revealed at the trial and logically is correspondingly less credible. Article 4 and section 35 apply where the prosecution have satisfied court that there is a case to answer and a defendant declines to testify in his or her own defence. The judge, in the presence of the jury, is empowered to tell the defendant that the stage has been reached at which he or she can give evidence and to issue a warning that if he or she remain silent, that it will be permissible for the jury to draw whatever inferences appear to be proper.

Though Bentham bears the burden of suggesting that the right to silence only protects the guilty and the criminally sophisticated when he wrote, "Innocence claims the right of speaking as guilt invokes the privilege of silence" he did so at a time when the right to silence as we know it did not exist, when the defendant was not permitted to testify in his own defence and when police interrogation did not exist. The pressure to answer police questions will necessarily bear on the innocent as well as the guilty. The controversy surrounding the right to silence encompasses empirical questions and evidential problems but ultimately it should be a decision based on concepts of due process of law and proper constitutional principles. It is another of those important markers, which define the relationship of State and citizen, delineating constraints on the State and our moral choice that prosecution, and punishment should not be based on evidence from the accused.

The specific encryption connection concerns the compelled or "interpretable" disclosure of decryption keys or plaintext of encrypted documents. This consideration was echoed in the German Interior Ministry official's suggestion that use of unlicensed encryption would give rise to criminal

---

42 Key Escrow Working Group, op. cit. 1996.
suspicion. To date, no prosecutions have sought such disclosure, but an individual in the Crown Prosecution Service stated that refusal to produce either a key or plaintext would “certainly be a matter for judicial comment.” Thus, while there is no definite decision one way or another, it is possible that failure to disclose one’s own private key could have negative consequences. It is not known whether this extends to third parties (though it would be a condition of licensure under the DTI proposals).

2.3.5. United States

2.3.5.1. Use of Encryption

In 1993, the Clinton Administration announced the Escrowed Encryption Initiative (EII), usually referred to as the Clipper Initiative after its first hardware implementation. The associated Escrowed Encryption Standard (EES) specified use of a classified secret-key algorithm called SKIPJACK. The ostensible goal was to provide citizens with secure communications while preserving law enforcement access via additional information that identifies the chip used to produce the encrypted message. Communications encrypted with EES can be decoded by combining two parts of that chip’s master key, obtained from two different escrow agencies with a court order.

The predictable quid custodiet opposition to government escrow agents led to the “commercial key escrow” (Clipper II) scheme that allowed users to choose private-sector escrow agents. The EES was billed as a voluntary standard for use in telephone communications, but privacy interest groups feared that its use might become mandatory once a sufficient market share had been achieved. The resounding rejection of the scheme makes this a distant possibility.

In March 1997, the Department of Defence announced that the developer of the Fortezza card used to implementing the EES key-escrow system would abandon EES in favour of a key management infrastructure (KMI) incorporating key escrow and key recovery. The KMI (or Clipper III, as it was inevitably dubbed) was first described in May 1996, in a paper entitled “Enabling Privacy, Commerce, Security and Public Safety in the GII”. Participation would be voluntary, and a free choice of encryption algorithms would be offered. A Policy Approving Authority (PAA) would be set up to license Certification Authorities (CAs) and set performance standards to ensure adequate law enforcement access. Users would be required to escrow their private keys with a (licensed or unlicensed) Escrow Authority before obtaining a public-key certificate. Firms would be allowed to hold their own and employees’ keys, provided the escrow division met PAA’s performance criteria, including independence from the rest of the organisation, compliance with key recovery requests and even, at one stage, employment of at least one individual holding a government security clearance.

Both official and unofficial bodies have expressed doubts about the viability of the key recovery proposals. In June 1996, the National Research Council (NRC) released a study, that calls on the government to promote widespread commercial use of cryptography without encouraging key escrow even if the government develops it for its own use. Even if the current uncertainty regarding key escrow were resolved, adoption of escrowed encryption (or of any other standard) should be voluntary.

Recent developments have commingled key recovery and trade controls. The temporary relaxation of export controls that accompanied a shift of responsibility from the State Department to the

---

44 Among the many sites dealing with the US situation, on-line sources for material used in this discussion include the EFF archives (footnote 6), the EPIC pages (footnote 7), and the Crypto Law Survey (footnote 3).

45 Initially, they were the Automated Systems Division of the Treasury Department and the National Institute of Standards and Technology.

46 Cryptography's Role in Securing the Information Society.
Commerce Department was meant to be seen as part of a broader encryption policy that claims consistency with the NRC recommendations. Choice of an encryption system and use of key escrow will remain unconstrained. The government does intend to promote key-escrow cryptography products by expanding its own purchases and use of them, promoting the practice in international fora and stimulating development of innovative key-escrow products and services by procurement policy and RTD assistance. The Administration has also sought, in a variety of legislative initiatives, to facilitate commercial key-escrow, including liability “relief” for escrow agents releasing keys.

A bill introduced as HR 3723 in October 1996 law includes an amendment requiring an annual account by the US Sentencing Commission of the use of computer encryption to conceal criminal activity.

At the end of March 1997, the “Electronic Data Security Act of 1997” draft was published. It provides for registration of Certification Authorities (CAs) and Key Recovery Agencies (KRAs). Registered CAs may only issue public key certificates to users who provide information to registered KRAs sufficient to allow timely decryption by authorised government agents. Registered or unregistered KRAs would be required to comply with warrants or authorisation by the Attorney General. After complaints that the Fourth Amendment prohibits authorisation without judicial review, the draft was amended in May 1997 to establish an equivalence between the legal criteria for plaintext recovery and wiretapping. As with the UK’s Interception of Communications Act 1985, users would not be informed of information released to government agents. Intentional violation of certain provisions (e.g., knowingly providing public key certificates to users who have not provided a KRA with sufficient information) is subject to criminal penalties and civil penalties that are reduced for registered CAs and KRAs. Use of encryption in furtherance of another crime can draw six months' to five years' imprisonment (though using key recovery encryption is an affirmative defence). Encryption products must be labelled to indicate whether the product uses registered KRAs. Finally, the law obliges the President to negotiate mutual recognition of registered KRAs with other countries. While the government is no longer seeking a sponsor for the draft bill, the provisions of the McCain-Kerrey Secure Public Networks Act (S 909) are essentially identical. Additionally, the latter would require government use and funding of encryption products based on key recovery cryptography, establish an Information Security Board and provide waiver authority for the President in national security cases. The bill was approved by the Senate Commerce Committee on 19 June 1997, including several amendments. The voluntary key recovery approach is restated in the “Magaziner group’s” Framework for Global Electronic Commerce.

The Anti-Electronic Racketeering Act introduced as S 974 by Senator Grassley would effectively prohibit encryption, only allowing the use of escrow-like software as an affirmative defence. The bill doesn't seem to have much support at present.

The Leahy bill and the SAFE Act (see p. 25) would penalise the use of encryption in furtherance of a federal felony, if the encryption is intended to obstruct investigation. It creates a framework for key escrow agents, including strict requirements for law enforcement access; anyone is free to use non-escrowed cryptography.

On the positive side, the Leahy bill and Pro-CODE (see p. 25) affirm citizens' rights to freely use encryption in the US (except as noted). Pro-CODE also limits the government’s authority to set limited key length and key escrow standards for encryption products used by private parties. The Communications Privacy and Consumer Empowerment Act introduced as H.R. 1964 by Representative Markey in June 1997 would prohibit interstate commerce restrictions on encryption use or sale.

47 Up to five years' imprisonment.
regardless of medium used or key length, and would expressly bar the government from requiring key escrow as a condition for certificates of authority or authenticity. In mid-September 1997, an attempt was made to amend the SAFE Bill to impose criminal penalties on the manufacturing or distribution of domestic encryption products that do not contain a government-mandated "back-door." The Oxley-Manton amendment was opposed by, among others, a group of 28 university law professors, who wrote to Congress challenging the Amendment as an unconstitutional attack on First Amendment free speech rights and Fourth Amendment proscription of secret searches and delineation of privacy rights. They further pointed out that the obligation (laid down in Section 501 of the House Intelligence Bill) to negotiate agreements with foreign nations for "mutual recognition of any key management infrastructures" magnifies the risk to US citizens, who would have no protection against foreign government access to their keys whether stored in the US or elsewhere. Moreover, they argue that the US would no longer be able to credibly claim to protect the interests of dissidents in other countries. Finally, they argue that the proliferation of key escrow systems would be used to weaken the confidentiality and thus the economic position of US firms operating in foreign countries. This was rejected by the committee.

Overall, the public perception and the weight of court decisions seem to be hardening against use restrictions. However, new approaches to mandated use of key recovery continue to be suggested by the government.

2.3.5.2. Trade in Encryption Software

Cryptography export used to be controlled by the International Traffic in Arms Regulation (ITAR), enforced by the State Department. In December 1996, The Federal District Court of the Northern District struck down portions of the ITAR. Within a few weeks, similar restrictions were transferred to the Commerce Department's Bureau of Export Administration (BXA). The export policy was relaxed to favour export of data recovery cryptography. However, on August 26 1997, the same court (in a continuation of the earlier case) the same case struck down the new arrangement, declaring:

"The court declares that the Export Administration Regulations . . . insofar as they apply to or require licensing for encryption and decryption software and related devices and technology, are in violation of the First Amendment on the grounds of prior restraint..."

As these rules represented the most recent expression of US policy, they will be briefly described here. The BXA initiative was first announced in advance of the ITAR decision by the Vice President on 1 October 1996, and further elaborated in a November 15, 1996 executive order and memorandum and the Commerce Department draft Export Administration Regulations of December 30, 1996. The initiative also included the Department of Justice in cryptography export decisions.

Making cryptography available on the Internet or a BBS is considered export, unless appropriate measures are taken to prevent foreigners from accessing the cryptography.

The new rules distinguished five types of controlled "encryption items" (EI).

- Certain mass-market encryption software could be released from EI controls after a one-time review.

49 The day following this action Alan McDonald, a senior counsel member with the Federal Bureau of Investigation, speaking at the International Conference on Privacy in Montreal, said "extremist positions on electronic encryption are not only threatening to normal law enforcement, but they are also elitist and nondemocratic."
50 Bernstein v. Department of State. The case involves the right to teach about cryptography and collaborate with colleagues in other countries.
• "Data recovery" cryptography (i.e., encryption items that permit government access to keys or plaintext with a lawful warrant) was eligible for an export license to non-embargoed countries.

• Cryptographic products using no more than 56-bit key lengths, after a one-time review, could be granted a six-month export license, provided the exporting business commits itself to incorporating a data recovery feature in its products within the next two years. This relaxation of controls was set to last until January 1, 1999: after this, the export of non-recovery 56-bit cryptography will be prohibited again, and the ITAR status quo ante would be restored (maximum 40-bit key length, exceptions for financial institutions).

• All other encryption items may be eligible for encryption licensing arrangements; items not authorised under a licensing arrangement will be considered on a case-by-case basis.

• Encryption “technology” may be licensed for export on a case-by-case basis.

The ITAR rules were amended in February 1996 to permit unlicensed temporary export of products to non-embargoed countries for strictly personal use (e.g. PGP on a laptop), provided the exporter took "normal precautions" to ensure the security of the product. Records of each export had to be kept for five years. Under the new rules, this personal use exemption was replaced by license exception. The Commerce Department announced plans to clarify the personal use exemption for laptops in February 1997.

Michael Froomkin argued that the government had no authority to steer industrial cryptography policy through export regulation. He further points out that one statute from which the power to restrict exports flows, the Export Administration Act, expired in August 1994, and the subsequent extension is based on a state of emergency declared under the International Emergency Economic Powers Act. This emergency was never fully specified, and it strains credibility to suppose that it has persisted this long.

The ITAR restricted export of "dual-use" cryptography by placing it on the Munitions List. Export licenses for strong products aimed at performing confidentiality functions were usually issued only for foreign branches of American enterprises and financial institutions. “Weak” cryptography (e.g., with a 40 bit maximum key-length) could also be exported.

Export of cryptography for authentication or integrity purposes was already covered by the Export Administration Regulations. Some public-domain products were placed on a Commerce Control List of permitted products.

In 1995, the Administration proposed allowing export of products using up to 64 bit keys, if they implemented key-escrow. Criteria for exportable cryptography were discussed at two meetings in September and December 1995; criteria for the escrow agents were handed out at the December meeting.

Cases

In addition to Bernstein v. Department of State, mentioned above, there are several other pending cases of potentially great importance. On March 22, 1996 the Washington, DC Federal District Court held that the export restrictions did not violate the First Amendment. The defence claimed the issue presented a political question for the two elected branches to decide. On 6 November 1996, the

---

51 E.g., locking the product in a hotel room or safe.
52 Cf. Export Administration Regulations License Exceptions at 15 CFR 740.4 and at 740.14 and the original ITAR version at 22 CFR Parts 123 and 126.
53 M. Froomkin, op. cit. (c.f. footnote 16 on page 9).
54 Karm v U.S., 925 F Supp 1 (D DC 1996). The case concerned a book, Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code, 1996), which was ruled freely exportable despite containing complete source code for strong encryption algorithms. The offence was to export a verbatim copy of the source code on a floppy disk.
Department of Justice filed a brief on their appeal. The case was remanded to the district court on 21 January 1997 in light of the BXA initiative; the constitutional issues were not resolved. Pending resolution of the constitutional issues, the Department of Justice has stated that it will continue to enforce the export restrictions. A related case, filed in August 1996 by law professor Peter Junger, seeks to assert the plaintiff's right to teach about cryptography (in a computer law course) without obtaining a license, even though foreign students might be present.

**Bills**

Three bills seeking to ease export controls have been proposed. First came the "Leahy bill" which would, *inter alia*, allow *generally available or public-domain* cryptography to be exported. At the same time, Representative Goodlatte introduced a similar bill, Security And Freedom through Encryption (SAFE) Act. SAFE received unanimous approval from the House Subcommittee on Courts and Intellectual Property (30 April 1997) and the House Judiciary Committee (14 May 1997). SAFE was further approved by the House International Relations Subcommittee on International Economic Policy and Trade (24 June 1997) and the House International Relations Committee (22 July 1997). Recently, an attempt to include an import restriction in the SAFE Bill was defeated and the Bill continues its passage through Congress.

The next bill to be introduced was Senator Burns' Promotion of Commerce Online in the Digital Era (Pro-CODE) Act. This bill seeks to relax export controls for *generally available or mass-market* cryptography. The later version would also establish an Information Security Board to provide special access to the development of new plans for privacy-enhancing technologies to law-enforcement agencies.

The McCain-Kerrey Secure Public Networks Act (S 909), introduced June 1997, would allow export of 56-bit non-key recovery cryptography under a license. Key recovery cryptography would be exportable regardless of key length, under a license. As noted above, this bill places serious limits on the use of unescrowed encryption by US citizens. In particular, it authorises the government to obtain private keys and other highly sensitive decryption information without a court order and without notice to the individual whose privacy is being compromised. These bills raise serious Fourth and Fifth Amendment concerns.

The Department of Commerce recommended easing export controls after a joint study with the National Security Agency found that the export restrictions harm US business. The National Research Council study on cryptography policy (see footnote 46) recommended that export controls be progressively relaxed, but not eliminated. Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable; for today, this would mean allowing export of 56-bit symmetric encryption products. Export of stronger cryptography (i.e., today, using more than 56 bits) should be exportable on an expedited basis to a list of approved companies if the proposed user agrees to provide the US government access to decoded information.

---

55 US Department of Justice, press release dated Tuesday, August 26, 1997.
56 The Encrypted Communications Privacy Act introduced 5 March 1996 as S. 1587, reintroduced 27 February 1997 as S. 376.
57 Introduced as H.R. 3011 in March of 1996, reintroduced on 12 February 1997 as H.R. 695.
58 The Judiciary Committee added three amendments: to ensuring that the bill only proscribes cryptography intended to conceal a federal felony; to correct a technical oversight; and, and require the Attorney General to maintain a registry of cases where cryptography has hampered an investigation.
59 The International Relations Committee rejected an amendment to reinstate controls if national security were compromised.
60 See discussion of the Oxley-Manton Amendment in section 0.
61 Introduced as S. 1726 in May 1996, reintroduced as S. 377 on 27 February 1997.
According to a draft paper *Enabling Privacy, Commerce, Security and Public Safety in the GI*, the government is working toward a policy that will readily license export of key-escrow systems, once the needed infrastructure and government-to-government agreements are in place.

Overall, despite repeated legal setbacks and waning public support, the government continues to press for export restrictions. Net browsers containing 128-bit encryption are freely exported (except to France), but exports of stronger products (such as version 5.0 of PGP software or email systems that include it) are still restricted as of September 1997.

### 2.3.5.3. Protection of Encrypted Information

The issue in the US is defined by the Fifth Amendment's command that no person "shall be compelled in any criminal case to be a witness against himself.", and (weakly) by the Fourth Amendment's protection against unreasonable search and seizure.

The Fourth Amendment provides little protection from the search and seizure of documents. In *Warden v. Hayden*, (387 U.S. 294, 304 (1967)) the Supreme Court discarded the rule that search and seizure depended on a superior right to the seized property. Before Warden, officers could search for fruits of a crime, contraband and for instrumentalities, but not for "mere evidence." Although the Court expressly refused to consider "whether there are items of evidential value whose very nature precludes them from being the object of a reasonable search and seizure," many now believe that all objects can be seized.

The Fifth Amendment protects against self incrimination; it allows compelled production of documents, because this does not compel anyone to write the documents. Thus, the government can compel the production of documents and any written key encrypting them. Under the *Warden* ruling and Fifth Amendment jurisprudence, written keys cannot be distinguished from the documents themselves: a key found by search can be used, and one can subpoena key if one can subpoena the underlying documents. The basis of protection must be a Fifth Amendment privilege against compelled disclosure of a memorised cryptographic key. The Fifth Amendment is now interpreted to bar only the production of "testimonial information," (incriminating communication that might "itself, explicitly or implicitly, relate a factual assertion or disclose information"). It is certainly possible to choose a testimonial phrase (e.g., "I, John Doe, stole a package of chewing gum from X") - there are many statutes that allow one to confess to crime via such a key, triggering criminal liability and Fifth Amendment protection. This will rarely happen, however, so it cannot be relied upon as the basis for a general rule. This seems to suggest that key production can be compelled. However, the line between testimonial and non-testimonial ways of expressing the same information is very fine. The central point is that production of the key testifies to a certain degree of connection with and integrity of the underlying document.

As a general rule, third parties can be compelled to produce keys unless doing so would incriminate themselves. An interesting side issue concerns key escrow: if the only written copy of an individual's private key is held by a third party, can the individual be compelled to identify that third party, and can the latter structure his records in such a way as to claim privilege against producing it (e.g. by double-encryption with a testimonially-incriminating key)?

One method for compelling production is to grant use immunity for key production. The vexed question is whether the intimate connection between the key and the documents provides derivative use immunity for the latter. Even if this derivative immunity does not follow, the documents may yet be

---

protected. One reason is that decryption gives the document a testimonial content; without the key, the
document would have no evidentiary value (see footnote 64). A second reason is that the key
authenticates the document.

The principal countervailing position to this view is a privacy-based approach reflected in a
series of early decisions\(^\text{65}\) that take a property-oriented approach to privacy and thus a broad view of
Fourth and Fifth Amendment protections.

2.4. SUMMARY AND COMPARISON

We begin with a summary discussion that highlights the answers to research questions 1-3. The
first part, "Issues Arising," answers the first research question, while the second, "Initiatives," sketches
the answers to the second two questions, describing legislation and other initiatives. The section
concludes with a short comparison of the surveyed countries.

2.4.1. Issues Arising

The availability of 'strong' encryption raises a number of distinct legal issues. The materials
reviewed in this survey suggested a division into three broad classes:

- use of encryption and provision of encryption services;
- restrictions on the export or import of encryption products (software and hardware); and
- legal protection of encrypted documents from compelled disclosure.

The use of encryption raises problems because it provides private or protected means of
communication and data storage even in the context of public networks or storage devices provided by
third parties. Some uses of encryption are meritorious, and are even viewed as essential to the
realisation of electronic commerce and other valuable uses of the electronic superhighway. However,
the same techniques can be used to protect activities that violate criminal law and/or damage national
security. The central problem is how to distinguish between meritorious and harmful uses, or how to
guarantee legitimate access whilst protecting valid privacy interests. Specific questions include:

- what legal categories of encryption use\(^\text{66}\) to establish;
- whether to compel individuals using encryption to make their private keys available for
  authorised access; and
- what legal status to give third-party providers of encryption services.

Trade restrictions have their origins in the possible use of encryption for purposes of espionage.
Encryption hardware and software implementations have sometimes been classified as munitions or
dual-use\(^\text{67}\) goods, and international trade restricted on that basis. Additionally, nations imposing use
restrictions may find it necessary to back them up with trade restrictions.

In cases where surveillance, investigation or court cases involve encrypted messages, a further
set of issues can arise regarding disclosure of encrypted messages. The specific questions are under
what circumstances such messages can be compelled, whether compelled disclosure extends to private
'decryption' keys or only to the content of the messages, and the application of this compulsion to those
who send and receive encrypted messages and third parties who may hold private keys.


\(^{66}\) e.g., encryption used for confidentiality vs. encryption used for authentication.

\(^{67}\) civilian and military
2.4.2. Initiatives

2.4.2.1. International

Use of encryption

We did not find any international initiatives restricting the use of encryption. Trade restrictions

The principal initiatives that restrict exports of dual-use commodities are the CoCom and Wassenaar agreements and EU Regulations, and the evolving OECD Guidelines concerning trade in dual-use commodities. In effect, these primarily restrict exports to nations whose governments are deemed to support terrorism.

Protection of encrypted material

With regard to the treatment of encrypted material, there are some initiatives being developed involving the surveyed countries and others to extend international surveillance to encrypted message traffic.

2.4.2.2. France

Use of encryption

France has had substantial restrictions on the use of encryption. They were most clearly spelled out in the 1990 Telecommunications law. These restrictions primarily took the form of advance high-level approval or declaration requirements, accompanied by a certain degree of disclosure. Approval could only be granted for encryption used for authentication and identification purposes. The 1996 Telecommunications law lifted declaration restrictions for this form of encryption, and allowed encryption for confidentiality purposes to be provided by trusted third parties.

Trade restrictions

In view of her use restrictions, France has trade restrictions that go beyond her international obligations. Under the 1990 law, imports and exports (like use) of encryption products that can only be used for authentication or identification are subject to advance declaration; all other products require advance authorisation. The 1996 law will (when implemented) broaden the scope of the declaration requirement while reducing the range of products subject to authorisation. Before they may be traded between France and non-EU countries.

Protection of encrypted material

Since the use of encryption is tightly restricted, France has not formally addressed the legal treatment of encrypted material.

2.4.2.3. Germany

Use of encryption

Germany has not hitherto restricted the use of encryption. There was a public declaration to that effect in 1995; since then, there has been some public discussion, but no concrete legislative proposals.

Trade restrictions

Germany's position on trade restrictions is clearly spelled out in the Aussenwirtschaftsgesetz that regulates trade in dual-use commodities. This law essentially implements the EU regulation, prohibiting exports to nations that support terrorism.

Protection of encrypted material

The legal treatment of encrypted material is beginning to be discussed. In particular, access by authorities to the plaintext of encrypted documents and extension of wiretap laws to Internet communications have both arisen in public discussion. As with use restrictions, no concrete initiatives have surfaced to date, though the wiretap issue may be clarified in the anticipated revision of the 1996
Telecommunications law.

2.4.2.4. United Kingdom

Use of encryption

The United Kingdom has no formal use restrictions, but does have proposals that would ensure key recovery and government access for certain uses of encryption. One such area is the use of encryption to protect confidentiality of messages and records within the National Health System, whose policies encourage the use of a specific encryption technology that includes government access provisions. The other initiative in this area is the trusted third party proposal formulated by the Department of Trade and Industry. In its original form, this would establish licensing requirements for third-party providers of encryption services that include authorised key recovery. It cannot be precisely classed as a use restriction, since use of third parties would be optional. However, all third party providers would be required to comply with the license conditions. These proposals have attracted much commentary, and the new government has yet to revise or withdraw them.

Trade restrictions

In addition to its international obligations, the trusted third party proposals call for licensing of encryption software imports.

Protection of encrypted material

The legal treatment of encrypted material has been the subject of considerable discussion in recent years, following the passage of the Criminal Justice and Public Order Act 1994. This law formalised an extended the notion of 'interpretable silence.' It has been suggested that failure to disclose private keys or plaintext of encrypted messages could be the subject of judicial comment to the jury.

2.4.2.5. United States

Use of encryption

Use restrictions are very much an active subject for discussion and legislative initiative in the United States. The discussions, debates, etc. typically turn on the tension between the legitimate needs of law enforcement and national security on one side and Constitutional freedom of speech and privacy rights on the other. More particularly, the free speech discussion has raised the question of whether encryption is free speech or is an essential means of protecting free speech. The legislative initiatives (known collectively as the 'Clipper' initiatives in popular parlance) began by specifying use of particular hardware or software approaches that embodied government access. Subsequent proposals favoured key escrow/key recovery. Recently, attempts have been made to re-introduce guaranteed government access in the form of 'trapdoors' supplied by telecommunications and/or Internet service providers. To date, no such restrictions have been implemented.

Trade restrictions

The United States has had a series of export restrictions that went well beyond her international obligations, in terms of both the items covered and the nations involved. Strong encryption products were placed on an embargoed 'munitions list' of dual-use goods. These restrictions have been motivated in terms of national security, law enforcement and the economic interests of the United States. The original restrictions were expressed in the International Traffic in Arms Regulation and enforced by the State Department. After judicial challenge, similar restrictions were transferred to the Commerce Department. This was successfully challenged in the courts, though the underlying Constitutional questions remain unresolved. The legislature is considering various proposals that would ease export restrictions, such as the Leahy, SAFE, Pro-CODE, and McCain-Kerrey bills. The first three would relax export controls for various classes of publicly-available encryption software, while the latter would
relax controls for relatively weak encryption and key recovery encryption.

Protection of encrypted material

The issue of compelled key disclosure has arisen in the legal literature and a smattering of cases. In essence, the question reduces to Constitutional issues involving the Fourth Amendment's protection against 'unreasonable search and seizure' and the Fifth Amendment's privilege against self-incrimination on one side and the degree to which key production constitutes production of testimonial information.

2.4.3. Comparison

The following Table briefly summarises the positions of the countries on several broad issues. The Table is based on the material in the Country Summaries above.

Table 2.2. Comparison of encryption issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of encryption restricted</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Key escrow/recovery</td>
<td>No</td>
<td>Attempted</td>
<td>Proposed</td>
<td>Many attempts</td>
</tr>
<tr>
<td>Trade restricted*</td>
<td>Yes</td>
<td>As EU</td>
<td>As EU</td>
<td>Yes*</td>
</tr>
<tr>
<td>Compelled key disclosure</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Unclear</td>
</tr>
</tbody>
</table>

1. Beyond the CoCom/Wassenaar provisions.
2. Just struck down (see footnote 50), but still being enforced.

In general, France imposes the most severe restrictions on trade and use, though there are signs that these will be gradually eased. Germany has had much discussion but few concrete proposals due to deep differences of opinion and an apparent belief that unilateral national action is unneeded, inappropriate or likely to be ineffective. In the UK, the previous government attempted to encourage use of encryption products and services that provided government access. These encountered much resistance, though discussion continues and the new government’s position has not been clarified. There seems to be no active discussion of trade restrictions. While there is a legal basis for compelled disclosure of private keys or access to plaintext, it has yet to be tested. The US government continues its attempts to control the use and trade in strong encryption products, despite a series of adverse court decisions and waning public support. Compelling individuals to provide access to their own keys or plaintext has been opposed on Constitutional grounds, but remains possible, as does compelled disclosure by third parties. Recently, it has been suggested that government efforts to limit encryption owe more to fears of lost tax revenue than to fears of drug traffickers and terrorists.

---

68 E.g. C. Arthur Encryption - it's a case of use it or lose it, The Independent, 30 Sept. 1997.
3. DIGITAL SIGNATURES

3.1. INTRODUCTION

In the previous chapter, we discussed legal issues involved in coding of electronic communications for purposes of confidentiality. Here, we turn to legal issues involved in coding for authenticity and verification. First, we define different types of electronic authentication and ways of certifying the authenticity of documents. Second, we discuss the general legal setting and the legal issues that have been raised with respect to digital signatures. This is followed by arguments for and against legislative resolution. The last section concentrates on the current situation and debate in the surveyed countries. This requires a somewhat different structure. For each country, we describe the current legal status of digital signatures and separately discuss the two most prominent legal issues: the relation between electronic and written signatures and the legal position of certification authorities. We end that section with a comparison of the various countries' positions.

3.1.1. The Use and Nature of Digital Signatures

Signatures mainly serve to identify a person, to associate that person with a document, and to authenticate the signed document. In a legal sense, the signature means that the signer assents to the document having legal weight and binds himself or herself to the document.

Digital signatures are a form of encryption focussed on meeting some or all of the purposes of signatures. For the purposes of discussing both the issues and the legal approaches that have been adopted, it is useful to distinguish electronic signatures and digital signatures. An electronic signature is a collection of electronically-manifested symbols, executed or adopted by a party to a transaction in order to authenticate a writing. A digital signature is an electronic identifier that uses cryptographic or other electronic security methods to ensure authenticity, integrity and nonrepudiation of the associated document, data or information.

Much of the legal apparatus is oriented towards written documents with written signatures. Electronic documents are far harder to authenticate than traditional written documents, because of the virtual indistinguishability of copies from originals and the ease with which documents can be altered. On the other hand, digital signatures can offer, subject to the reliability and security of those who vouch for them, far higher levels of assurance and accuracy than written signatures.

Digital signing is a two key system: a private key is used to sign the message and a public key is used to verify the integrity and authenticity of the message. This integrity and authenticity is vouchsafed by a Trusted Third Party (TTP), who provides different services. A major function a TTP might perform is to act as a Certifying Authority (CA), issuing a certificate of authenticity with respect to a signature. Because TTPs and certificates are central to the legal position of digital signatures, we describe them in detail.

3.1.1.1. Trusted Third Parties and Certifying Authorities

As the electronic highway establishes connections between remote parties who may have little prior or sustained contact, the need for a reliable means of ensuring identity increases. Cryptography by itself is only part of the story; in situations where other means of ensuring trust are weakened, it may be necessary to involve trusted "neutral" third parties to mediate between the two primaries. In ordinary

---

commerce and other contractual matters, this role can be filled by banks, notaries, public escrow agents, etc. In the combined cryptographic and social protocols governing electronic transactions, the duties and liabilities of these new entities (TTPs) must be clarified to facilitate the spread of electronic commerce and avoid unnecessary litigation.

Critical distinctions can be made among TTPs depending on the extent to which they provide:

- registries of public keys
- issuance, verification and revocation of certificates authorities (CAs); and
- (private) key escrow; and/or key recovery.

The role of the CA is to issue digital signatures, and certify and revoke keys, timestamps and so on. The CA vouches for both the authenticity of the public key and the identity of the owner of the private key. The rights, duties and liabilities of TTPs in general and CAs in particular become an electronic highway issue because the proximity of the TTP to the transaction is itself a function of the new technology. For the purposes of this section, it is the CA function of TTPs that is most relevant.

In Internet commerce, moving value and ensuring secure communication are far more difficult than in face-to-face transactions. The parties neither know each other nor have any direct, real-time contact. This brings about problems about identity, eligibility, confirmation, agreement, and protection (against delays, misspecification, faulty goods and the like). In cases where the exchange is not simultaneous, or where money must be conveyed over the network, these problems may require the intervention of CAs for whom the duties and liabilities must be fixed. In a sense, sales of tangible goods over the Internet resemble mail-order or telephone sales, with the vital difference that mail or telephone help to fix the location, if not the identity, of the other party. The same cannot be said for email addresses. Commerce in information is even further from conventional sales. It often has the simultaneity of face-to-face transactions with an additional component of anonymity. After digital cash has been exchanged for information, there may be no record to allow either party to trace the other. While there may be legal means to safeguard the parties' interests in some cases, they are probably inappropriate to the many tiny transactions that may take place. These "nanotransactions" will become increasingly prevalent as the Internet moves from the initial academic/public good model with flat-rate pricing to a market-oriented model with usage- or content-based charges. The practical alternatives involve some mix of credit/debit cards and "electronic cash," and require attention to the legal issues

---

71 More generally, a CA issues digital signatures, certifies and revokes keys, maintains a registries of valid and revoked keys, timestamps communications, etc.

72 Key escrow/recovery services include key storage, recovery of keys or encrypted data, providing law enforcement access, etc.

73 In principle, applications such as IRC chat, Internet telephony or CUSEEME can provide real-time contact, but they are little-used for commercial activity. This distinction is recognised in par. 9 EU, Directive on the Protection of Consumers in Respect of Distance Contracts, 97/7/EC.

74 In principle, email addresses identify the sending machine. However, this does not necessarily identify the location of the sender of the mail (e.g. the client of the ISP or the user of an anonymous remailer). In some cases, security measures (e.g. firewalls) prevent the recipient from verifying the location associated with the email address. This issue has surfaced recently in connection with US encryption export controls; individuals using firewall systems (located in the US) that do not permit "reverse DNS lookups" have been refused access to encryption products on the grounds that their location "could not be verified." More specifically, the US District Court, in Reno v. ACLU 922 F. Supp., 1997, p. 845, said: "[a]n email address provides no authoritative information about the addressee, who may use an email "alias" or an anonymous remailer." More specifically, the US District Court, in Reno v. ACLU 922 F. Supp., 1997, p. 845, said: "[a]n email address provides no authoritative information about the addressee, who may use an email "alias" or an anonymous remailer."

75 For example, the use of credit cards or other instruments requiring sustained legal contact.

76 The "smart markets" and "Microcash" systems proposed for Internet pricing are good examples.
raised by the change in scale and the current liability limits for consumers in the first instance, and the
need for mechanisms to prevent respending and guard against money-laundering in the second.

One-shot, simultaneous exchanges may have less need for digital signatures as a result of the
intervention of conventional trusted third parties (credit card companies or banks) and clear liability
rules (e.g. caveat emptor) that recognise the difficulties of these transactions and clearly assign
responsibility (though perhaps not where it ought to lie on efficiency or equity grounds). Ongoing
transactions may have much stronger needs for authentication and identification: the party who first
tenders value needs assurance that the other party is who she claims to be and is authorised to do what
she proposes to do; if this assurance is provided by certificate, he needs further evidence that the
certificate is valid - this in turn means ready access to a CRL, which brings us back to the electronic
highway.

3.1.1.2. Types of Certificate

A certificate is a computer-based record issued by a CA identifying both the CA and the
"subscriber," containing the subscriber's public key and signed by the CA. It usually specifies the
steps the CA has taken to verify the subscriber's identity - higher specifications increase both the value
of the certificate and (potentially) the liability of the CA should things go wrong.

Certificates come in different forms for different purposes. We will look briefly at the types of
certificate, the issues involved in their use, and the Internet commerce activities where certificates can
contribute to solutions. At present, CAs offer four types of certificate.

• An identifying certificate binds a public key to a name. It can be stored on a computer or used in a
Smart Card for banking, obtaining government services, and other commercial transactions. After
creation, it can be published on the Web, given to the subscriber, or be released on email request.
It is not foolproof: the CA may not be reliable; the CA may have been misled; the subscriber's
private key may be compromised, etc. There are various ways to control these risks of which the
most critical is the Certificate Revocation List (CRL). This is a public registry of formerly-valid
certificates that have lapsed and should no longer be relied on. There are as yet no clear rules
about the duty to check CRLs, so those accepting certificates may adopt rules of thumb; these
may impose risks and costs of their own.

• An authorising certificate certifies other facts besides identity. It provides access control on the
electronic highway in the same way that, e.g., professional qualifications might. One pointed
example might be a certificate attesting to US citizenship that could be used to proscribe
"personal-use" export or download of strong cryptography in cases where the requesting
machine's location cannot be fixed with certainty. In this role, such certificates could help those
who make such software available minimise their legal or liability risk.

• A transactional certificate attests to some aspect of a transaction. It is a "one-time" certificate that
some fact or formality (e.g. a signature) was witnessed. In this way the witness' signature is bound
to that of the original signatory. The differences between a transactional certificate and a digitally
signed statement attesting to the fact are purely legal. First, the act of affixing a signature will
probably be a formal one in order to enable "recordation" even in cases such as Power of
Attorney or corporate share transfer where ordinary notary certification is not sufficient.
Moreover, such a certificate can add information (about the level of inquiry, time-stamping, etc.)
to the document. Finally, the liabilities associated with issuing transactional certificates are tighter
than those surrounding identifying certificates. This is because the nature of the reliance that third
parties place in the certificate is controlled by the CA.

---

77 The different status of these transactions on-line is recognised in Par 10 of Directive 97/7.EC (see
footnote 73 supra).
78 Not necessarily by name.
79 Not accepting undated certificates or those older than a certain date.
80 The American Bar Association is contemplating the creation of a "cybernary" legal speciality.
A time stamp proves that a document was in existence at a particular time. In general, it is easy to establish that a document existed after a given event (by referring to it); proof of earlier existence is much harder, but often of far greater legal importance. The legal standard for this proof is to cause an event based on the document that can be observed by others. This is expensive and compromises the individual’s privacy.

Each type of certificate helps solve a specific set of legal problems. Some of these are more acute as a result of the electronic highway; others can be dealt with more expeditiously by using certificates on the electronic highway. In order to do so, the legal problems faced by CAs will need solutions. Thus certificates can be regarded as a technical solution to certain legal challenges that needs legal help in order to work.

3.2. LEGAL ISSUES SURROUNDING ELECTRONIC AND DIGITAL SIGNATURES

The use of electronic and (especially) digital signatures is a critical part of the distant transactions characteristic of the electronic highway. The principal legal issues around electronic signatures are the extent to which they can be used in place of ordinary signatures, and the role of ancillary means for ‘verifying’ them. The role of TTPs, especially their legal status, is an important part of these issues, and will be discussed separately.

3.2.1. Uses and Verification of Digital Signatures

In the specific commercial application of digital signatures, the most vexed questions beyond the technical aspects of certification involve the legal system, jurisdiction, venue, choice of law and conflict of law problems relating to the relations between consumers, certification authorities, firms and (in some cases) third party providers of telecommunications, network, authentication, etc. services. Additional issues arise in identifying the appropriate role of government in solving problems unique to electronic authentication: data integrity; non-repudiation; evidentiary standards; choice of technology; liability standards; contractual freedom; consumer protection; and cross-border recognition of electronically signed documents.

The important caveat from a legal point of view is that access to private keys in a digital signature system, like access to encrypt/decrypt keys in a single-key system, allows the person with access to produce “perfect forgeries.” Even when no such forgery has occurred, the possibility can jeopardise the admissibility of digitally signed evidence or the reliance that contractual parties place on digitally signed documents.

One basic policy question is whether to establish minimum requirements for a signature that digital versions must meet or rules to encourage and validate more secure signature and authentication systems. In practice, digital signature legislation tends to follow one of four approaches:

1. **Electronic signature laws**: these laws simply stipulate that an electronic signature will be accorded the same treatment as a written signature.

2. **Criterion-based laws**: these laws establish security and trustworthiness conditions that

---

81 E.g., for statute of limitations purposes.
82 E.g., by publishing in a newspaper.
83 For example biometric verification in which the electronic signature is accompanied by a video or similar record of the individual in the act of signing.
84 E.g. they should be: i) unique to the user; ii) capable of verification; iii) under the user’s sole control; iv) inescapably linked to the signed document (so that changes in the document invalidate the signature); and v) consistent with appropriate law.
electronic signatures must satisfy before they can have the same legal effect as a written signature. Interestingly, these conditions establish higher standards for electronic signatures but do not grant them greater effect.

3. **Cybernotary laws**: these laws establish commissioning and licensure conditions for purveyors of electronic authentication services (CAs). Their certificates can have greater legal effect, and the CAs themselves may be protected from liability.

4. **Public-key infrastructure (PKI) laws**: these laws seek to create a specific regulatory and statutory framework for digital signatures, public key encryption and (sometimes) key recovery.

In the European context, it is important to take account of the differences between the legal concepts underlying signatures and requirements of form and procedure. These influence the type of law that may be passed and thus the recognition afforded electronic and digital signatures. The differences can be further analysed.

When the item in question is intended to serve as a declaration of intent, it may be argued that its delivery was sufficiently instantaneous as to undercut the imputation of deliberate intent. If electronic documents are regarded as fully binding, additional safeguards against hasty decisions and against disparities between the displayed and stored versions of documents may need to be added.

Since a digital certificate is actually bound to a private key rather than a physical or "moral" person, the possibility that the private key may be compromised or used in unauthorised ways constitutes a liability risk for the key holder and a risk of repudiation for those who rely on the signature. Here, it may be necessary to grant formal legal recognition to reliance limits attached to specific certificates.

For efficiency reasons, many documents incorporate other documents by reference. These other documents may need to meet requirements of form to ensure that they are fixed and reliable. References to unsigned electronic documents or information contained on unsigned Web pages may be insufficiently reliable to guard against legal effects other than those produced by their incorporation in the signed document.

Finally, ensuring legal equivalence between written and electronic signatures is complicated by differences in their characteristics. For instance, copies of electronic documents are indistinguishable from originals, which creates problems for civil law countries, which debar use of copies. Moreover, single legal entities can have more than one private key, while digital signatures for distinct documents are completely different, even if produced using the same private key. For these reasons, the legal treatment of these products is closely connected with the trustworthiness of the certification authorities who vouch for them.

3.2.2. **Liability of Certification Authorities**

The legal position of CAs remains unclear. As "new" parties to commercial transactions, there is broad agreement on the need to clarify their regulatory and liability position. The legal uncertainties, in particular fears of liability, may "chill" the use of such signatures except for large corporations making substantial transactions.

85 This is distinct from the common-law position that computer documents without direct evidence from their creators represent verbal evidence. See further discussion in Section 0 infra.

86 After setting the general framework in the Digital Signature Act, the German authorities still face the challenge of clarifying these legal issues.
The task of fixing liability for erroneous or false certificates is a difficult one at this point. Ultimately, legislation will be required if certificates are to move beyond the confines of large-scale commerce. Among the legal questions that must be resolved are:

- Are CAs selling a good, a service, or a mixture of the two? This affects the applicable law in most jurisdictions, especially as regards default rules, statutes of limitations, express and implied warranties and their disclaimer. In mixed cases, courts use various tests\(^{87}\) to set the applicable law and the results may be unpredictable. Even current efforts to extend the reach of commercial law to software products will not completely resolve this matter.

- What influence does the specific service have on liability? CA requirements could form the basis for a statement of their duties, and also provide both minimum and maximum liability for specific risks.

- What are the CAs liabilities with respect to undetected misrepresentation by the subscriber? In contract, the CA may be liable to the subscriber or another party such as the subscriber’s employer. The CA is probably not liable to the person defrauded or misled, but this certainly depends on the strength of privity in the relevant jurisdiction\(^{88}\). In tort, recovery would likely be based in breach of a duty of care or strict liability, though the terms of the contract do influence the tort if the CA specifies its level of inquiry. The legal problems arise as a result of differences in the duties expected of the CA and the limits placed on negligent misrepresentation. Some jurisdictions allow third parties to recover if their reliance was foreseeable, others require that the reliance be actually foreseen, while others require privity between the CA and the third party.

- Should CAs bear strict liability? Strict liability is generally imposed in sales of goods where an asymmetry of information exists, or for ultrahazardous activities. It also covers injury rather than economic loss. In the case of a faulty computer used to generate certificates, for example, one might claim for a design defect. This might be an attractive legal alternative in view of the absence of consensus on CA duties of care. Strict liability follows the good and requires no proof of fault. Various doctrines, such as the “least-cost-avoider” test have been used to assign strict liability.

- Should law protect or pre-empt contractual attempts to limit liability? The substance of this question is the extent to which this might undermine the advantages of certification, particularly in the case of closed legal relationships (see following section).

3.2.3. Legal Relationships in Certification

Transactions systems may be open or closed. An open system is one in which consumers will obtain a certification of identity from an independent CA and use that certificate in a wide range of transactions. By contrast, a system is closed if there exist a complete set of contracts specifying the rights and duties of all parties. This closure can come from a payment mechanism (credit cards, non-currency forms of “cybercash”). The buyer’s right to use a credit card is based on a contract between the cardholder and an issuing institution (e.g. a bank) which in turn has a contract with a card company. The card company also has a contractual relationship with the seller’s financial institution. The final link is provided by the sales contract between the buyer and the seller. This connection serves to define each party’s rights and duties and to allocate risk.

Conventional implementations of certification as portrayed in actual and proposed legislation are predicated on the open model, where there is no contractual relationship between the CA and the seller. The open system creates legal uncertainty and raises problems of liability and loss allocation, especially in situations where no (or more than one) party is at fault, or where there are sound public policy reasons for limiting one or more parties’ liability for loss. It also represents the situation where

---

\(^{87}\) E.g. the predominant factor, final product or separate portions tests.

\(^{88}\) Privity has recently been relaxed to some extent in the US.
the argument for government intervention is perhaps the strongest. Finally, it provides guidance for default rules to be used in the result of contract failure in a closed system. On the other hand, perhaps as a result of the intractability of these problems, relatively few firms have availed themselves of the opportunity to enter the open system and the closed model appears to be gaining ground. However, the jurisdictional problems and difference between legal systems alluded to above will undoubtedly force international arrangements, at least, to have some degree of openness.

Whether as a means of analysing proposed laws based on the open model, as a source of insight into the default rules that may evolve or a model for developing international arrangements, the open system remains a popular one for legal scholars 89 in this field.

The use of this model raises several concrete issues:

- What legal relationship 90 should link the CA and the consumer?
- What legal relationship should link the CA and the firm?
- How should losses be assigned as a function of the performance of each party?

Based on its comparison and analysis of national laws, the ILPF report (see footnote 121) argues that the legal relationships should be those shown in the following diagram:

![Diagram of legal relationships between CA, consumer, and firm.](#)

For the US, the tort would be negligent misrepresentation.

The argument is essentially that competition between CAs and the special role of the consumer sustain a contractual relationship, particularly since each party has fairly clear duties in respect of the other over a prolonged relationship. Defaults would be provided by statute law or (again, in the US case) by the Uniform Commercial Code 91 . On the other hand, the relation between the firm and the CA would probably not repay the investment of contract formation: the firm’s benefit from the contract is limited to the money paid by that particular CAs customers; and the firm may need to accept certificates from many CA, and to check their CRLs and verify the continued validity of their certificates over a sustained period. The negligent misrepresentation tort (where available) lets the CA internalise its costs without needing to impose large fixed transactions costs for contract formation; moreover, the CA is provided with incentives to avoid or limit liability by “reasonable behaviour 92 ” without being subject to moral hazard in the form of abusing the contract formation process.

---

89 E.g. Froomkin (1996) op. cit., Internet Law & Policy Forum op. cit.
90 I.e., what are the rights and duties of each party?
92 E.g. careful checking of consumer details, accurate representation of certificate levels, maintenance of CRLs, etc.
On the issue of loss allocation, the ILPF lay out candidate duties for each party, with the expectation that dereliction would attract liability. They are silent on the assignment of joint liability and the efficiency of their proposed rule. However, they do discuss the situation where a loss occurs despite the non-negligent behaviour of all parties. First, they believe that the need to encourage consumers to use CAs, coupled with the potentially unbounded liability they face creates a presumption that their losses should be limited. They cite the analogy of the US Electronic Funds Transfer Act of 1978 (EFTA) that limits consumer liability for lost or stolen credit cards (or credit card numbers) to $50.00. The "infant industry" argument is used again to justify the limitation of CA liabilities, at least until a secondary insurance market in CA risks emerges, at which point more risk should naturally fall on CAs in light of their ability to diversify and reallocate risk costs. This leave firms with the liability in the no-fault situation, a position that the ILPF justifies by noting that firms have superior information of the value of transactions, and can recoup their costs through the prices they charge consumers. They might also have noted that the firm’s exposure is less, an argument that arises in the context of analogous assignments of liability to telephone or mail-order merchants.

Even if consumers are negligent, the same arguments apply. The EFTA limits are not reduced by customer carelessness, and this position is backed up by general principles of consumer protection. Moreover, the consumer's duties are potentially complex and their liability unbounded. This could lead some substantial proportion of them to exercise "too much" care, under-use their certificates, or opt out of the system altogether.

3.3. ARGUMENTS FOR AND AGAINST LEGISLATIVE RESOLUTION

Do any of these problems need legislative resolution? The answer is not yet clear, but some issues can be mentioned on either side. On the pro-legislation side, law can clarify matters and reduce uncertainties that could cripple certification through underproduction or over-disclaimer. In particular, law can place efficient and equitable limits on CA liabilities, reducing the costs of insurance and the consequent likelihood of self-insurance followed by bankruptcy. If liability is to be fixed, the limits should be carefully crafted to balance protection against incentives - perhaps by being tied to negligence. Law may also be needed to provide continuity when a CA goes out of business with outstanding certificates; it may have no way and little incentive to recall its certificates, notify its former clients, etc. In the case of transactional certificates, the span of the certificate may be very long indeed - as long as the document it attests. Legislation can also serve consumer protection goals, by analogy with the licensing of notaries public. Because the electronic highway commerce to which they apply spans jurisdiction, legislation has the potential to reduce the need for duplicative litigation and the contracting uncertainties surrounding applicable law. Perhaps the strongest argument is that law could regularise the rights and duties of CAs, subscribers and third parties across jurisdictions and liability regimes. This may be of particular importance on the electronic highway where geographical location may not be observable or verifiable.

On the other side it may be too soon to craft adequate laws. On top of this, laws limit choices; they may go too far where the ultimate shape of the industry is so uncertain - it may even be that the combination of technology and market forces will resolve all these issues. In particular, the parties may self-select in ways that limit the chances of abuse. One way in which this could happen is through signalling strategies similar to those seen in warranty provision. A "good" firm may demonstrate this fact by taking on extra liability. Alternatively, a good firm may choose to "stake its reputation" on its

---

93 Either to reduce exposure or as a market response to high prices charged to cover insurance.
performance by reducing its liability, relying on word of mouth of exposed (and therefore motivated) customers.

Finally, legislation at the national level may create problems for the international harmonisation that seems a natural desideratum in view of the border-crossing nature of electronic commerce. There are currently no uniform international regulations regarding CAs or digital signatures94. This lack of legal certainty may create further problems in terms of mutual recognition, liability, etc. One proposed solution95 is the adoption of common requirements and a common legal framework for CAs covering: data protection; verification of user information; liabilities and insurance coverage; technical considerations; personnel security; and hierarchies of trust.

3.4. COUNTRY SUMMARIES

In this section, we will discuss separately for each country surveyed the current legal status of digital signatures, the relation between electronic and written signatures, and the legal position of trusted third parties (especially certification authorities). We close this section with a brief summarising comparison of countries.

3.4.1. France

3.4.1.1. Current Legal Status of Digital Signatures

A June 1996 report96 to François Fillon, Minister of Post and Telecommunications mentions seven propositions to develop the Internet in France. The fourth proposition “favoriser le développement du commerce électronique” mentions signature électronique:

**Proposition 4: Encourage the development of electronic commerce:**

Because of the formal nature of the protection they propose, current laws on electronic commerce seem to be difficult to reconcile with the instantaneous aspect of electronic commerce regarding intangible goods; consumer protection will be organised therefor less in a centralised and uniform way then through contracts and adapted technical mechanisms: it is necessary therefore to encourage the elaboration of standard contracts by professional organisations or the AFCEE (French association for Electronic Commerce and Exchange) to work for the recognition of the validity of an electronic signature, and to consider establishing a “sales tax” to be levied on the destination country so as to limit evasion apparent today in the commerce of intangible goods; it is necessary, finally, to accept the intervention of a TTP in transactions, this “Cybernotary” guaranteeing the solvency of the purchaser and that the vendor is honourable, providing the confidential service outlined in the new law on telecommunications regulations, making a transaction secure and keeping a record of it.

3.4.1.2. Relation between Electronic and Written Signatures

There is no law ruling directly the use of digital signatures and the validity of digital signatures in court. According to a French lawyer, digital signatures might be accepted as “commencement de preuve”. The French government isn’t planning anything on this subject, even though there are some MPs and senators who are raising questions about it.

---

94 Preliminary steps are described in Section 0.
96 Report written by and named for Mme Isabelle Falque-Pierrotin
3.4.1.3. Digital Signatures and Certification Authorities

The subject of trusted third party appears for the first time in the Law on Telecommunications of 1996. France was the first country to deal with this subject in law. The term is not mentioned explicitly in the text, but appears in the explanation of motives for the new law of the Ministry of Post and Telecommunications. While the law does not explicitly include the CA role of TTPs, it lays the foundation for such a role, and may be considered an example of a PKI-type law.

Art. 28 of the law, makes TTPs who manage private keys used to provide confidentiality on behalf of others subject to prior approval by the Prime Minister. They may not disclose information brought to their notice while carrying out their approved functions. TTPs are required to store the private keys they manage, and to send copies to legal authorities or to use them to fill appropriate official decryption requests. These requests may come either under conditions laid down in law n° 91-646 of 10 July 1991 (on the confidentiality of information transmitted by telecommunications networks) or within the framework of inquiries conducted under Chapters I and II of Title II of Book I of the Criminal Procedure Code. TTPs who disclose private keys to the public prosecutor conducting a criminal investigation shall inform users.

This law has the same goals as the Escrowed Encryption Initiative in the US\textsuperscript{97}; namely to provide users with high-quality professional encryption services while preserving government access for law enforcement or national intelligence purposes. A State Council decree defines conditions for approval of TTPs and sets out procedures and technical provisions required to fulfil their obligations. This decree has to be sent to the Conseil d'État for advice before coming into force.

At this time, it is not clear who the TTPs will be. It seems some companies with relations with the French military have already been chosen to serve as TTPs for the French government. Until the 26th July law is implemented, the old restrictions remain in place.

A November 1996 draft of the decree indicates the likely requirements for TTPs. The government (SCSSI) would authorise cryptography suitable for key-escrow and decide upon who can serve as a TTP. The TTP would have to be French. Users would not be allowed to use cryptography without first depositing keys with a TTP. Important issues such as international co-operation and liability are not addressed in the draft. The new government doesn't seem to be very preoccupied with the subject.

3.4.1.4. Summary

France has yet to take concrete steps to promote the use of electronic signatures, though the subject is being discussed. Developments on the digital signature front are also occurring slowly, and appear to be headed in the direction of a highly prescriptive approach to public key infrastructure.

3.4.2. Germany

3.4.2.1. Current Legal Status of Digital Signatures

Germany passed the first full Digital Signature Act (DSA)\textsuperscript{98}. In the wake of this law, the current discussion centres about:

\textsuperscript{97} Cf. p. 21.

\textsuperscript{98} This is Article 3 of the comprehensive Informations- und Kommunikationsdienstegesetz.
Table 3.1. German digital signature issues

<table>
<thead>
<tr>
<th>Topic</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal validity of digital signatures</td>
<td>No legal resolution yet</td>
</tr>
<tr>
<td>Development of technical standards</td>
<td>Initiated by law</td>
</tr>
<tr>
<td>Provision of security conditions/conditions in which digital signatures can be used securely</td>
<td>Main objective of the DSA</td>
</tr>
<tr>
<td>Position of CA/hierarchical structure of certifying</td>
<td>Resolved by law</td>
</tr>
<tr>
<td>Relationship with foreign certificates</td>
<td>Mentioned by law</td>
</tr>
<tr>
<td>A bit of data protection</td>
<td>Mentioned by law</td>
</tr>
<tr>
<td>Liability of TTPs</td>
<td>No legal resolution yet</td>
</tr>
</tbody>
</table>

3.4.2.2. Relation between Electronic and Written Signatures

According to the Bundesnotarkammer, electronic documents have a different legal status than written ones, because they do not meet the requirements of the Zivilprozessordnung (ZPO), "an expression of ideas which is embodied and identifiable/issued\(^\text{99}\)." In the academic world, this statement is not completely undisputed. Some legal scholars have stated that no change in law is required to provide electronic documents with the same status as written ones. However, the Bundesnotarkammer has stated that unless German law is changed an electronic contract should be deemed ineffective. In court electronic documents are not accorded the status of physical documents and are therefore treated as so-called visual evidence (Augenscheibeweiss). The DSA is rather ambiguous about the current status of digital documents. It says that it should be further examined whether there is a need to the change evidentiary law to comprehend electronic documents after there has been an evaluation of actual security of digital signatures. Where legal requirements explicitly demand written documents, it will be examined whether there are cases in which it would be instrumental to also accept digital documents.

Although the DSA is primarily aimed at providing the conditions for a secure infrastructure, a next step is to examine the legal validity of electronic documents. The German Ministry of Justice is currently doing exactly this. In a large number of German laws and regulations (almost one thousand), there are close to four thousand references to documents in written form. These references serve different and multiple legal purposes. For each, the ministry is examining whether the term "digital documents" can be added. Where this cannot be done without legal problems, alternatives are being investigated.

3.4.2.3. Digital Signatures and Certification Authorities

The German Digital Signature Act was accepted by the Bundestag in mid 1997 and took effect on August 1, 1997. Along with this law, a Digital Signature Ordinance was introduced. The Ordinance provides more specific elaboration of the general terms in the Act. In contrast to the legal developments mentioned above, the Act does not provide any clarification of the legal status of digital signatures. Their validity is not mentioned at all, nor is it addressed in the German Civil Code. However, the Federal Ministry of Justice has begun to address the legal effects of the use of digital signatures. The underlying thinking is that widespread and practical use of digital signatures requires an underlying infrastructure to issue unambiguous key pairs, assign an unambiguous encryption key to an identified person and make the public key certificates available to everyone.

The major objective of the Act is to create conditions that make forgery of digital signatures and falsification of signed data reliably noticeable. The Act sets out conditions for:

- Obtaining a license for certifying;

A license can be obtained by a higher federal authority indicated in Art. 66 of the Telecommunications law, which falls under the responsibility of the Ministry of Economic Affairs.

The requirements for obtaining a license are indicated in general terms and have to do with the organisation's reliability (i.e., compliance with legal requirements), expert knowledge (experience, qualifications) and further operational requirements (specified in the ordinance).

- Issuance of certificates (CA duties).
- CAs need to clearly identify the persons or organisations applying for certificates and to guarantee confidentiality of private signature keys.
- At the same time, CAs need to instruct applicants on the technical components and actions that contribute to a secure environment.

- Contents of the certificates.
- Each certificate should identify the name, the public key, the algorithm, the validity of the certificate, and the types of allowed applications.
- Time stamps do not have to be included automatically, but will be included upon request of the certificate owner.

- Data protection.
- CAs will provide data concerning the real identity of pseudonymous certificate holders to proper authorities upon request for reasons of criminal investigation; key owners will be notified of these requests as long as no other considerations (e.g., the progress of the criminal investigation) will be endangered.

- Design of the technical components that will have to support the secure use of digital signatures.

- Use of foreign certificates is allowed as long as they satisfy equivalent security conditions. The Act and the Ordinance are silent as to how these conditions can be met or who should evaluate them.

The law has been heavily criticised for providing the Bundesamt für Sicherheit der Informationstechnik (BSI) with a dominant position with respect to developing and evaluating technical standards. This limits, in the view of some critics, the opportunity for competition and emphasises the role of government too much. This, on its turn, could lead to limited confidence in the use of digital signatures.

3.4.2.4. Summary

The German Digital Signature Act of 1997 presently confines itself to drawing up CA registration and monitoring procedures to provide secure technical and administrative infrastructure requirements. Issues of liability are not touched upon yet. The Germans perceive this necessary condition to allow electronic documents to be used legal cases and to prevent an uncontrolled growth of procedures with a multitude of certified investigations in court.

3.4.3. United Kingdom

3.4.3.1. Current Legal Status of Digital Signatures

The UK has yet to adopt any legislation dealing with electronic or digital signatures or the role and duties of CAs. However, there has been extensive discussion of both issues, centred around two proposals circulated by the previous government.

3.4.3.2. Relation between Electronic and Written Signatures

The discussion of electronic signatures in policy terms has, so far concentrated on
communications between the public and the government. In November 1996, the government issued a green paper *Government Direct: A Prospectus for the Electronic Delivery of Government Services*\(^{100}\) that laid out its view of a more efficient, accessible, convenient and quicker way of providing information and other services. Chapter 8 of that document addresses the problem of identity, citing the combination of PIN numbers and bank records as a modern means of accomplishing a task (authorising payment) formerly assigned to signatures. The green paper proposes electronic signatures as a means of authorising provision of many sorts of services. These could either be incorporated in “Smart cards” or based on private memorised information. They further open up the possibility that the former approach could be broadened to cover a wide range of services, including private sector services and electronic payment. These proposals excited substantial comments from all sectors of the public\(^{101}\). In response to the question: “What are the implications of using electronic signatures in transactions with government?” the respondents cited various concerns. These include the need for an assurance of security; and adequate protection (of both parties) against fraud. It was felt necessary to provide alternatives, both in the form of written signatures and for emergencies that prevent use of Smart Cards or private keys. Several respondents cited the possibility of individuals being forced to surrender their Smart cards or reveal their private keys under duress. One consequence was a call for supplementary (especially biometric) means of verification. Another was a generalised concern for confidentiality and security of information. Many requested that guidelines be established and enforced before the system was privatised, and others pointed out that records of citizen dealings with government could be used in particularly intrusive forms of targeted marketing. These same concerns were cited in a general resistance to an expanded role for such Smart Cards. In particular, there seemed to be a general feeling that electronic signatures should not be required for basic information access.

3.4.3.3. Digital Signatures and Certification Authorities

The principal digital signature initiative in the UK is contained in the Department of Trade and Industry (DTI) proposals for a system of Trusted Third Parties to offer encryption and certification services (see footnote 39). On its face, this applies squarely to CAs; it requires licensing of all those who offer encryption services to the public (par. 18). Encryption services are broadly defined:

"Encryption services is meant to encompass any service, whether provided free or not, which involves any or all of the following cryptographic functionality - key management, key recovery, key certification, key storage, message integrity (through the use of digital signatures) key generation, time stamping, or key revocation services (whether for integrity or confidentiality), which are offered in a manner which allows a client to determine a choice of cryptographic key or allows the client a choice of recipients\(^{102}\)."

Of course, a CA does not need to hold private key material in order to certify a public key, but their function can be improved by doing so, particularly if the private key is used to validate the binding of identity. The proposals attempt to exempt this use of private keys:

"In terms of Key Recovery the proposed legislation is concerned solely with legal access to private encryption keys (which are used to protect the confidentiality of information) required by the authorities in connection with the lawful interception of communications (i.e. information on the move) or for lawful access to data stored and encrypted by the clients of licensed TTPs. There is, of course no intention for the Government to access private keys used for only integrity functions. Legal access to encryption keys will be

---


\(^{102}\) Sec. VI, par. 38.
permitted through serving warrants on TTPs."

This distinction is a nice one; CAs may be able to occupy only a very narrow market niche.

The proposals take a broad view of territoriality: they try to bind all firms offering encryption to members of the UK public, and envisage "key exchange" with complying foreign governments:

"Although the legislation will require foreign TTPs offering or providing encryption services to clients in the UK to have a registered base in the UK (which will allow for the licensing of non-UK bodies with no trading presence in the UK), there will be no provision requiring UK clients to use a UK licensed TTP. They are, and will be, free to register with foreign TTPs. It will therefore be necessary (for law enforcement purposes) to establish arrangements with other countries for the exchange of keys. The UK Government believes that these arrangements will be on the basis of dual legality."

The proposals also include a section on digital signatures per se (par. 10-13 and Annex A) that raises the issue of what would be required to ensure that digital signatures meet the requirements of form in contract and statute law. Annex A cites the Society for Computers and Law Working Group, which found that, while many words (e.g., "information," "document" and "recording") could be extended to electronic analogues, "signature" and "writing" could not. For existing laws, the Working Group suggested altering the Interpretation Act (the government rejected this as too complex). The other approach would be piecemeal amendment of existing laws, but the identification and analysis of all occurrences of these terms is surely a daunting task. Therefore, the government asked (par. 13) whether contract law would provide a reasonable short-term expedient - presumably, this invokes a more-or-less closed model. Reassuringly, the Working Group's recommendations are broadly compatible with the United Nations Commission on International Trade Law (UNCITRAL) model law.

The proposals further question whether admissible digitally-signed documents could be relied on in court, and the utility of a rebuttable presumption of identity and integrity. This discussion emphasizes the benefits of legislative certainty and official licences over private relationships of trust. Interestingly, almost all comments on the proposal reject these benefits, seeing little or no business need for licensed CAs (or, in some cases, any TTPs at all).

The Notarial Forum points out that self-regulation works reasonably well for non-digital providers of authentication services. They also raise the following substantive objections:

- The proposed extension of liability to providers of encryption services outside the UK and the procedures for "key exchange" with complying foreign governments raise serious problems of enforceability and territoriality.
- The definition of encryption services (cited above) implies a choice of recipient, suggesting that no licensing is required where clients do not choose recipients (the open model again).
- The difference between "providing" and "using" encryption services may be more illusory than real and the Forum is concerned that no reference is made to archiving of encrypted material.
- The requirement for dual legality could prove to be a significant hindrance to the competitiveness of UK business to deal with the global market.
- Warrants for access should be issued by a court rather than the Secretary of State.
- Private encryption keys should be defined in such a way to make it clear that they are incorporeal, personal or movable property, and as such capable of being stolen, with the resultant liability to criminal and civil sanctions.
- Liability should be assigned on the basis of fault rather than the strict liability proposed by the

\[103\] Sec. VI, par. 5.
\[104\] Sec. VI, par. 55.
\[105\] See references at footnote 40.
This position was endorsed by Akdeniz et al (see footnote 105), who see both US and UK proposals for key recovery as a source of new risks, new complexities, new costs and new targets for key attack. They develop an alternative proposal called "key archiving" to permit free development of the TTP/CA industry without the need for artificial distinctions (e.g. between keys used for identity, authentication and privacy) or identifications (e.g. of TTPs/CAs with escrow/recovery agents). The proposal rests on the idea that users will wish to archive their keys in order to facilitate information and fund exchange with strangers and to guard against loss or destruction of their personal copies. The significant difference is that the archived key could only be recovered from the TTP after it has been invalidated (e.g. via a CRL) against all subsequent use\textsuperscript{106}. This provides twin benefits: letting users know in an unambiguous and timely fashion when their keys have been revealed, and limiting the risk of forgery due to key compromise. The knowledge and assurance may limit the actual or anticipated abuse of the system by unauthorised persons, and reduce the likelihood of attack on the TTP.

3.4.3.4. Summary

Electronic signatures in the context of communications with the government are being actively discussed, but to date no concrete legislative proposals have emerged and the new government has yet to respond to the comments on the green paper. The digital signature and TTP (CA) proposals go into more detail on the legal status of electronic signatures (which are referred to as digital signatures), but primarily in the context of an envisaged PKI system with substantial key recovery properties.

3.4.4. United States

3.4.4.1. Current Legal Status of Digital Signatures

We distinguish between state laws and federal laws because a variety of US states are pursuing parallel initiatives. This constitutes a highly-relevant "natural experiment" that will be worthy of close comparative study as the results unfold. A large number of overtly experimental initiatives establish study groups or task forces to investigate digital signatures, and often include provisions for the government to act as a CA. They include:

- 1997 Connecticut S.B. 1308 studies the use of digital signatures, including creation, signer authentication and digital verification, and the relationship of such processes to the legal concept of signature;
- Florida "Electronic Signature Act of 1996" authorises the use of electronic signatures for signing writings electronically, authorises the Secretary of State to be a certification authority for the purpose of verifying digital signatures, and requires a study of the use of digital signatures for commercial purposes;
- 1997 Georgia S.B. 103 provides that any person "may, but shall not be required to" accept or agree to be bound by an electronic record executed or adopted with an electronic signature, and further provides that where a person agrees to be bound by an electronic record executed or adopted with an electronic signature, then applicable writing and signature requirements shall be deemed satisfied - also sets up study group;
- Hawaii Rev. Statutes, Chapter 601 sets up group to study electronic filing of court documents;
- 1997 Maryland H.B. 1386 establishes a task force on digital signature law;
- 1997 Nebraska Legislative Resolution 262 provides for a study of issues surrounding the enactment of digital signature legislation;

\textsuperscript{106} Practically, a "notice of revocation" generated for the public key is required to access the archived copy of the private key.
• 1997 North Carolina House Bills 290 and 1047 establish legislative studies commission on electronic commerce and information technology that affects public policy;
• 1997 North Dakota Senate Concurrent Resolution 4024 directs legislative council to study the development of an electronic mail and records management policy for governmental entities, includes digital signatures;
• Oklahoma House Bill 1690 creates task force on Electronic Signature Technology; and
• 1997 Virginia House Bill 2138 establishes Joint Commission on Technology and Science.

On the federal level, the National Conference of Commissioners on Uniform State Laws is studying electronic commerce legislation, but the NCCUSL Scope and Programs Committee decided in January 1997 that it was too soon to begin work on a uniform digital signature law. The government plans to revise the Digital Signature Standard (FIPS 186). The draft Electronic Data Security Act of 1997 aims for:

"the development of a key management infrastructure for public-key-based encryption [...] that will assure that individuals and businesses can transmit and receive information electronically with confidence in the information’s confidentiality, integrity, availability, and authenticity, and that will promote lawful government access."

Under the Act, the Secretary of Commerce will be authorised to register CAs and issue CA regulations in order to enable disclosure of encrypted messages in case of criminal investigations and prosecutions. The US Food and Drug Administration (FDA) has also implemented regulations for Electronic Records and Electronic Signatures as of 20 March 1997.

Finally, the American Bar Association has been studying the issue of digital signatures. They have produced published a draft digital signature law107.

3.4.4.2. Relation between Electronic and Written Signatures

The bulk of the 94 state laws, pending bills and draft laws we found fall into this category. Rather than list them separately, we will simply describe an example, California Government Code Section 16.5 (1995). This statute governs only electronic signatures affixed to communications with public entities. The Act provides that any party has the option to use or accept an electronic signature (called a “digital signature” in the statute), which shall have the same force and effect as a manual signature if: (1) it is unique to the person using it; (2) it is capable of verification; (3) it is under the sole control of the person using it; (4) it is linked to data in such a manner that if the data are changed, the digital signature is invalidated; and (5) it conforms to regulations adopted by the Secretary of State.

3.4.4.3. Digital Signatures and Certification Authorities

Within this area, there are both Cybernotary laws and more ambitious PKI laws. The Cybernotary laws that govern the commissioning of authentication service providers.

• 1997 Florida House Bills 957 and 1413, Senate Bill 998 authorises the Secretary of State to provide commissions for notaries public to perform electronic notarisations, establishes a voluntary licence program for private certification authorities and commissions international electronic notaries. It includes rules to provide: (a) licensing fees; (b) standards and requirements for licensing; (c) audit procedures; (d) insurance reserve or bonding requirements; and (e) procedures for license revocation and suspension.
• 1997 Georgia House Bill 479 provides for electronic notarisation of tax returns.
• 1996 Utah Senate Bill 188 and 1997 Utah House Bill 95 contain provisions relating to notary publics - e.g. that a notary’s acknowledgement on an electronic message or document is considered complete without the imprint of the notary’s official seal if the message has been

107 The Spring 1998 issue of Jurimetrics will be devoted to this and related digital signature issues.
digitally signed in the presence of a notary, and the notary signs the acknowledgement with a digital signature.

- Virginia Senate Bill No. 923 is a limited digital signature statute that provides legal recognition for digital signatures and allows digital signatures to serve in place of notarised or acknowledged signatures when filing documents with executive government agencies.

Public Key Infrastructure (PKI) bills are more ambitious in scope. The first such bill was the Utah Digital Signature Act of 1995\textsuperscript{108}, which provides a legal framework for the use of cryptography for authentication and integrity purposes. The Utah Act's stated goals are: (1) to facilitate commerce by means of reliable electronic messages; (2) to minimise the incidence of forged digital signatures and fraud in electronic commerce; (3) to implement relevant standards, such as Standard X.509 of the International Telecommunication Union; and (4) to establish uniform rules regarding the authentication and reliability of electronic messages.

Under the Utah Act, a government agency assumes the role of “top level” CA obliged to make policy, facilitate implementation of digital signature technology, and exercise regulatory oversight. While licensing is voluntary; licensed CAs are offered certain legal benefits that amount to a “safe harbour against much liability. The same legal benefits may be provided to CAs licensed by other jurisdictions if their regulations are substantially similar to those in Utah.

CA Duties. Prior to issuing a certificate, the CA must confirm that: (1) the prospective subscriber is the person to be listed in the certificate; (2) other certificate information is accurate; and (3) the subscriber is entitled to hold the corresponding private key. Neither the CA nor the subscriber can waive these requirements. Issuing a certificate constitutes a warranty to the subscriber that the certificate contains no information the CA knows to be false and that it satisfies all material requirements of the Utah Act. These warranties cannot be limited or disclaim. The CA further certifies to all who reasonably rely on its certificates that the information in the certificate is accurate and that the subscriber has accepted the certificate.

Subscriber Duties. By accepting a certificate, a subscriber certifies to all who reasonably rely on the certificate that he lawfully holds the corresponding private key and that all representations made by him to the CA or otherwise incorporated into the certificate are true. Subscribers are obligated to indemnify CAs for loss or damage caused by issuing certificates in cases of: material misrepresentations of fact by subscribers; or subscribers’ failure to disclose material fact if done intentionally to deceive the CA or a person relying on a certificate or negligently. This obligation cannot be disclaimed or contractually limited. A subscriber also assumes a duty to exercise reasonable care to retain control of his private key and prevent its disclosure to any person not authorised to create the associated digital signature.

CAs are not liable for any loss caused by reliance on a false or forged digital signature if they comply with all material requirements of the Act with respect to the false or forged digital signature. This immunity can be waived by the CA. Licensed CAs are not liable in excess of the amount specified in the certificate as the recommended limit for loss caused by reliance on a misrepresentation in the certificate of any fact that the licensed CA was required to confirm. Licensed CAs are liable for direct compensatory damages and not for punitive or exemplary damages, damages for lost profits or lost opportunity, or damages for pain and suffering.

If reliance on a digital signature is “not reasonable under the circumstances,” the recipient of that digital signature assumes the risk that digital signature is forged.

\textsuperscript{108} The Utah Act contains conditions for Cybernotary licensure and much more besides.
Several evidentiary presumptions arise under the Act. A certificate digitally signed by a licensed CA and published in a recognised repository or made available by the issuing CA or by the listed subscriber is presumed to have been issued by the CA which digitally signed it and accepted by the subscriber listed in it. The information listed in a valid certificate and confirmed by a licensed CA issuing the certificate is presumed to be accurate. A digital signature is presumed to have been created before it was time-stamped by a disinterested person utilizing a trustworthy system. Finally, a digital signature verified by the public key listed in a valid certificate issued by a licensed CA is presumed to:

- be the digital signature of the subscriber listed in that certificate; and
- have been affixed by the signer with the intention of signing the message.

A recognised repository, or its owner or operator of a recognised repository, has a waivable immunity from liability for failure to record certificate suspension or revocation for one business day after notice was received. Otherwise, the repository may be liable for direct compensatory damages for a person who relied on a revoked or suspended certificate, up to the recommended reliance limit on relevant certificate. Repositories are not liable for misrepresentation in certificates published by a licensed CA.

The Utah statute sets evidentiary presumptions against private key holders and grants statutory liability limits in favour of certification authorities. Regulations to be promulgated by the state government must conform to a detailed set of standards. Utah was the first state in the nation to pass legislation that provides for licensing of CAs. The Utah legislation takes a highly prescriptive and regulatory approach in an attempt to facilitate electronic commerce. More recent legislation does not make particular technologies necessary for legally enforceable electronic signatures, and tends not to create statutory government intervention in liability apportionment between parties or set evidentiary presumptions. Serious questions have been raised as to whether legislation should be less detailed, more technologically neutral, less pro-industry by giving away liability limits to certification authorities, and impose lighter burdens and risks on the consumer. Excellent summaries of these initiatives can be found on the Web.

3.4.4.4. Summary

Overall, about 40 states have considered or enacted electronic signature laws, but most have been narrow in scope. Twenty-one states have proposed laws covering both public and private sector communications, but only ten states have enacted such laws. Most laws (twenty-three states) apply only to communications with or within government or narrow types of private sector communication. The breakdown of these initiatives by type of law is:

---

109 Many jurisdictions have considered this approach, only one other state (Washington) has adopted such legislation to date.


111 E.g., use of electronic signatures by health care providers.

112 Table based on Gidari, A. and J. P. Morgan op. cit. and material available online (see footnote 110).
The first and most comprehensive of the CA laws was the Utah Digital Signature Act. It lays down very specific conditions for CA licensure, and provides in return a safe harbour against most types of liability. However, it does not specify liabilities for unlicensed CAs. Perhaps as a result of the remaining legal uncertainties and the stringency of the conditions, to date Utah has no licensed CAs.

Overall, the trend seems to be away from Cybernotary laws, or at least towards laws that avoid specifying technologies or mandating public key systems. The only laws to address mutual recognition issues were the Cybernotary laws, which placed stiff requirements on the originating state. Choice of law and forum issues have not really been addressed.

3.5. SUMMARY AND COMPARISON

We begin with a summary discussion that highlights the answers to research questions 1-3. The first part, "Issues Arising," answers the first research question, while the second, "Initiatives," sketches the answers to the second two questions, describing legislation and other initiatives. The section concludes with a short comparison of the surveyed countries.

3.5.1. Issues Arising

In principle, the issues raised by the emergence of digital signature technology and the growth of electronic commerce and other forms of interaction that rely on it can be divided into broad categories, such as:

- The distinctions between written and electronic documents and between electronic and digital signatures;
- The legal position of certification authorities, including the type of regulation to adopt and the associated rights, duties and liabilities;
- The changing nature of the legal relationships between those who provide, certify and rely on digital signatures;
- The relative merits of specific legislation, general regulation and self-regulation and the appropriate timing for legislative initiatives in a rapidly-developing field; and
- The consequences of the international scope of the interactions supported by electronic and digital signature technology, including provisions for mutual recognition.

In light of the rapid evolution of technology and practice in this area, current discussions and initiatives in the surveyed countries divide the issues along somewhat different lines. Moreover, it is appropriate to recognise that many of the existing and proposed initiatives represent 'natural experiments' and attempts to forestall future problems by providing certainty rather than 'solutions' to existing problems. It is convenient to divide the discussion into two parts.

- The status of electronic signatures that accompany electronic documents as substitutes for written signatures on written documents involves re-examination and, in some cases, modification of a wide range of existing laws.
- The legal status and position of digital signatures and other certificates, and the role and status of licensed and unlicensed certification authorities refers to substantially new forms of interaction, legal relationships and transactions.
With regard to the first of these it is also appropriate to note here a systematic difference between civil law and common law countries regarding the standing of electronic documents. Roughly speaking, in civil law countries, where the requirements for documentary evidence are laid down in rules for conduct of transaction and treatment of documents, potential problems arise from the fact that electronic signed documents are *ipso facto* copies - the general rule is that documentary evidence submitted in advance should take the form of a signed original, stored until the window of opportunity for litigation or official inspection has closed. There are exceptions to this rule for small transactions, or in cases where the parties agree in advance to some other form of contract and record. In addition, France allows verbal evidence if it is impossible for one party to get a written copy of the contract. However, no exceptions are allowed for consumer credit or insurance transactions.

In common law countries, special standing is given to verbal evidence; it is only accepted from those having first-hand knowledge of the subject matter. By the same token, documents are classed as *hearsay* unless witnessed by their authors. For instance, under the UK’s Civil Evidence Act 1968, a computer document may be admitted if the creator testifies to direct knowledge of the data it contains. Likewise, the requirement of the *Best Evidence Rule* that only originals are admissible unless they are unavailable can be met for documents for which there effectively is no original. However, this position remains to be clarified.

### 3.5.2. Initiatives

#### 3.5.2.1. International

International attention to the issue of electronic signatures to date tends to combine the electronic document and digital signature aspects. The United Nations Commission on International Trade Law (UNCITRAL) has produced a paper that lays the groundwork for a future electronic signature agreement. More recently, a report to the European Commission outlined some of the legal issues surrounding a pan-European system of trusted third parties and made suggestions for a draft agreement. This was followed by a Communication that followed-up the Bonn Ministerial Declaration to develop a policy framework for digital signatures, with particular emphasis on the development of markets for cryptographic services and products. It traces the weakness of the market to legal uncertainty surrounding the status and uses of these technologies as a result of the absence of common requirements and clear liability rules for certification authorities, and common technical specifications and legal recognition for their products. The emerging OECD standard and attention being paid to varied national experiences suggest that an international solution may emerge at some point. These efforts are still in their early stages and were not closely reviewed in this study.

---


114 *Civil Code Article 1348*.


117 "Towards a European Framework for Digital Signatures and Encryption"

3.5.2.2. France

Current Status

Current policy and political discussions have expressed interest in providing formal recognition for electronic signatures and establishing a trusted third party/Cybernotary infrastructure. The 1996 Telecommunications Law contains some preliminary steps in this direction.

Electronic Documents and Signatures

France is a civil law country, and so withholds recognition from electronic signatures on the grounds that they are copies. To date, there are neither plans nor specific laws to change this situation, although the issue is beginning to be discussed.

Digital Signatures, Certificates and Certification Authorities

The 1996 Telecommunications Law sets out some initial steps towards the creation of an infrastructure of trusted third parties that could, inter alia, provide certification and digital signature services. Specifically, it limits the role of such entities as providers of confidentiality services, establishes their duties of disclosure to government authorities and information of users. The law also tries to establish a role for certification authorities who do not provide confidentiality services and suggests, in line with the overall policy on encryption, that they would not be subject to these duties.

3.5.2.3. Germany

Current Status

Germany is a civil law country, and does not afford electronic documents the same status as written ones. The official position is that the security of such documents needs to be established before their evidentiary weight can be re-examined. Germany has recently enacted a Digital Signatures Act that establishes minimum conditions for secure use of digital signatures and lays out the role and hierarchical structure for certification authorities.

Electronic Documents and Signatures

As noted, electronic signatures are currently unacceptable. The Digital Signature Act takes an ambiguous position, since it merely concentrates on the conditions under which the security of electronic documents could be re-examined. At the same time, an inventory of references to written documents is being conducted.

Digital Signatures, Certificates and Certification Authorities

While the new Digital Signature Act does not address the legal standing of digital signatures and other certificates, it does lay out licence eligibility, terms and duties of certification authorities. It also establishes conditions on the necessary contents of certificates and provides for data protection and mutual recognition. The law has proven controversial, not least because it is viewed as specifying a central role for government information security officials in developing and implementing technical standards.

3.5.2.4. United Kingdom

Current Status

The United Kingdom is a common law country, and requires personal confirmation of electronic and computer-generated documents. Both electronic documents and digital signatures have been discussed, and proposals touching on each have been circulated.

Electronic Documents and Signatures

In the area of electronic documents, the general discussion centres on the degree to which it is appropriate to: a) modify existing laws by changing their wording to refer specifically to electronic
signatures; b) use the Interpretation Act to change the meanings of terms currently held to imply written
documents or signatures; c) pass new laws according separate status to electronic signatures; d) 
consider the issue on a case-by-case basis; or e) rely on specific contracts, at least in the short run. One 
specific initiative envisages extensive use of electronic documents and signatures for dealings between 
citizens and government. General conditions under which electronic signatures would meet 
requirements of form in contract and statute law are contained in the Department of Trade and 
Industry’s proposed Trusted Third Party Regulations, identifying specific terms that could be extended 
to electronic counterparts, and those that could not.

Digital Signatures, Certificates and Certification Authorities

The proposals for electronic communications between citizens and government make explicit 
provision for forms of digital certification (as well as Smart Cards and other emerging technologies). 
More generally, the Department of Trade and Industry’s proposed regulations establishing a Trusted 
Third Party infrastructure describes a framework within which digital signature certificates would be 
regulated as one aspect of the licensing of providers of broadly-defined “encryption services.” 
However, the main thrust of the proposals is directed towards key recovery, and particularly recovery of 
keys used for confidentiality purposes. The part of the proposals that deals with digital signatures per 
se, in addition to making proposals regarding the treatment of electronic signatures, favours legislative 
certainty over private solutions to questions of reliance on admissible documents and fairly 
unambiguous liability assignments. This part of the proposals has been almost uniformly condemned.

3.5.2.5. United States

Current Status

The United States has a rich assortment in the several states of enacted and proposed digital 
signature laws, varying widely in purpose, coverage and legislative approach. There have been a few 
limited initiatives at the Federal level, but these are primarily concerned with specific communications 
between citizens and the government. As with the UK, there is a tendency at the national level to 
combine approaches to this area with initiatives aimed at resolving problems with encryption used for 
confidentiality purposes.

Electronic Documents and Signatures

Among the many state laws concerned with the legal treatment of electronic signatures, most lay 
down mild requirements for them to be accorded “equal treatment.” In some cases, the laws lay down 
conditions of uniqueness, verifiability, control, connection to signed documents and compliance with 
other regulations. If these conditions are satisfied, these laws makes no further distinction between 
written and electronic signatures. In other cases, the treatment of electronic signatures is further 
restricted to certain legal functions - either by limiting their validity to specific transactions or by 
stipulating that they can be relied on only for certain purposes or up to certain limits.

Digital Signatures, Certificates and Certification Authorities

Among the digital signature/CA laws, there is again a wide spectrum of approaches. On one side 
are detailed prescriptive laws governing licensing and operating conditions for CAs in exchange for 
immunity from certain liabilities. These laws also set stiff conditions for mutual recognition. On the 
other end are more flexible laws establishing very general conditions for use and provision of digital 
signature services and CA liability and duties. The recent trend seems to be towards the more flexible 
approach.

3.5.3. Comparison

The surveyed countries are approaching the issue of electronic and digital signatures from
different directions and at different rates. In addition to the national initiatives, there are signs of international developments. The United Nations Commission on International Trade Law (UNCITRAL) has produced a paper\textsuperscript{119} that lays the groundwork for a future electronic signature agreement. More recently, a report to the European Commission\textsuperscript{120} outlined some of the legal issues surrounding a pan-European system of trusted third parties and made suggestions for a draft agreement. The emerging OECD standard and the attention being paid to the national experiences\textsuperscript{121} suggest that an international solution may emerge at some point. These efforts are still in their early stages and were not closely reviewed in this study.

One significant observation with regard to the surveyed countries is that the legal status of electronic documents (and thus of the electronic signatures attached to them) differs between civil and common law countries.

Roughly speaking, in civil law countries, where the requirements for documentary evidence are laid down in rules for conduct of transaction and treatment of documents, potential problems arise from the fact that electronic signed documents are \textit{ipso facto} copies - the general rule is that documentary evidence submitted in advance should take the form of a signed original, stored until the window of opportunity for litigation or official inspection has closed\textsuperscript{122}. There are exceptions to this rule for small transactions, or in cases where the parties agree in advance to some other form of contract and record. In addition, France allows\textsuperscript{123} verbal evidence if it is impossible for one party to get a written copy of the contract. However, no exceptions are allowed for consumer credit or insurance transactions.

In common law countries, special standing is given to verbal evidence; it is only accepted from those having first-hand knowledge of the subject matter. By the same token, documents are classed as \textit{hearsay} unless witnessed by their authors. Under the Civil Evidence Act 1968, a computer document may be admitted if the creator testifies to direct knowledge of the data it contains. Likewise, the requirement of the \textit{Best Evidence Rule} that only originals are admissible unless they are unavailable can be met for documents for which there effectively is no original. However, this position remains to be clarified.

The following Table briefly summarises the positions of the countries on several broad issues.

Table 3.3. Comparison of digital signature issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic signatures</td>
<td>Little interest</td>
<td>Not resolved</td>
<td>Green paper, case law</td>
<td>State laws, federal study</td>
</tr>
<tr>
<td>Separate CA legislation\textsuperscript{1}</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>State laws, federal study</td>
</tr>
<tr>
<td>PKI/TTP legislation\textsuperscript{1}</td>
<td>Yes</td>
<td>No</td>
<td>Proposed</td>
<td>Many attempts</td>
</tr>
</tbody>
</table>

1. This may bundle escrow agents and CAs together.


\textsuperscript{121} A recent report by the Internet Law & Policy Forum, \textit{The Role of Certification Authorities in Consumer Transactions}, April 1997, available at http://www.ilpfl.org, contains a detailed analysis of the legal issues surrounding the creation of a public key infrastructure and a detailed survey of international law.

\textsuperscript{122} UNCITRAL, \textit{Electronic Data Interchange: preliminary study of legal issues related to the formation of contracts by electronic means}. Report of the UN Secretary-General, 23rd Session, June-July 1990.

\textsuperscript{123} \textit{Civil Code Article 1348}. 
France appears to be proceeding slowly in regularising the use of electronic signatures, though there are policy declarations of the importance of electronic and digital signatures to the development of electronic commerce. The more advanced capabilities of digital signatures do not appear to be actively pursued in pending legislation, except as part of the overall approach to establishing a public key infrastructure. In this area, France continues to maintain a more restrictive policy than the other surveyed countries.

Germany, too, has yet to formalise the status of electronic signatures. However, they passed the earliest national digital signature law, which combines the CA and PKI approaches and is viewed as a necessary precondition to determining conditions under which electronic and digital signatures can have legal force.

The UK has yet to produce concrete legislative proposals regarding electronic signatures. There is a proposed public key infrastructure initiative. Both the electronic signature discussion in the Government Direct green paper and the proposed TTP legislation have engendered lively debate.

The individual US States are experimenting with a wide variety of approaches to electronic and digital signatures. The trend appears to be away from prescriptive approaches towards a more flexible structure. The most common enacted laws simply provide legal force for electronic signatures, often for restricted types of communication. Specific federal action appears to be slow on both fronts: only modest steps have been taken towards a homogeneous national digital signature law, and attempts to pass PKI/TTP legislation are stalled by public and judicial resistance to the key recovery and export restriction provisions.
4. PERSONAL DATA

4.1. INTRODUCTION

The collection and use of personal data has become a very sensitive topic in recent years. The technological drivers behind the emergence of these issues include the availability of faster, more powerful, networked computers. When the data protection laws in each of the surveyed countries were first drafted, computers were relatively slow and isolated, so the potential for abuse of personal data was relatively low. In recent times, these “hardware” developments have been complemented by the emergence of powerful techniques for database management and, more importantly, data matching and data sharing. The value-added by personal data beyond the immediate needs of the transaction has increased substantially relative to the costs. While personal data may not appear to have a direct connection to the electronic highway, it is certainly far easier to collect such data in the course of electronic transactions, and the costs of reusing such data in that context are smaller and the benefits to the user larger than in conventional media. In addition, the advent of “open government” initiatives in which public bodies exchange data with one another and the general public and provide services over the electronic highway creates a greater need for the collection and storage of these data.

The following part of the introduction provides some background and contextual information, followed by a discussion of the legal issues. This discussion focuses on the principles governing personal data, subject rights, and other legal problems that are beginning to surface, particularly the issue of transborder data flows. The discussion of these issues, especially the latter, primarily take place in the context of the European Union. All EU member states will have implemented the Personal Data Protection Directive\(^{124}\) (PDPD) by the end of 1998\(^{125}\). Because of this dominance, special attention will be paid to this directive in the country summaries section.

4.1.1. Background

Data matching\(^{126}\) is of particular importance, both as an activity that looks set to grow rapidly and as a potential loophole in the current data protection structure. The term covers comparisons of individual-level data to check for errors, unusual changes or patterns and side-by-side comparisons of aggregated or anonymised data sets to identify emerging trends, anomalies, duplicates, etc. These developments open up new public and private possibilities for exploiting personal data.

On the commercial side, mass-marketing campaigns can be replaced by targeted marketing, benefiting\(^{127}\) from a more complete picture of customers’ characteristics and reduced database errors. Some data (e.g. medical records) are well-protected by confidentiality laws and data protection acts\(^{128}\), though doubts have arisen about the security of e.g., genetic test results. For commercial purposes, these data may be partially proxied by profiling techniques without raising privacy concerns. In other commercial applications, data matching is used to reduce financial fraud and risk, particularly in credit

---

\(^{124}\) EU, Directive 95/46 of 24/10/1995 for the protection of individuals with regard to automatic processing of personal data.

\(^{125}\) The European Union has been harmonising privacy laws since 1976. The fact that this issue is being dealt with on a supranational level limits the range of different legal approaches in the surveyed EU countries.

\(^{126}\) These activities comprehend what is sometimes called “data mining.”

\(^{127}\) Consumers can benefit as well - for instance if data on childbirth or change of address permits a bank to anticipate customers’ needs for extra assistance.

\(^{128}\) And even by approved uses of encryption, as in the UK’s Red Pike block encryption scheme for patient medical data on the NHSNet - though Red Pike does offer a government ‘back door.’
reference bureaux.

Outside the commercial sphere, personal data have been used in political campaigns; the UK Prime Minister wrote to all registered voters who owned shares in the privatised utilities during the last General Election campaign, and all parties used data matching to identify and target “floating voters.” Governments carry out computerised cross-checks to determine eligibility for a wide range of services, permits, etc. Finally, matching of tax and benefit records is used to identify cases of benefit fraud connected with: provision of false details; deliberate individual fraud; and organised fraud. These initiatives have been resoundingly successful in financial terms wherever they have been applied, and the demand for their extension is growing with shrinking budgets and increasingly-stringent benefit eligibility criteria. In view of the data protection acts, this extension generally requires specific legislative authorisation.

4.2. LEGAL ISSUES

4.2.1. Principles

Data protection is usually governed by a set of principles binding on all those who collect, process and use personal data. The statement of these principles varies across jurisdictions, but they generally require that data shall be:
- fairly and lawfully obtained and processed;
- held for lawful purposes that are clearly and openly described;
- used or disclosed only for those purposes;
- adequate, relevant and not excessive for those purposes;
- accurate, timely, and not held for longer than necessary;
- held in a way that gives subjects rights of access, and appropriate correction and erasure; and
- secured against unauthorised access.

Some of these principles can be waived where required by law, or where their application might jeopardise crime prevention or detection, arrest of criminals, collection of taxes, etc. They are not all relevant to the electronic highway, but must be taken as a whole in identifying the issues their implementing legislation creates for electronic data collection and re-use. On their face, they do not seem to rule out data-matching in situations where consent has been given for the disclosure or sharing of data - it may not be obvious when the consent was obtained that the subject understood the impact of data-matching. There are even ambiguities about the extent to which data-sharing between government agencies or the use of so-called “data matching agents” constitutes the type of disclosure requiring notice. Indeed, specific laws in all four countries exclude access for law enforcement purposes from subject notification requirements altogether. The principles are also somewhat silent on the timing of required notification.

4.2.2. Subject Rights

One important right is the right to refuse to allow data to be collected and to insist that it not be used in specified ways. This raises enforceability issues with respect to contracts containing clauses

---


130 This right of informational self-determination is laid down in the French Law on Personal Data 1978, the German Constitution, and the UK Data Protection Act 1984. The US does not recognise such a right.
that apparently require consent to information collection and validity issues for negative consent devices ("Check here if you do not wish to receive information about...") that attempt to serve the dual purposes of giving notice of intended purpose and authorising disclosure. Recent case law\textsuperscript{131} has begun to address the ambiguity of the first of the principles listed above as applied to "list rental" and other secondary markets in personal information collected in the context of commercial transactions. Various voluntary Codes of Practice and the PDPD take the position that, while subjects should be notified when their data are disclosed to third parties for direct marketing, this notification could take place long afterwards. The legal issue turns on whether this fact should be disclosed to the subject when the original agreement is entered. The burden of the recent decisions in the UK is that advance notice must be given and positive, rather than negative assent obtained.

A related issue that has been the subject of a great deal of debate\textsuperscript{132}, legislative proposal and market development is that of unsolicited commercial offers, or "Spam\textsuperscript{133}". The personal data involved may be no more than an email address or a name and telephone number, but often much more is involved. In the non-electronic world self-regulatory devices such as the "Robinson List" have been implemented - these are lists of people who have asked not to receive commercial solicitations through specific media. Originally implemented by voluntary Codes of Conduct, they have sometimes been accorded regulatory protection. They have been applied to mail and telephone solicitation and initiatives to extend this to fax and even (in the US) email are under preparation. In substantive terms, the existing and pending bills provide a mix of approaches: some are technical standards, while others invoke notions of fraud or deceptive practice. Some involve regulatory enforcement action, while others (esp. the \textit{Telephone Consumer Protection Act of 1991 (TCPA)}) rely on a private right of action. The effectiveness of enforcement of existing "telemarketing" rules, whether based on personal data concerns or not, has certainly been spotty at best.

In addition to the issues involving data collected through Internet activities, questions have arisen regarding effective protection in cases where data are obtained through such activities as posting a message to a Newsgroup, sending an email to a commercial account, or allowing a Web site to set a "cookie." While the information that each provides is limited, it can certainly be used to invade privacy and through data matching may violate the data protection principles.

4.2.3. \textbf{Other Issues}

There are certain other legal problems that are beginning to be felt in the area of personal data. Some of the most critical ones occur in the context of the \textbf{implementation of the PDPD}. The Directive sets very general terms for its twin objectives of protecting information privacy and removing restrictions on the free flow of information between Member States for reasons of privacy protection. Within these (minimum and maximum) limits, Member States are free to determine the boundaries of lawful processing. The Directive makes no formal distinction between the public and private sectors, except in exempting processing falling outside the scope of EU Law, such as public and state security, defence and criminal law. Processing for personal, journalistic, artistic and literary purposes is also exempt. Certain categories of data\textsuperscript{134} must not be processed - these exclusions will certainly create

\textsuperscript{131} E.g., \textit{Innovations (Mail Order) Ltd. v. the Data Protection Registrar}

\textsuperscript{132} In the US, efforts begun under the \textit{Telephone Consumer Protection Act of 1991 (TCPA)} have led to Federal Trade Commission hearings and various private workshops on Unsolicited Email. In addition there are a number (5 at last count) of bills pending in the US House and Senate that modify or extend the earlier protections.

\textsuperscript{133} There are separate aspects of email, fax, telephone, mail and newsgroup versions that we ignore here.

\textsuperscript{134} E.g., those "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership," health or sexual preference.
problems for both public and private data users. Enforcement rests on both public and private rights of court action. Private codes of conduct are also encouraged\textsuperscript{135}. Jurisdictional matters within the EU are addressed by a “control test” that fixes the applicable law where a data user (“controller”) is located, supplemented by a “processing test” that looks to the forum where processing equipment used by an extraterritorial user is situated. Notice that “equipment” here refers to processing rather than transmission.

One topic of particular relevance\textsuperscript{136} to the electronic highway is the Directive’s prohibition on data export to non-EU countries that lack “adequate” data protection laws. The question of Transborder data flows (TDFs) has been a vexed one for both personal data and intellectual property rights. The principle issues raised are the need for a common approach\textsuperscript{137} and the enforceability of the requirement. The PDPD does not say whether states must allow transfers to conforming countries; this may weaken the Directive’s intended incentive to other countries’ data protections. The transitivity of this requirement is also unclear: does “adequate” protection mean that a non-member state prohibits transfers to other countries that do not offer adequate protection? Various definitions of adequacy have been proposed, such as certification that a given country complied with the Council of Europe Convention. Data transfers may include Automatic Teller Machine or credit card transactions; this would seem to pose serious problems for a broad interpretation of adequacy applied to the entirety of a country’s data protection laws rather than to specific transfers, particularly in cases where the third country offered adequate protection of those data. It is also unclear whether adequacy is to be measured the PDPD principles (however implemented) or the specific enforcement provisions? In any case the PDPD does provide certain exemptions\textsuperscript{138}.

4.3. COUNTRY SUMMARIES

Within each of the surveyed nations, there are forces trying to extend the protections afforded personal data and forces trying to weaken them. It appears that civil liberties groups, justice officials and Data Protection officials favour expansion of privacy rights in this area, while commercial interests, tax and social benefit officials and law enforcement favour expanded powers to collect and correlate such information.

4.3.1. EU Personal Data Protection Directive

This Directive, due to take effect next year, is largely modelled on the most restrictive current data protection laws (those of France and Germany). One striking feature is an ambitious right of informational self-determination: personal data relating to a consumer’s activities on the Internet can only be stored and processed with the subject’s “clear unambiguous consent.” It also prohibits transfer of personal data to countries that lack “adequate” data protection laws, thus creating incentives for increased data protection around the world, particularly in relation to the private sector. It has already resulted in a new Hong Kong law\textsuperscript{139} imposing similar restrictions on “data exports,” and according to the Preamble,

\textsuperscript{135} New Zealand’s Privacy Act 1993 provides for such codes to supplant national law.
\textsuperscript{137} To prevent data from leaving the EU via Member States without this prohibition.
\textsuperscript{138} Transborder flows to countries without adequate protection are allowed in cases of unambiguous consent, necessity to certain contract formation or performance elements, public interest, legal claims, protection of subject’s ‘vital interests,’ and data from public registers within their terms of operation.
\textsuperscript{139} Still in force as of this writing.
"gives a signal to the EU's trading partners, such as Canada, Japan and the United States, of the importance the EU gives to the protection of the individual's rights in the application of new technological developments."

It is worth noting that the US does not recognise informational self-determination and thus does not offer "adequate" or "equivalent" protection.

The principles laid out in the Directive are:

• **Data quality.** Personal data must be (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and used in a way compatible with those purposes; (c) adequate, relevant and not excessive in relation to those purposes; (d) accurate and, where necessary, kept up to date; and (e) not kept in identified form for longer than is necessary for those purposes.

• **Legitimate processing.** Personal data processing (collecting, recording, using and communicating) is only lawful if it comes within one of the following conditions:
  - It is with the unambiguous consent of the data subject. Consent is only valid if the data subject receives prior notification of the purposes of collection and any proposed recipients, and may be withdrawn prospectively.
  - It is necessary for the performance of a contract with the data subject, or for steps requested by the data subject prior to a contract;
  - It is necessary to comply with a legal obligation to which the controller is subject;
  - It is necessary to protect the vital interests of the data subject;
  - It is "necessary for the performance of a task in the public interest or carried out in the exercise of public authority vested in the controller or in a third party to whom the data are disclosed;" or
  - It is "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject." These public and private personal data processing conditions leave member states considerable latitude.

• **Finality.** Use and disclosure of personal information are limited to original purposes of collection. The six general grounds for processing given above can justify exceptions.

• **Other subject rights.** These include rights:
  - to be informed at the time of collection of the purposes of collection, whether it is obligatory, intended recipients, and subject rights;
  - to a copy of the data, including information about its use, to obtain corrections, erasure or suppression of data processed in violation of the Directive and to have such corrections, erasures or blocking communicated to third parties to whom the data has been disclosed;
  - to object to processing on "compelling legitimate grounds," and to "opt out of data use for direct marketing;"
  - to be immune to significant decisions based solely on automated processing intended to evaluate personal characteristics except where pursuant to contract or legislative authority in

---

140 According to Greenleaf, *op. cit.*, "Article 7 does not elaborate on how this balancing is to be achieved, but the preamble says that Member States remain free to determine the appropriate balance in relation to use of information for 'legitimate ordinary business activities' and conditions of disclosure for marketing purposes. The Commission commented on the 1992 draft that '[t]his balance-of-interest clause is likely to concern very different types of processing, such as direct-mail marketing and the use of data which are already a matter of public record.' " The most contentious privacy decisions are therefore left to Member States.

141 "Processing" as used here includes both use and disclosure.

142 There are similar rights where information is obtained from someone else other than the data subject.
the presence of suitable safeguards of the subject's legitimate interests;  

- **Security.** Data controllers must implement appropriate security safeguards, and have significant responsibilities in relation to entities who processes personal data on their behalf.
- **Notification.** The national supervising authority must be notified in advance of automated processing by private and public sector bodies. This need not amount to licensing; exemption or simplification of notification is allowed for processing that is unlikely to damage subjects' rights and freedoms, or organisations that have independent data protection officials. Notified data is to be used so that a public register can be kept by the supervisory authority. National laws must specify "processing operations likely to present specific risks" to permit "prior checking" by the supervisory authority, who must be notified of such proposed operations by the controller or data protection official. Public registers are exempt from notification requirements, implying that they are generally subject to the principles.
- **Special categories.** Processing of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership" and health or sex life is generally prohibited subject to numerous exceptions. Offence or "security measure" data can only be kept under official authority. The Commission must be notified of any derogation.

4.3.2. France
   In 1996 the French government asked for an overview of the legislation that could be applied to the Internet. The government had two major concerns: the protection of the individual and the public order, and the protection of the user. An interministerial working group was set up to study the legislative framework and come up with propositions (adjusting existing laws or creating new laws). The commission concluded that there was no judicial gap; the bulk of the current laws could be applied to the Internet (with some adjustments). The principle law in this area is the *Loi no. 78-17 relative à l'informatique, aux fichiers et aux libertés* (the Act of 1978 on Data Processing and Individual Liberties).

4.3.2.1. Principles
   The 1978 Law was passed to protect individuals from disclosure of personal data that may also impair their reputations. As Art. 1 explains:
   
   "Data processing shall be at the service of every citizen. It must operate in the context of international co-operation. It shall infringe neither human identity, nor the human rights, nor privacy, nor individual or public liberties."

   In general, the principles behind the 1978 law agree with those of the PDPA.  

4.3.2.2. Subject Rights
   French law recognises an individual's right to informational self-determination. This is spelled out clearly in Article 34:
   
   "Any person proving his identity shall be entitled to question the departments or organisations using automatic processing, a list of which shall be available to the public under Article 22 above, to determine whether such processing involves personal data concerning him, and if they do, to obtain access thereto."

   Later, in Article 36:
   
   "The holder of a right of access may require the correction, addition, clarification, updating or erasure of data concerning him which are inaccurate, incomplete, 

143 This right of access includes the right to know "the logic involved" in any such automated decisions. It has been claimed that these provisions, derived from French law, will cause considerable difficulties for US companies.
ambiguous, outdated or of which the acquisition, use, disclosure or storage is prohibited.”

Penalties are laid out in Chapter VI of this law. See e.g. Art. 43, Chapter VI, which applies to any person who undermines privacy of individuals:

“Art. 43. Sera puni d'un emprisonnement de deux à six mois et d'une amende de 2.000 à 20.000 Francs, ou de l'une de ces deux peines seulement, quiconque ayant recueilli, à l'occasion, de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, des informations nominatives dont la divulgation aurait pour effet de porter atteinte à la réputation ou à la considération de la personne ou à l'intimité de la vie privée, aura, sans l'autorisation de l'intéressé, sciemment porté ces informations à la connaissance d'une personne qui n'a pas qualité pour les recevoir en vertu des dispositions de la présente loi ou d'autres dispositions législatives.

Sera puni d'une amende de 2.000 à 20.000 Francs quiconque aura, par imprudence ou négligence, divulgue ou laisse divulguer des informations de la nature de celles mentionnées à l'alinea précédent."

The law deals with individual privacy, setting standards for security of information systems and databases for business and personal use. It is linked to French criminal law, in particular to Articles 323-1 to 323-7 of the 1994 French Penal Code. A government body, the National Liberties and Information Commission (CNIL), enforces the law.

The law defines automatic processing of personal data as: “any series of operations effected by automatic means, involving the collection, recording, preparation, modification, storage and destruction of personal data as well as any series of such operations relating to the use of files or databases, including interconnections or comparisons’.

The law applies from the moment that a person (public or private) collects personal data, registers them and subjects the data to automatic processing. The law focuses on all data that identifies a physical person, either directly (e.g. by name) or indirectly (e.g. by place of residence).

Personal data processing on behalf of the State, public establishments or private legal entities managing a public service is authorised by a regulation adopted at the urging of the Commission Nationale d'Informatique et des Libertés (CNIL). Data processing on behalf of other parties must be declared to the CNIL. This includes so-called “cookies” (fichiers implicits, automated collection of personal data by Web sites).

The law establishes certain specific exemptions. According to Art. 15, decrees made in the Conseil d'Etat may protect certain data processing affecting national security, defence and public safety. Art. 26 mentions that the right to object, with legitimate reasons, to processing of personal data does not apply to data processing concerned with national security, defence and public safety, as designated in regulations provided for in Art. 15.

4.3.2.3. Other Issues

Data Matching

There do not appear to be any legal restrictions on data matching beyond those implied by application of the existing Law. We found no cases that addressed this subject.

Transborder Flows

Art. 24 of the law states that the transmission between France and another country of any form of personal data subjected to automatic processing may require prior authorisation from the CNIL or a decree from the Conseil d'Etat.

One specific issue that is limited to the French situation is with respect to the implementation of the EU directive. Although the PDPD is largely modelled on French law, France has proposed an
implementation delay of three years. A report of two State councillors compares the Directive and the French law. It finds what it regards as strong contradictions. One is potential conflict between the goals of stimulating the free circulation of personal data between states and protection of the fundamental rights of people (Art. 3). Another is the difficulty of harmonising member states' data protection laws of EU while preserving the wide implementation latitude that resulted from the long negotiations over the Directive. In particular, they fear that countries that give their citizens the highest degree of protection risk economic disadvantage because the existence of the internal market will facilitate data delocalisation. The following articles offer such latitude:

### Table 4.1. Areas of the EU PDPD allowing latitude

<table>
<thead>
<tr>
<th>Article(s)</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Sensible data. 2.a Consent of the person. 4. Motive of important public interest 5. Data on civil judgements and administrative sanctions. 7. National identification numbers.</td>
</tr>
<tr>
<td>9</td>
<td>Regime of freedom of expressions. Choice of derogation.</td>
</tr>
<tr>
<td>10-11</td>
<td>Personal information in databases (minimal information or supplementary)</td>
</tr>
<tr>
<td>13</td>
<td>General regime of derogation. Choices between applications and motives of derogation.</td>
</tr>
<tr>
<td>14</td>
<td>Right of opposition - national laws can exclude this right in certain cases.</td>
</tr>
<tr>
<td>18</td>
<td>Obligation of notification. Several decision points: exoneration, simplifications etc.</td>
</tr>
<tr>
<td>20</td>
<td>Prior checking of processing operations for specific risks.</td>
</tr>
<tr>
<td>21</td>
<td>Publishing of the data processing.</td>
</tr>
<tr>
<td>26</td>
<td>Dispositions on transfers to a third country.</td>
</tr>
<tr>
<td>28</td>
<td>Powers of <em>a posteriori</em> control.</td>
</tr>
<tr>
<td>32</td>
<td>The delay allowed for annual files.</td>
</tr>
</tbody>
</table>

Beyond this, there are some options that the French government might decide to take, regardless of the choice of other EU countries such as allowing the users to decline to declare their "cookies." The councillors further concluded that the Directive is too detailed and will raise difficulties when transposed into French legislation because it: i) emphasises control *a posteriori*, instead of the *a priori* control in the French law; ii) fails to distinguish public and private data processing; and iii) does not take the current situation with enforcement by the CNIL into account. According to the councillors, the Directive should be a general basis for national legislation rather than a detailed description.

### 4.3.3. Germany

#### 4.3.3.1. Principles

Personal data is protected on three different levels in Germany. The highest level of protection is stated in the German constitution's principle of informational self-determination: the authority of individuals to determine in an absolute sense the disclosure and application of his or her personal data.

General principles of data collection are laid down in the *Bundesdatenschutzgesetz*, while data protections in the area of telecommunications are represented in various laws: the Telecommunication act, the Ordinance on Data Protection for companies providing telecommunications services, and the newly introduced *Teledienstdatenschutzgesetz* (TDDSG).

Until recently, emerging privacy issues were considered to be adequately dealt with by concepts laid down in the constitution and in data protection laws on both the Federal and the *Länder* level. General principles of data protection as formulated in the constitution and in data protection acts are:

- Protection of use and processing of personal data for commercial use;

---

144 Lalande, P. *L'Internet, a vrai défi pour la France*, report to the Prime Minister, April 1997.
• Limitation of purposes for which data can be collected and stored; and
• Consent for use.

For example, Article 10 of the constitution deals with privacy of letters, posts, and telecommunications:

“(1) Privacy of letters, posts, and telecommunications shall be inviolable.

(2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.”

In the area of telecommunication, the principle of informational self-determination is translated into “communicative self-determination” and telephone confidentiality. In the traditional concepts of the Bundesdatenschutzgesetz (BDSG), this means:

• Freedom of the individual to decide who would use their personal data and for what purposes;
• Transparency about who would use their personal data and for what purposes;
• Strict connection between data and the purpose of use;
• Technical and organisational protection of data processing against use for other purposes;
• Prevention of stockpiling personal data and formation of user profiles;
• Control over data processing and manipulation by independent institutions; and
• Assurance of confidentiality of telecommunication.

The concept of self-determination is based on a direct and centrally controlled link between an individual and a party that processes or receives their personal data. The nature of communication on the electronic highway, however, allows for processing of personal data in many forms and media, not only by authorised parties but also by others beyond their control.

In the context of the multimedia use of telecommunication networks, aspects of certain rules and regulations concerning the protection of communicated and stored data cannot be enforced or applied. The German government acknowledged the special conditions initiated by electronic highway developments by introducing the Teleedienstdatenschutzgesetz (TDDSG). The TDDSG (Article 2 of the Information- und Kommunikationsdienstegesetz) restricts itself to regulating data protection in the specific area of teleservices. It aims to preserve current high levels of data protection in an environment that collects and uses data in very different ways.

The personal data protection principles used in traditional electronically centralised or paper-based environments have been complemented or replaced in information exchanges through teleservices by principles of self-protection, system data protection and transparency. The principles used in the TDDSG are:

• Personal data may be collected, processed and used by providers for performing teleservices only if permitted by this Act or some other regulation or if the user has given his consent.
• The provider may use data collected for performing teleservices for other purposes only as specifically permitted by law or user consent.
• The provider shall not make provision of teleservices conditional upon user consent to data processing or reuse unless some other means of access to these teleservices is provided.
• The design and selection of technical devices to be used for teleservices shall be oriented to the

145 This may be construed as an argument against data matching.
goal of collecting, processing and using either no personal data at all or as few data as possible.

- The user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data. In case of automated processing which permits subsequent identification of the user and further collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure. Users have a waivable right of access to such information. A record shall be made of the information and the waiver.

- Before giving his consent, the user shall be informed about his right to withdraw his consent at any time with effect for the future.

4.3.3.2. Subject Rights

The BDSG requires written consent for the collection and use of personal data, at least as far as such collection is permitted in the first place. Individuals must be informed about the purpose of data storage, the character of data collected and any possible data transfer beforehand, and the consequences of rejection of approval should be made clear. The TDDSG adds the possibility of electronic consent subject to five conditions:

- consent can be given only through an unambiguous and deliberate act of the user;
- consent cannot be modified without detection;
- the creator can be identified;
- the consent is recorded; and
- the text of the consent can be obtained by the user on request at any time.

The TDDSG contains a short reference to the obligation to notify users when data are forwarded to another provider. The provider offering access to teleservices cannot transmit any data to other providers of teleservices to the same user other than:

- anonymised utilisation data for the purposes of their market research; and
- accounting data to the extent necessary for collecting a claim.

The user's right to inspect, free of charge, stored data concerning his person or his pseudonym cannot be limited or denied by §34 (4) of the BDSG. That paragraph refers to the situation in which individuals do not have to be informed because data were stored for data security or data protection control, and if they could not be deleted for legal or contractual reasons.

4.3.3.3. Other Issues

Data Matching

While the BDSG has data protection provisions that distinguish between public and private organisations, the TDDSG does not make this separation. This has not been considered appropriate or useful in the specific field of data protection in teleservices.

Transborder Data Flows

Neither the BDSG nor the TDDSG address international issues. User groups and legal scholars have been critical of the lack of provisions regulating transborder data flows. A new draft of the BDSG, however, will implement the requirements that are laid down by the EU directive on this issue.

4.3.4. United Kingdom

The Data Protection Act 1984 was the first law in the UK to address the issue of computers. It establishes a Data Protection Registrar charged with carrying out the provisions of the Act, which applies only to automatically processed data relating to living individuals. Data users (entities holding personal data about living individuals or who have such information processed on their behalf by others) are required to register, specifying:
the data user’s name and address
purposes for which personal data are used;
types of data held;
source(s) of data;
identities of those to whom data may be disclosed; and
a list of countries to which the data may be transferred.

The PDPA is not yet implemented, but the Data Protection Registrar’s analysis shows few major problems in doing so, beyond a particular problem with transborder data flows (see section 0).

4.3.4.1. Principles

Registered data users must comply with the data protection principles (roughly those listed at p. 56 supra), but the Registrar cannot enforce them against unregistered users. Subjects are entitled to access, compensation and correction of inaccurate data. Neither the registration requirement nor subjects’ rights are preserved with regard to exempt data. These data include:

- Data concerned with or held for purposes involving national security;
- Data held for recreational purposes or for managing personal, family or household affairs;
- Data held for payroll, pension and accounts (unless used for other purposes);
- Membership lists for unincorporated clubs and mailing lists.

In the latter two cases there are restrictions on disclosure.

Data users may also withhold data from subjects where this would prejudice:

- crime prevention or detection;
- apprehension or prosecution of offenders; and
- assessment or collection of taxes or duties.

The implementation of the Act has changed over the years, and the Data Protection Registrar has played an active role in improving data protection throughout the UK and particularly in the context of the various Information Society Initiatives. There has been some discussion of, in particular, the registration requirements as they touch on the issue of sensitivity. Currently, data may be considered sensitive (and thus exempt from access) based on their type or their purpose. Some users (particularly those involved in large complex processing operations) feel that any data may be sensitive for some purposes. For instance, a list of names collected from those who connect to pornographic Web sites could be considered sensitive, even though a name is about the least sensitive type of data imaginable. Others, however, object that there is no basis in law for considering some purposes more sensitive than others. This issue is still under consideration.

4.3.4.2. Subject Rights

Considerable controversy surrounds the collection and use of personal data (even lists of names) for direct marketing purposes. The law stipulates that data must be fairly and legally obtained and processed - this broad requirement raises three issues with regard to subject notification of re-use of personal data (e.g. for direct marketing):

- Is there a requirement for subject notification? (Yes)
- Must notification be direct (vs. a generic statement in the data user’s registry entry)? (Yes)

• When should the subject be notified?

The latter issue is critical to the "right to object" identified in 1985 by the Council of Ministers and later enshrined in the EU Directive. In a mail order case \(^{147}\), the Tribunal held that subjects should be notified and provided with the opportunity to object when the data were collected. In this connection, it is worth noting that the relevant section (5) of the Data Protection Act 1984 was amended by Section 161 of the Criminal Justice and Public Order Act 1994 to create three new data protection offences:

• knowingly procuring disclosure of information not covered by the data user's register entry;

• selling information procured in this way; and

• offering for sale information that has been or will be procured in this way.

The main focus of this change is obtaining personal data through corruption, staff connivance or intimidation, but it also applies to creation and resale of targeted marketing lists. This issue arose again the following year \(^{149}\) in the context of email addresses collected by Web site operators or automated news group scanning programs without notification or registration. It is not clear whether registration is required or enforceable. There appears to be a legal solution through analogy with ordinary mail and/or fax communication, and a technical or self-regulatory solution, possibly requiring statutory assistance.

In the UK, those obtaining information to rent out or use for non-obvious purposes must notify the individual of that fact when they first obtain the information. However, this is not a universal requirement nor does it replace the need for effective suppression mechanisms. Traditional postal direct marketing uses Robinson Lists; the UK equivalent is the Mailing Preference Service (MPS): an independent organisation maintains a central register of individuals who have notified them that they do not want to receive direct marketing material. This is made available to direct marketers, who "clean" their mailing lists by applying a suppression marker to anyone in the MPS file. Marketers are not required to apply MPS suppression to lists of their own customers but should apply it to general consumer lists used for promotional mailings. More recently a Telephone Preference Service (TPS) has been introduced, and a fax preference service is under development. In many countries the Robinson List concept is incorporated into relevant industry standards and codes of practice. Additionally, the Data Protection Registrar can take action against data users who fail to honour suppression requests. Can such a system be devised for email addresses?

Robinson Lists are national lists whereas the Internet is international, not owned or controlled by any one group, and largely self policing with its own etiquette and standards of behaviour. A suppression system is more likely to be effective if it is owned, driven and used by individuals rather than imposed by government or regulatory bodies, and if it does not unduly inhibit the rights of individuals to speak or trade freely. It should also be capable of integration with industry standards, codes of practice and regulatory regimes. It should therefore be simple and universally applicable.

The UK Data Protection Registrar has proposed that consumers be able to indicate and communicate their wishes directly in their e-mail addresses. This could be backed up by regulatory sanctions where appropriate; in the UK a directmailer who failed to honour this indication would be subject to regulatory action under existing law. In other jurisdictions it might be the basis for an individual civil action.

\(^{147}\) Innovations (Mail Order) Ltd. V. the Data Protection Registrar.


The concept of a marker could allow for a variety of messages in addresses analogous to the "Ja/Nee" and "Nee/Nee" stickers used on Dutch mailboxes. For example, an address in the form "NAME+ PRIV@ADDRESS" might indicate that an individual does not want any information sent to him or her. Alternatively, he or she might use "NAME+ PER@ADDRESS" to indicate that he/she does not want the address passed on to others, although he/she would object to information from the site owner. Markers could allow the individual the freedom to make different choices about different contacts. An individual might put a marker on visiting one site but not put the marker on when visiting another or he might use different markers on different sites.

4.3.4.3. Other Issues

Data Matching

In its efforts to reduce fraud and abuse, regulate direct mail and implement electronic delivery of government services, the UK government has used data matching. The problem is that combined data may be more valuable, sensitive or prone to abuse than their component parts, so descriptions of purpose and type in separate data users' registry entries may provide inadequate guidance or protection.

With regard to electronic delivery of government services, the Data Protection Registrar called for specific legislation to limit data sharing and matching and for clear guidelines on the circumstances and scope of permitted activity, especially with respect to proposals for:

- fraud protection (matching data in Inland Revenue and Benefits Office computers);
- rationalisation of government databases (though a unified central repository was disclaimed);
- multi-use Smart Cards for obtaining government services; and
- provisions for use of "data donors" (e.g., financial institutions).

In a related paper, the Office of Science and Technology observed that the Data Protection Act was written at a time when computers were relatively slow and isolated and thus requires specific legislation for data sharing and data matching. They point out that valuable data matching applications in direct marketing (as an alternative to undirected "Spam") are limited by the Act and confidentiality law. The private sector makes extensive use of data matching to detect fraud and reduce financial risk. The same techniques are increasingly used to reduce benefit fraud. The legal issues reflect the inadequacy of existing law to distinguish good and bad uses of the technique and to provide appropriate incentives. They also reflect technical factors such as the increasing decentralisation of data and processing, reliability problems associated with matching (and the assignment of liability for incorrect matches), the need to avoid mistakes and a strong tendency to function creep, whereby the purposes for which data are held gradually expand.

Transborder Data Flows

Section 12 of The Data Protection Act 1984 lets the Registrar prevent transfers of personal data to a place outside the United Kingdom if she is satisfied that it is likely to lead to a contravention of the Data Protection Principles. She cannot stop transfers to places bound by Treaty unless the data will

---

150 See footnote 100.
153 Examples include: credit reference agencies; County Court bankruptcy judgements; the Comprehensive Underwriting Exchange used to detect multiple insurance claims; the Possessions Register that tracks repossessions; the Credit Industry Fraud Avoidance Scheme database of known criminals; and the Gone Away Information Network registry of individuals who have left no forwarding address and missing debtors who have been located.
be passed to a third country, even if the ratifying country has no data protection legislation in force or lacks equivalent protection because of the inadequacy of the other country's legislation.

The Registrar is able to restrain transfer of "personal data." As a consequence of the definitions in the 1984 Act, data have to be "recorded;" this involves some degree of permanent intention. It is common for overseas transfers to be made by electronic copying to a distant site. The Registrar has called for legislation to clear up this problem.

The PDPA allows no transborder restrictions within the EU. Subject to a substantial list of derogations (e.g., unambiguous consent of the data subject) transborder data flows may only take place to non-EU countries that provide adequate data protection, where adequacy is determined by looking at a variety of circumstances, not just formal law. Finally, the EC can produce "black" and "white" lists.

The Registrar feels that such prior vetting is neither practical nor appropriate. The planned UK law must permit action to enforce any EU black list; an enforcement provision based on Section 12 of the 1984 Act might secure that objective and remedy the problems of individual data subjects.

If it is inappropriate to satisfy the adequate protection requirement by licensing or vetting, it may be possible simply to transfer the duty imposed on Member States to data users. The Hong Kong Personal Data (Privacy) Ordinance Ord. No. 81 of 1995, undertaken in partial response to the EU Directive, takes this approach. It also provides models of black and white lists and other flexibilities in the PDPA. Prohibitions are enforced by an enforcement notice procedure similar to the UK's.

How can users ensure that data are properly handled when sent abroad? The Council of Europe has developed a set of model contract conditions intended to ensure the equivalent protection of data in transborder data flow cases. Data exporters must comply with domestic law on transborder data flows and importers undertake to respect the principles in Treaty 108 and prevent data use outside the contract. The conditions have been criticised by lawyers from common law jurisdictions as being ineffective to protect data subjects who lack privity. It is also unclear what loss the data exporter would have suffered which would give rise to an action for damages in the absence of a domestic law imposing sanctions on him. This raises the questions of whether contract conditions will work, what legislative framework is needed to support them, and whether the Hong Kong model is adequate for a new transborder data flow regime.

4.3.5. United States

4.3.5.1. Principles

Despite the importance of First Amendment free speech protection, there is considerable impetus behind calls for greater data privacy. Current limited protections for personal credit, subscription and EFTA data are very likely to be extended. This may limit free speech about others' personal data. There have been several overt statements of data protection principles, but little comprehensive and effective legislation. In 1973, the Department of Health, Education and Welfare described the basics of "fair information practices." More recently, the various bodies concerned with the National [now Global] Information Infrastructure have produced similar statements of principle.

---

154 R. v Gold & Another [1988] 2 WLR 984 (HL)
Fundamentally, this reflects that fact that the US does not recognise informational self-determination and that Constitutional privacy rights are concerned with government rather than commercial intrusion.

Privacy protection in the US today remain a pastiche of specific laws and self-regulation\(^\text{157}\). This absence of clear direction coupled with the growing awareness of commercial intrusions into consumer privacy was recognised by the Federal Trade Commission (FTC), which held workshops on online consumer privacy in 1996 and 1997\(^\text{158}\).

### 4.3.5.2. Subject Rights

Most of the discussion centres around the appropriate use of consumer information, rather than its collection\(^\text{159}\). The relevant right seems to be “the right to be left alone” rather than the more specific rights of access, objection or correction embodied in European laws. This blurs the boundaries between the “data protection” aspect of using names, telephone numbers, email addresses, IP addresses, etc. to create mailing or calling lists and the “content” aspect of unsolicited commercial messages or “Spam.”

This document treats both matters under the data protection heading, since email Spam requires the use of personal data in a setting where the data subject received no notice, had no opportunity to object, and where the use, accuracy, retention and processing of the data are largely uncontrolled. The sole exception would be unsolicited posts to newsgroups, but no legislative solution is being sought there.

In addition to those mentioned in footnote 157, the following actual or proposed laws place important limits on the collection and use of personal data:

- The Telephone Consumer Protection Act of 1991 (TCPA) contains a provision for a “do not call list” that is seen by many as a model for online marketing\(^\text{160}\). It also establishes a private right of action for individuals to use in asserting their rights. More specifically, the TCPA appears to prohibit both current practices and self-regulation guidelines (see below) by banning “the sending of unsolicited advertisements from a telephone facsimile machine,” which is defined as:

  “...The term “telephone facsimile machine” means equipment which has the capacity

  - (A) to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or

  - (B) to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

- The Electronic Communications Privacy Act of 1994 prohibits “[i]nterception and disclosure of wire, oral, or electronic communications,” “[u]nlawful access to stored communications,” and “[w]rongful disclosure of video tape rental or sale records.” While not aimed specifically at personal information, it clearly forms part of the same matrix of online privacy protection.

- Part of the Telecommunications Reform Act of 1995 provides protection for personal privacy. There are provisions which limit the use and disclosure of customer proprietary network

\(^\text{157}\) These include: the Privacy Act 1974 5 (USC 552a, limiting federal data collection, use and dissemination); the Tax Reform Act 1976 (26 USC 6103, restricting disclosure of tax information); the Right to Financial Privacy Act 1978 (12 USC 3401, protection of individual bank records); the Fair Credit Reporting Act (15 USC 1681, credit records); the Family Educational Rights and Privacy Act 1974 (20 USC 1232g, student records); the Video Privacy Protection Act 1988 (18 USC 2710, video rental records); the Cable Communications Policy Act 1984 (47 USC 521, cable subscriber information); and others mentioned in the body of the text.

\(^\text{158}\) Details are available at http://www.ftc.gov.

\(^\text{159}\) This is borne out by survey research, e.g. L. Harris and Associates, Interactive Services, Consumers and Privacy, in 70 Privacy & American Business, 1994.

information ("CPNI") i.e. quantity, type, destination and amount of use of a telecommunication service by a customer, information available to the carrier by virtue of their relationship with the customer and to that which is necessary in providing that service to the customer.

- The Health Insurance Portability and Accountability Act of 1996 includes a mandate that privacy rules must be enacted by Congress or by the Executive branch within the next four years, in order to govern the privacy of health information in electronic form.

- Section 702 of the Telecommunications Act of 1996 "makes it the duty of every telecommunications carrier to protect the confidentiality of proprietary information of ... customers." It further requires "a carrier that receives proprietary information from another carrier or a customer for purposes of providing any telecommunications service to use such information only for such purpose." Carriers are permitted to use, disclose, or permit access to aggregate customer information for other purposes. In particular, carriers that provide telephone exchange service are required to provide subscriber list information to any person upon request for the purpose of publishing directories in any format.

- The withdrawn Communications Privacy and Consumer Empowerment Act of 1997 (H.R. 3685) would require the FTC and the Federal Communications Commission (FCC) to examine the impact of new technologies on privacy rights and to engage in rule-making as necessary to correct defects in consumers' privacy rights and regulate marketers' use of personal information, including those marketers using the Internet as an advertising medium. The bill included a specific provision directing the Commission to determine whether parents do or can exercise privacy rights on behalf of their children.

- The withdrawn Children's Privacy Protection and Parental Empowerment Act of 1997 (H.R. 3508) would prohibit the sale or purchase of personal information about children without parental consent; require list brokers and solicitors to disclose to parents, upon request, the source and content of personal information on file about their children and the names of persons or entities to whom they have distributed personal information; prohibit prisoners and convicted sex criminals from processing the personal information of children; prohibit any exchange of children's personal information that one has a reason to believe will be used to harm or abuse a child; preserve all common law privileges, and statutory and constitutional privacy rights; and provide for civil and criminal penalties, as well as a private cause of action. The Bill specifically proscribes list brokers who sell information about children without parental consent, the information tending to enable the child to be contacted. This is due to the fact that WWW browsing leaves "mouse droppings" revealing where a child has visited and where they are from and that children are seen as more vulnerable to solicitation either by marketers or even paedophiles.

- The pending Consumer Internet Privacy Protection Act of 1997 (H.R. 98) would prohibit an interactive computer service from disclosing to a third party any personally identifiable information provided by a subscriber without the subscriber's informed written consent. It permits the subscriber to revoke such consent at any time and requires the service to cease disclosing such information. It prohibits such service or its employee from knowingly disclosing to a third party any personally identifiable information provided by a subscriber that such service has knowingly falsified. It requires, at a subscriber's request, such service to: (1) provide such individual with his or her personally identifiable information maintained by the service; (2) permit the subscriber to verify and to correct such information; and (3) provide to the subscriber the identity of the third party recipients of such information. It prohibits the service from charging a fee to the subscriber for making such information available. It grants the Federal Trade Commission the authority to: (1) investigate whether a service has been or is engaged in any act or practice prohibited by this Act; and (2) if so, issue a cease and desist order as if such service were in violation of specified provisions of the Federal Trade Commission Act. Finally, it allows a subscriber aggrieved by a violation of this Act to obtain appropriate relief in a civil action.

Direct marketers feel these pending bills may cripple their industry. But a January 1997 Government report called for consumers to be informed about Internet information gathering practices and given the right for the information to be used only with their consent. Congress has also requested a Federal Reserve Board study to examine the risk of fraud raised by the disclosure of personal
information, after an outcry over the sale of personal information by Lexis-Nexis P-Trak service.

Participants in the FTC Privacy Workshops reached broad agreement on important subject rights, though they disagreed as to the role, if any, of legislation. These proposed rights include:

- **Notice**: participants agreed that subjects should be notified of information practices, including the identity of the collector, the uses to which the information would be put and the measures available to limit disclosure.

- **Choice**: it was broadly agreed that subjects should be able to choose whether and how their information is used, though there was disagreement as to whether this should involve positive ("opt-in") or negative ("opt-out") consent.

- **Access**: most participants agreed with a subject's right of access to information held by businesses, and further that data users should take steps to ensure timeliness and accuracy.

In addition to its Online Privacy Workshops, the FTC has acted to inhibit collection of information from children. A staff letter dated 17 July found KidsCom in violation of its rules for collecting personally identifiable information from children for one purpose without notifying parents that the data might be used for other purposes.

A consortium of Internet companies launched a programme called "Privacy Assured" in October 1996, established to design rules to make the Internet "safe" for personal and commercial use. A logo on a company's web page will show that the organisation has agreed to not knowingly list information on individual users without prior consent; block reverse searches which can be used to retrieve user names, addresses, email and phone numbers; and issue only aggregated-use statistics which cannot identify individuals. There would also be a link to the consortium's web page. Also in October 1996, eTrust was formed by a partnership between the Electronic Frontier Foundation (the "EFF") and CommerceNet. eTrust is a global initiative to establish consumer trust and confidence in electronic transactions. The key principles are:

- informed consent - the right of consumers to be informed about the privacy and security consequences of an online transaction before entering into one;

- no privacy exists without appropriate security - they are inexorably linked in an online transaction; and

- privacy standards vary according to the context of use - no single privacy standard covers all situations or all participants.

There are also arguments for a right to corporate privacy, although there is only one case where a corporation was granted a corporate tort privacy right. Privacy of commercial information is protected. Concerns were expressed in the FTC Workshops as to whether this should be extended; corporations were viewed as responsible for most invasions of consumer privacy and such a right could be used to ensure that information is not made available to the public.

To date, compliance with and enforcement Acts like the TCPA is decidedly mixed. Various
telemarketing organisations\textsuperscript{164} have developed individual or joint codes of conduct, but they do not seem to be honoured and in any case conflict with the TCPA. The current consensus outside the marketing community is that clarification of existing law is needed. The Workshop participants were pessimistic about the enforceability of new laws and the effectiveness of self-regulation. They favoured a change from negative consent ("opt-out") to positive consent ("opt-in") and expanded use of the private right of action found in the TCPA.

4.3.5.3. Other Issues

Data Matching

Data matching is one of the topics discussed under the general rubric of electronic commerce and the need to protect individual privacy. It should be noted that the US has no formal right to privacy, though various decisions involving the Fourth Amendment (see discussion of encryption) have produced an implicit definition. The main legislative initiative in this area is the Computer Matching and Data Privacy Protection Act of 1988 (Public Law No: 100-503). It requires Federal agencies to enter into written agreements with other agencies or non-federal entities regarding the disclosure and use of information generated by computer matching programs used in making determinations to provide Federal financial assistance, establishes Data Integrity Boards in each agency to oversee and coordinate implementation, and prescribes procedures for verification of information produced by such programs. Since then, a very large number of bills aimed at reducing welfare fraud and restricting eligibility for benefits payments have included explicit provision for data sharing and data matching. To date, there appears to be no restriction of private data matching.

This issue has also surfaced in the discussions around the FTC workshops on consumer privacy and the effectiveness of the online industry's efforts at self-regulation. However, it forms a minor part of the picture.

Transborder Data Flows

Relatively little attention has been paid to this topic in recent years. One interesting possible development is that it remains unclear that the US satisfies the "equivalent protection" conditions specified in the EU PDPD.

4.4. SUMMARY AND COMPARISON

This summary discussion highlights the answers to research questions 1-3. The first part, "Issues Arising," answers the first research question, while the second, "Initiatives," sketches the answers to the second two questions, describing legislation and other initiatives. The section concludes with a short comparison of the surveyed countries.

4.4.1. Issues Arising

The ease with which personally identifiable information can be collected, stored, processed and re-used on the electronic superhighway strengthens the need for protection of personal data.

Data protection is usually secured by a set of principles binding on all those who collect, process and use personal data.

Subject rights include individual rights of informational self-determination\textsuperscript{165}; data matching and sharing, use of profiling to generate mailing lists for unsolicited commercial offers and collection

\textsuperscript{164} Direct Marketing Association and Interactive Service Association, Joint Statement on Online Notice and Opt-out, presented to the June 1996 FTC Workshop.

\textsuperscript{165} Roughly, informational self-determination includes the right to refuse to allow data to be collected and
and re-use of data through such activities as posting to newsgroups, sending email to commercial accounts or connecting to Web sites.

The issue of transborder data flows concerns the restriction of data transfers to countries that do not offer 'equivalent' data protection. This issue highlights the need for a common approach.

4.4.2. Initiatives

4.4.2.1. International

All EU members will have implemented the Personal Data Protection Directive (PDPD) by the end of 1998. This Directive is largely modelled on the most restrictive Member State data protection laws (e.g., those of France and Germany). The Directive embodies the following principles: data quality, legitimate processing, finality\textsuperscript{166}, other subject rights, security, notification, and prohibition of special categories\textsuperscript{167} of data.

With regard to transborder data flows, there is a fair amount of current discussion as to whether the concept of 'equivalent protection' required of destination countries can be met in terms of specific data flows (e.g. EFTA or credit-card communications) or must be met across the board.

4.4.2.2. France

Current Status

An interministerial commission concluded that the bulk of existing French laws could be applied to the Internet, including the law on data protection: 

\textit{Loi no. 78-17 relative à l'informatique, aux fichiers et aux libertés.} In general, the principles behind the French law correspond with the PDPD. No adjustments have been made for electronic highway developments. Although France has the strongest legal protections, it is very reluctant in terms of PDPD implementation. The reason is that France finds what it regards strong contradictions in the Directive and that French law distinguishes public and private data collection and processing, with stronger restrictions on the private sector.

Subject Rights

French law recognises an individual's right to informational self-determination.

Data Matching

There are no legal restrictions with regard to data matching.

Transborder Data Flows

Transborder flows of any form of personal data subjected to automatic processing between France and another country may require prior authorisation from the national committee of informatics and liberty or a decree from the \textit{Conseil d'Etat}.

4.4.2.3. Germany

Current Status

The highest level of protection is stated in the German constitution's principle of self-determination. More general principles are laid down in the \textit{Bundesdatenschutzgesetz} (BDSG). Data protection in the area of telecommunications is provided in various laws: the Telecommunication Act, the Ordinance on data protection for companies providing telecommunications services; and the new teleservices law (\textit{Teledienstdatenschutzgesetz}, or TDDSG). In the area of telecommunications, the

\textsuperscript{166} Data can only be used for the purpose for which they were collected.

\textsuperscript{167} Data on race, ethnicity, religion, political opinions, etc.
constitutional principle of self-determination is translated into “communicative self determination” and telephone confidentiality. The German government acknowledged the special conditions created by electronic highway developments by introducing the TDDSG.

The principles laid down in these laws include:

- Protection and use of processing of personal data for commercial use
- Limitation of purposes for which data can be collected and stored
- Consent for use.

**Subject Rights**

Both BDSG and TDDSG deal with subject rights. Written consent is required for data collection and use. The user has a right to inspect stored data concerning his person.

**Data Matching**

Data protection provisions that distinguish between public and private law can be found in the BDSG, but not in the TDDSG.

**Transborder Data Flows**

Neither the BDSG nor the TDDSG address international issues. A pending new draft of the BDSG will implement the requirements of the PDPD. Germany provides strong protections and the implementation of the PDPD may fill in the gap in current protections on transborder flows.

4.4.2.4. United Kingdom

**Current Status**

The Data Protection Act of 1984 was the first law to addresses the issue of computers. A Data Protection Registrar was established to carry out the provisions of the Act, which applies only to automatically processed data relating to living individuals. Registered data users must comply with the data protection principles but the Registrar cannot enforce them against unregistered users.

**Subject Rights**

Subject rights are laid down in the Data Protection Act. Self-determination is a recognised right in the UK. In order to set up procedures whereby data subjects can 'opt out' of targeted and untargeted commercial electronic mail, the UK Data Protection Registrar has proposed that they be able to indicate and communicate their wishes directly in their email addresses.

**Data Matching**

Current discussion of legal issues regarding data sharing and matching indicate that existing law is unable to adequately distinguish good and bad uses of new techniques and provide appropriate incentives. The Data Protection Registrar called for specific legislation to limit data sharing and matching and clear guidelines on the circumstances and scope of permitted activity, with particular regard to electronic delivery of government services.

**Transborder Data Flows**

The PDPD restriction on transborder data flows will be a barrier to its implementation. The UK Registrar can prevent TDF if she is convinced that it can lead to a contravention of the Data Protection Principles. The PDPD allows no transborder restrictions within the EU. TDF to non-European countries can only take place after thorough derogation. The Registrar feels that such prior research is neither practical nor appropriate. The planned UK Law must permit action to enforce any EU black list.
4.4.2.5. United States

**Current Status**

Privacy protection in the US today is a pastiche of specific laws and self-regulation. There is no formal right to privacy. Although specific formal (First Amendment free speech protection, Fourth Amendment protection against unreasonable government search and seizure and numerous other laws) and informal (e.g. self-regulation) privacy protections are in place, there is a demand for greater data protection, especially from private parties. Current limited protections for personal credit, subscription and EFTA data are likely to be extended. The Federal Trade Commission (FTC) acknowledged this absence of clear direction coupled with the growing awareness of commercial intrusions into consumer privacy, and held workshops on online consumer privacy in 1996 and 1997.

**Subject Rights**

Most of the discussion on subject rights centres around the appropriate use of consumer information rather than its collection. Self-determination is not a recognised right in the US.

**Data Matching**

The main legislative initiative in the area of data matching is the Computer Matching and Data Privacy Protection Act of 1988. This does not appear to effectively restrict private data matching.

**Transborder Data Flows**

Relatively little attention has been paid to transborder data flows in the US. As a result of this and the weak protections against private collection and re-use of data, it appears unlikely that the US will qualify as an authorised destination for transborder data flows under the PDPD.

4.4.3. Comparison

The following Table, drawn from the country summaries above, briefly summarises the positions of the countries on several broad issues.

### Table 4.2. Comparison of personal data issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Levels of protection:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Constitutional</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes*</td>
</tr>
<tr>
<td>General data</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated processing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Special Subject Rights:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td>?</td>
<td>Positive</td>
<td>Negative</td>
<td>No^2</td>
</tr>
<tr>
<td>Spam</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Children</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>List removal</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Data matching</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. According to early 4th amendment jurisprudence and some isolated recent decisions.
2. No uniform right of consent in statute law, some in codes of conduct.

Overall, France provides some of the strongest legal protections. Despite this, France is the most reluctant of the Surveyed Member States in terms of PDPD implementation, perhaps because of the perceived disadvantages of offering strong protections when data mobility within the EU becomes unrestricted. French law distinguishes public and private data collection and processing, and places stronger restrictions on the private sector. There is little activity with regard to data matching, and vague restrictions on transborder data flows.

Germany also provides strong protections via the Constitution, data protection laws and...
(recently) the new law on “teleservices.” Implementation of the PDPD is imminent, and may fill the gap in current protections on transborder data flows.

The UK offers medium levels of protection in law, but stronger protections in policy via the activist Office of the Data Protection Registrar. Perhaps as a result, questions of timing of notification, data matching and transborder data flows remain active subjects for discussion and debate. In addition to preparations for PDPD implementation, there are moves towards self-regulation.

The US recognises no general data protection rights and lacks a unifying data protection law. The privacy rights that are recognised are aimed at protecting citizens from government intrusion. Therefore, while the US, like France, recognises a difference between public and private data processing, it places stronger restrictions on the latter. The record of compliance with the scattered laws and codes of conduct is poor, but there are growing indications that measures will be taken to enhance consumer privacy.
5.1. INTRODUCTION

This section discusses some of the issues arising with respect to the “infrastructure” layer. To put the area in perspective, we begin by noting that both one-to-one (telecommunications) and one-to-many (broadcast) activities are regulated, but under very different legal regimes. This is of great practical significance to the electronic highway since the assumptions underlying each are very different while many acts on the electronic highway can be classified under either. The distinction between the two areas is eroding from within (through cross-ownership and the proliferation of value-added telecommunications and interactive broadcast services) and without (through the introduction of new on-line substitutes for or complements to traditional telecommunications or broadcast services). This erosion reflects a combination of technological developments and market liberalisation.

Because regulation in these areas balances many different types of objectives, it is important to ensure that liberalisation originating in one sphere does not compromise interests in others. The clearest example of this is the way competition undermines the subsidies associated with provision of universal service. Much of telecommunications and broadcasting law relates only indirectly to the electronic highway. In addition, telecommunications and broadcast law are used as vehicles for addressing concerns arising in other areas treated in this report. Therefore, this chapter concentrates first on providing a necessary background dealing with general issues, then focuses on three specific legal issues: classification of activities; universal service; and the regulatory and liability treatment of service providers. This is followed by specific country summaries.

5.1.1. Background--General Issues

It is important to recognise the special importance of administrative law168 (regulation) and the difference between sector-specific and general regulatory approaches. To date, both law and policy are strongly influenced by the distinction between telecommunications and broadcasting. Both telecommunications and broadcasting law involve unique concerns and approaches developed long before the electronic highway was identified.

Regulation has its roots in a combination of economic, technological and social factors whose structure and importance differ from country to country. With the advent of economic liberalisation, it is increasingly important to balance the peculiar economic features of these sectors in order to provide the necessary institutional framework for healthy competition and advancement of other policy interests. As with most regulated industries, and particularly those being liberalised, economic factors are particularly important.

The distinction between telecommunications and broadcasting is founded in the same considerations as the argument for their regulation. Telecommunications, it is argued, is characterised by a degree of natural monopoly born out of economies of scale and the possibility that “bottleneck” networks will lead to vertical market foreclosure and/or inefficient bypass. Either exercise of market power will produce allocational and productive inefficiency and social inequity.

Broadcasting, on the other hand, started with the “merit good” argument. Its regulated status is due in no small part to the benefits of an informed public and the perceived need to control the power of

168 For a review of the vast body of law applying to the electronic highway, see e.g. Rose, L. Netlaw: your rights in the Online World, Berkeley, Osborne McGraw-Hill 1995.
that information flow to ensure (depending on jurisdiction) that public information was freely available, unbiased, supportive of social or cultural goals and/or reflective of a plurality of voices. In addition, there was a “natural monopoly” argument predicated on the scarcity of useable electromagnetic spectrum.

In both cases, doubts about the efficacy and effects of unfettered competition played a significant role, even after the technological basis for these doubts had eroded. In particular, in some countries there is a strong presumption that telecommunications content, while it may be tapped, should not be restricted. This is not uniformly the case with broadcasting. This distinction also makes a difference to the nature of regulation: whether it is handled at the federal or state level, the specific regulatory instruments used, etc. The distinction fails the “technological neutrality” principle, and has led to a facility-oriented approach to regulation with spatial jurisdictions. Even the broader policy debates over the electronic highway emphasise facilities while the market developments are increasingly shifting emphasis from the physical to the service layer, with such applications as email, voicemail, and virtual retailing, forming vital links in the value chain. This independence of applications and services from physical location may create problems for the underlying regulatory model. The distinction between facilities and services is mirrored in the liberalisation process, which typically begins with services while restraining facility competition. From a regulatory perspective, the important observation is that market power is more likely to be grounded in integrated market dominance than in exclusive control of essential facilities. This may weaken the argument for separate telecommunications and broadcasting regulation, but it may not follow that a homogeneous and symmetric regime would be an improvement. Equal treatment of wireless and wireline communications and data transmission may be costly and reduce the scope for innovation. An evolutionary approach using a presumptive relaxation of rules based on delivery mechanism might produce a smoother adjustment. As liberalisation and convergence proceed, rules reflecting privacy, security, copyright, content and contract concerns may increase in importance relative to the more economic rules that dominate (esp. telecommunications) regulation. Regulation based on scarcity, plurality of voices and bottleneck resources may well give way to new regimes based on access.

The other crucial point is that telecommunications and broadcasting law may be used to resolve other issues. Some harmful content legislation is contained in telecommunications acts; some copyright law is to be found in broadcasting statutes - we discuss them in that context. This applies to questions of jurisdiction, liability, etc. as well: if the Internet is viewed as a network of relationships rather than a diffuse “virtual space,” jurisdictional questions may be settled by analogies to telecommunications law. The legal metaphor chosen may reflect such features of the Internet activity as:

- whether information is transmitted one-to-one or one-to-many;
- whether information exchange was initiated by the sender or receiver;
- whether information exchange is one-way, two-way or multilateral;
- whether the recipient desired or accepted the information;
- whether the communications system was open or closed, etc.

Many Internet-related legal issues arising in recent years belong more properly to other areas identified in this report, though they may be dealt with using existing telecommunications or broadcast law. The following table gives examples for each of the other areas in the report.

169 This comment refers to e.g. “watershed” and broadcast standards rules as well as censorship per se.
170 Based on vertical and horizontal integration of facilities, services and content.
Table 5.1. Overlap between telecommunications and other areas

<table>
<thead>
<tr>
<th>Area</th>
<th>Issue</th>
<th>Infrastructure area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Network security</td>
<td>Telecom</td>
</tr>
<tr>
<td>Digital signatures</td>
<td>Internet payment schemes</td>
<td>Telecom, ISPs</td>
</tr>
<tr>
<td>Personal data</td>
<td>Subscriber lists</td>
<td>Telecom, cable</td>
</tr>
<tr>
<td>Content</td>
<td>Obscenity</td>
<td>Telecom, ISPs, cable, broadcast</td>
</tr>
<tr>
<td>Intellectual property</td>
<td>Copyright violations</td>
<td>ISPs, Cable, broadcast</td>
</tr>
<tr>
<td>Contract</td>
<td>3rd-party role in TTP/CA</td>
<td>ISPs, Telecom</td>
</tr>
<tr>
<td>Antitrust, Regulation</td>
<td>Internet voice telephony</td>
<td>ISPs, Telecom</td>
</tr>
<tr>
<td>Tax</td>
<td>International settlement agreements</td>
<td>Telecom</td>
</tr>
<tr>
<td>Computer crime</td>
<td>Mobile phone cloning</td>
<td>Telecom</td>
</tr>
</tbody>
</table>

As noted in the Introduction, our focus here is primarily on those aspects of this process that a) raise legal issues (though in this area they are perhaps harder to separate from economic and policy issues than elsewhere) and b) reflect developments on the electronic highway. We concentrate on three aspects, connected to the electronic highway as follows:

- **Classification and convergence**: the Internet is used to deliver new services, filling market niches and triggering realignment of existing markets. These niches reflect demand, supply and legal factors, and in turn change them.

- **Universal service**: Internet services provide an alternative that can either erode subsidies or provide a superior method of delivering an expanded bundle of "universal" services with new funding mechanisms. In extreme cases, it may be possible to provide the services competitively.

- **Treatment of service providers**: ISPs are service providers, and affect the appropriate regulatory structure. It is also necessary to resolve questions of licensing/authorisation, cross-ownership and competition policy for them.

5.2. **LEGAL ISSUES**

5.2.1. **Classification and Convergence**

Should specific services be considered telecommunications, broadcasting or something else? If one of the first two, it remains to determine their regulatory status. For instance, delivery of audio or video images over the Internet may plausibly be regarded as broadcasting, especially if posted to a news group. Exposure of the same material on a Web site seems closer to telecommunications, at least in the sense that a telephone operator delivering video-on-demand is still a telecommunications operator. The technological manifestations may be novel, but the issues are not. They have heretofore been resolved in a regulatory framework - a telecommunications operator offering entertainment or a cable television operator offering telephony remains a licensed entity subject to direct government control. However, this is changing with the liberalisation of markets and weakening of the regulatory framework. Thus the situation of, say, Internet voice telephony or video-conferencing simply calls for new application of an existing framework.

The issue of classification lies at the heart of the use of legal metaphors or analogies to resolve issues with existing laws or legal principles. In the case of the Internet, however, this may be only a short-term expedient. On one side, if a service like Internet voice telephony (IVT) behaves like other forms of voice telephony, it would seem to make sense to regulate it in the same way. On the other, convergence is rarely complete. Economic regulation, for example, is based on both supply and demand considerations, and IVT's cost and industry structures do not resemble those of conventional voice telephony. Beyond this, the intrusion of IVT into the market may change the basis or desired characteristics of existing regulation of conventional operators. It is even possible for electronic
highway service providers to straddle traditional lines between demand (service users) and supply (service providers).

The traditional classification problem is the separate treatment of broadcasting. Broadcasters were, in one sense, the first service operators along the electronic highway. While much of today's traffic is one-to-one, there are still strong one-to-many aspects. In particular, those who publish Web pages or post to Usenet discussion groups have been likened to broadcasters; at the same time content providers have developed "narrowcasting" technologies that make them seem more like cable operators than traditional broadcasters. We tend to view broadcasting as a neighbouring industry with strong reciprocal ties to the electronic highway. Traditionally, broadcasters have been subject to localised jurisdiction and a combination of regulatory restraints (pricing, investment, plurality, content, etc.) and protection (access to viewers/listeners, protection from competition, subsidised funding, some content liability, etc.) The underlying scarcity and merit-good arguments have begun to erode, especially with the advent of unregulated competitors. For their part, broadcasters have begun to move into areas such as teletext and interactive broadcasting to which the old metaphors do not apply. These changes have led to a broad perception that the existing legal and regulatory framework needs to be changed.

However, the primary changes being considered concern policy matters such as licensing mechanisms and rights to new technologies such as digital terrestrial broadcasting (DTB). The example of DTB can indicate the sort of legal issues that may arise. DTB is being deployed in the face of digital and analogue satellite broadcast as well as cable and expanding terrestrial broadcast. It offers a solution to the scarcity problem through the ability of a single "multiplex" channel to carry multiple programs. This introduces a new market structure linking content providers, multiplex channel providers and conditional access providers (who control the "set top" boxes needed to receive the content). At the moment, terrestrial broadcasters face severe regulatory constraints in token of their public broadcast role; DTB bidders are also regulated as to ownership, organisation and content in ways that satellite and cable providers are not. In part, this reflects the continuation of metaphors distinguishing closed and open communication. The emerging patterns of control threaten to undercut the plurality and access arguments for separate treatment of broadcasting. At a practical level, the possibility exists that satellite and cable operators will be able to control the industry from beyond the reach of regulation. Current proposals mix regulatory regimes: broadcast regulation for media providers, telecommunications regulation for multiplexers and conditional access providers; and antitrust regulation for all others.

The emergence of new services also erodes the separation between telecommunications and broadcasting. In particular, it may be necessary to re-think existing restrictions on cross-ownership or cross-market activity. In the country reports, we describe the preliminary steps that have been taken to classify new entities and to change the restrictions on existing ones in light of new technologies and emerging markets.

5.2.2. Universal Service

Universal service is a term that has been used in the telecommunications world since its earliest beginnings. Its social and legal meanings have changed over time. In one form or another, it remains a prime example of a social policy goal to be furthered by interference with market forces. In this section, we briefly review the history of the concept, and present several alternative views of its future. The country reports go into more details about the definition, regulation and funding of universal service, and the summary contrasts attitudes and approaches in the US and Europe.

\footnote{In fact, the German Länder have recently implemented the Mediendienstes Staatsvertrag that incorporates the issues pertaining to the Internet.}
The key elements of a universal service policy are: the definition of the service bundle to be provided (and those to whom it should be made available); the concept of affordability (if any) regarding its provision; the selection, rights and duties of the service provider; the nature of any subsidies paid to providers or users; and the funding mechanism (who must pay and on what basis).

The existing universal service structure is based on infrastructure expansion, and speaks of affordable access by large numbers to certain core services. Recently, this has been expanded to include technological upgrades (e.g. network digitisation) and access by specific groups (schools, libraries, some health care facilities) to advanced information services.

The original idea of “universal access” was developed to promote interconnection in response to the fragmentation of the emerging telephone system. As this interconnection progressed to monopoly it evolved into a means of ensuring affordable access by large numbers, via subsidies embodied in regulated prices. For some time, loss of subsidies (and thus loss of universal access) was used as an argument against liberalisation. As vertical break-up and competition succeeded monopoly, subsidies were protected, first through entry restrictions and later through the formal universal service obligations paid for by universal service funds to which competitors and governments contributed. In essence, they still involve payment of subsidies for access provision to dominant suppliers. More importantly, they are centred on physical means of access via the home. These practices, and the model on which they are based, may be obsolete. The issue is no longer infrastructure provision or even maintenance so much as improving the use of available infrastructure; hence “universal service.”

The old regulatory model rests on a dominant supplier of vertically-integrated services. It distinguishes access from usage, particularly in terms of demand. This sanctions two-part pricing with usage subsidising access. The theory also finds a compelling public interest (“equality of opportunity”) in promoting access - this supports access subsidies in much the same way that political forces acting on local public utilities commissions promoted subsidy of local services by long-distance services. Finally, the theory assumes that the originator of a “call” derives the main benefit and “should” be made to pay.

There is an interesting contrast between the telecommunications model (natural monopoly, caller benefits and one-to-one communication) and the broadcast model (congested public goods, “merit good” content and one-to-many communication). These alternative models produced very different regulatory schemes and business alignments.

Emerging telecommunications markets offer increasing possibilities of shared access by many users, number and service portability and many alternative means of access and “value-added” usage services. In addition, infrastructure growth, withering of dominant positions, and emergence of alternative payment schemes suggest that access is becoming satisfactory and usage may need assistance.

These developments are producing new relations between users and suppliers (credit v. debit payment and approval schemes, alternative liability rules); usage and/or content-based costs and prices; account portability; card-based access (CBA); and bundling of access with many more services.

To summarise, universal service will, in the future probably be extended onto the electronic highway. This extension will have physical infrastructure, service bundle, provider structure and funding aspects. For infrastructure, requirements in all surveyed countries already stipulate telephone access that is capable of supporting Internet connections of some form as well as “fully digitised” networks. Some see this being extended to high-speed access (e.g. ISDN). Service bundles may expand to include universal Internet services or universal email. The provider structure may (will) evolve away from a dominant-operator obligation to something that one or more firms compete to provide in exchange for some combination of subsidies, regulatory relief and/or liability immunity (along the lines of common carrier protections). Finally, a wide variety of proposals for funding have surfaced. As the
foregoing analysis indicates, these may be collected from entities other than competing service providers, paid to users rather than operators, and tied to service utilisation rather than access. In particular, the emergence of mobile access and the need to maximise use of terminal and/or high-speed connection equipment may combine to remove access (in the sense of a physical connection to each person’s dwelling) from the universal service equation.

5.2.3. Treatment of Service Providers

This heading refers to several related aspects of telecommunications regulation. The consideration of these issues is relatively recent and varies from country to country, and will be discussed as appropriate in each country summary. These areas include: licensing and other requirements for service providers, conditions for access by ISPs to the telecommunications infrastructure, changes in telecommunications secrecy obligations triggered by electronic highway traffic, measures taken to enhance telecommunications competitiveness in light of the proliferation of new services and major changes in regulatory structure.

5.3. COUNTRY SUMMARIES

5.3.1. European Union

The European Union has been active in many aspects of telecommunications and broadcast policy. Because EU policy is increasingly likely to be determinate in this area, we give it somewhat greater treatment here than in other chapters. The three directions having the greatest bearing on the material discussed here are measures to enhance competition (affected by classification and convergence), universal service and treatment of service providers.

5.3.1.1. Classification and Convergence

There are at least 6 Council Directives172 bearing on competition in telecommunications, together with several discussion documents, notices, etc. The overall program began with the 1987 telecommunication Green paper setting out a framework for the introduction of a single telecommunications market by 1998. The Full Competition Article 90 Directive deals with interconnection arrangements between service providers, encouraging negotiation in the first instance. It envisages reopening the interconnection question if harmonising legislation is adopted, such as the proposed Interconnection Directive. This invokes the Open Network Provision (ONP) principles, placing no restrictions on negotiation between service providers, and mandating negotiation for telecommunications organisations. Interconnection must be made available on a non-discriminatory basis (by service element) under a two-part, cost-based tariff system that permits quantity discounts and universal service surcharges. Another important element is the specification of policy goals that can be used to justify limitations of interconnection rights - network security, integrity and interoperability, and technical factors such as spectrum scarcity. It also provides for dispute resolution via the member States or the Commission. In this area the European Parliament has gone so far as to recommend establishment of a European Regulatory Authority to control licensing rules, interconnection terms, etc. with powers to investigate, settle disputes and possibly award damages. A related proposal aimed at

172 E.g., 90/388/EEC “on competition in the markets for telecommunications services,” 94/46/EC “satellite communications,” 95/51/EC “abolition of the restrictions on the use of cable television networks for the provision of already liberalized telecommunications services,” 96/2/EC “mobile and personal communications,” 96/19/EC “implementation of full competition in telecommunications markets” and 97/13/EC “on a common framework for general authorizations and individual licences in the field of telecommunications services.”
“adaptation to a competitive environment in telecommunications” calls for “light-handed” and independent regulation. Beyond this, it seeks to apply ONP principles to leased lines as a means of encouraging the entry of alternative service providers.

The Licensing Directive lays out a common framework for authorisation and licensure of telecommunications service providers. To ensure the widest possible entry, it favours a declaration procedure for new entrants, except where there exist technical (spectrum scarcity), network (integrity and security), data protection or environmental justifications for limiting the number of licenses. It also provides for a “one-stop-shop” for authorisations. Operators wishing to operate in more than one Member State may request that they co-ordinate authorisation, and can appeal to a new European Union Telecommunications Committee, though the powers of the Committee are still vague. Indeed, EC would establish a single clearinghouse to forward requests to Member States, though would-be entrants will still be subject to different procedural and substantive rules.

5.3.1.2. Universal Service

The EU currently defines the service bundle in the Voice Telephony Directive as: “an obligation to provide access to the public telephone network and to deliver an affordable telephone service to all users reasonably requesting it.” It has recommended costing and funding mechanisms in the proposed Interconnection Directive. A recent communication elaborates and expands on these elements. It bases the call for harmonisation on arguments that the uneven pattern of development under monopoly might be exaggerated under liberalisation, with resulting barriers to market growth and effective competition. It also cites the consumer protection requirements of the Maastricht Treaty.

The service bundle serves two roles at the EU level: a minimum level of service that must be offered, and a maximum bundle for use in the computation of Universal Service costs to be shared among market players. The current bundle includes voice telephony via a fixed connection that is capable of supporting fax/modem connections - the latter provides the possibility of Internet access for those with computers and an ISP account. In addition, the current bundle includes services like operator, emergency and directory assistance as well as the provision of public (pay) telephones. It is left to the member States to determine the meaning of affordability; the Directive serves merely to authorise price controls, etc. designed to ensure affordable service. Funding is based on the Full Competition and (proposed) Interconnection Directives. It includes common costing rules and a choice at national level between an independent Universal Service Fund from which payments would be made to operators or a system of access surcharges paid by service providers to telecommunications operators who provide universal services. Proposed new directions include changes in the service bundle, particularly for network digitisation and (possibly) ISDN lines and the inclusion of advanced-service access for such “public access” facilities as schools, hospitals, public offices and libraries. Other changes being considered in light of convergence and liberalisation are the possibility that funds would be provided from entities outside the traditional telecommunications sector (e.g. ISPs), government funds and public-private partnerships.

5.3.1.3. Treatment of Service Providers

There are some initiatives aimed at providers of specific services. These include Directive 89/552/EEC on “TV without frontiers” and the March 1996 Green paper on “legal protection for

---

173 95/62/EC on “the application of Open network provision (ONP) to voice telephony.”
174 COM(96) 73 on “universal service for telecommunications in the perspective of fully liberalised environment.”
encrypted services in the single market." Here, "encrypted services" refers to "services which are encrypted to ensure payment of a fee," including pay TV, digital TV, pay-per-view, video-on-demand and its relatives, games and software "on demand" and interactive teleshopping. The problem is that Member States' degrees of legal protection (particularly against unauthorised decoding) inhibits the development of the market for those services. It recommends prohibition of the possession, manufacture, trade, installation and use of decoders "designed to permit access to encrypted services without the encryptor's authorisation," as well as any unauthorised decoding of such services. Implementing legislation should include both penalties and a private right of action.

Finally, the EU has recently issued a notice "on the status of voice on the Internet under Directive 90/388/EEC" in which it finds that Internet voice telephony (IVT) does not meet the definition of voice telephony under the Directive. This is based on the argument that IVT would need to:

- be offered commercially;
- be provided for the public;
- connect switched network termination points on the fixed telephony network; and
- involve direct transport and switching of speech in real time.

The legal consequences of this determination are:

- IVT providers, like other Internet access and service providers, may not be subjected to prior licensing requirements. A general authorisation or declaration procedure that does not discriminate (in particular between Internet and other data transmission or value-added service providers) is the most that can be applied;
- Member States must provide concrete reasons and an appeal mechanism if they wish to discontinue an Internet service; and
- Internet access and/or service providers cannot be compelled to contribute to universal service funds (unless the rules change as envisaged in the Universal Service Communication (see footnote 174).

As IVT grows, this position will not change, providing that IVT is an "additional feature" of an Internet service package chosen for other reasons. More generally, if IVT users can connect to users of voice telephony networks (paying by pre-payment, credit card or electronic cash) and if IVT improves to the point where it becomes the main "selling point" of the service, IVT might be re-classified as voice telephony.

5.3.2. France

5.3.2.1. Classification and Convergence

There is no specific legislation/regulation on new services in place. The Telecommunications Act covers both new services in its definition of communication services.

In France, law governing communication can be divided into law on la correspondance privée (characteristics of telecommunication) and on la communication audiovisuelle (characteristics of broadcasting). The first is governed by the post and telecommunications code, the second by the Loi du 30 septembre 1986 relative a la Liberté de Communication. All forms of audio-visual communication are subjected to content control in France. Reasoning from jurisprudence and opinions expressed by French legal experts, Internet services are considered hybrid and its status will have to be interpreted by judges on a case by case basis.
5.3.2.2. Universal Service

The Telecommunications Act requires licensed telecommunications network operators in France to meet universal service obligations.

Universal access to the electronic highway has been highlighted in several government documents. The 1994 Théry report states that because the development of the global electronic superhighway is inevitable, France has to participate actively. Théry advocates universal access to the electronic highway:

“All French households and firms should be connected to the Information Superhighway by 2015. Access to the IS must be universal in order to allow equal access among citizens and avoid discrimination between the poor and the rich, between urban and rural areas, between professional users and domestic users.”

French politicians regularly insist on the necessity of providing all in France with access to the information society. Universal access as proposed by the Théry report has been endorsed by the French government, but no legal basis has been created, nor have any concrete steps been taken.

In contrast, the principle of universal service in telephony and related services has been enshrined in telecommunications law. The Telecommunications Act of 1996 defines universal service in telephony as “the provision to the public of a quality telephone service at an affordable price.”

Aside from the basic telephone service, this definition includes the provision of information services, directory services, pay phones in public places and free emergency calls. The public operator France Télécom is currently named as the sole operator responsible for universal telephony service. In addition, article L.35-5 of the Telecommunications Act specifies a package of additional mandatory services, including ISDN, leased lines, packet-switched data services, enhanced voice telephony services and telex to which France Télécom must provide access throughout France. To ensure that services are affordable, the Act stipulates that all tariffs set by France Télécom have to be approved by both the Minister of Telecommunications and the (new) Telecommunications Regulatory Authority. The Telecommunications Act makes a license to operate a telecommunications network in France conditional on certain obligations, including the ability to guarantee user and employee safety, network security and protection, and data protection. An operator is defined as:

“[…] toute personne physique ou morale, exploitant un réseau de télécommunications ouvert au public ou fournissant au public un service de télécommunications.”

Treatment of service providers

The French government endorses the criteria for voice telephony on the Internet as set by the EC’s Communication on the status of voice over the Internet (conform the Directive 90/388/EC) of 7 May 1997 (previously discussed in section 5.3.1.3). 177

5.3.3. Germany

5.3.3.1. Classification and Convergence

The Telekommunikationsgesetz (TKG) focuses primarily on providing conditions that should guarantee a smooth transition to a liberalised telecommunications market. Most parts of this law entered into force on August 1, 1996. It spells out provisions for competitive operations that will change an


176 Loi No. 96-659 du 26 Juillet 1996 de Réglementation des Télécommunications.

infrastructure formerly designed to serve a monopolistic actor, but that in the future will have to accommodate several telecommunications operators. The general principles that will have to be introduced and that are applicable to most of the liberalising European countries are treated in the TKG: licensing, frequency allocation, interconnection, open network provision, numbering, universal services, etc.

Another law that more closely deals with services related to the electronic highway is the Teledienstegesetz (TDG), article 1 of the Informations- und Kommunikationsdienstegesetz (luKDG). The TDG has been introduced to provide the conditions for conducting business and providing services "which are designed for the individual use (...) based on transmission by means of telecommunication (teleservices)." These teleservices are not drawn up to be meant as conclusive, but do encompass the following activities in particular:

- services offered in the field of individual communication (e.g., telebanking, data exchange)
- services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environmental and stock exchange data, the dissemination of information on goods and services),
- services providing access to the Internet or other networks,
- services offering access to telegrams,
- goods and services offered and listed in electronically accessible databases with interactive access and the possibility for direct order.

The law excludes telecommunication services (defined by the TKG as the commercial provision of the technical process of sending, transmitting and receiving any kind of message in the form of signs, voice, images or sounds by means of telecommunications systems). It also excludes content with emphasis on editorial agreement to form public opinion. This basically refers to functions exercised by radio, television and print media. Those services are covered by the Staatvertrag über Mediendienste, governed by the individual Länder and based on the utilisation of electromagnetic oscillation, disseminated wireless or by cable.

The question of whether information exchange on the electronic highway is a telecommunication (teleservices) or a broadcasting (media services) issue has played a dominant role in the preparation of the Information- und Kommunikationsdienstegesetz in Germany. While it has been (temporarily) resolved by the passage of two laws that address the specific activities associated with broadcasting or telecommunication in similar fashion, the question of which takes precedence is not quite resolved.

From several perspectives (academic as well as political opposition parties), this arbitrary division of competencies has been criticised. The main thrust of the argument is that convergence of individual (telecommunication) and mass (broadcasting) communication services make it difficult to determine which of the two laws applies. This could foster legal uncertainty. While the legal texts appear to be almost identical (esp. with respect to data protection), the fear is that the different interests of Länder (in charge of broadcasting) and the Federal government (in charge of telecommunications) could lead to different interpretations.

5.3.3.2. Universal Service

The stipulations of the TKG are aligned with European Union policies. The universal service

178 Also referred to in the sections on Harmful and Illegel Content, Copyright (see further)
179 luKDG, Article 1, par. 2 (1)
180 luKDG, Article 1, par. 2 (2)
requirement is defined as "a minimum set of telecommunications services for the public in respect of which a particular quality has been defined and to which every user shall have access, irrespective of place of residence or place of work, at an affordable price." The accompanying Telecommunications Ordinance spells this requirement out in concrete terms. In particular, the universal service bundle includes:

- voice telephony service with ISDN features;
- directory inquiries and editing of directories
- provision of public telephone and facilities for emergency calls, and
- provision of transmission facilities.

This definition of universal service was the first formalisation of this concept in German law.

5.3.3.3. Treatment of Service Providers

According to the TKG, licenses are only required for providing transmission facilities for telecommunication services to be used by the public and public telephone services. To provide any kind of telecommunication services using networks of other providers, no license is required. In establishing the TDG, major emphasis was liberalising market access as much as possible. Therefore, teleservices as defined by the TDG are not subject to licensing or registration at all.

The TDG aims at clarifying the liabilities of service providers. The provisions of the TKG relate more to data protection and telecommunications secrecy. In that context, providers of telecommunications services are obligated to maintain telecommunications secrecy. To guarantee this, service providers have to take technical precautions against unauthorised access, nominate security officers and design security catalogues. If they do not meet these obligations, regulatory authorities may prohibit operation or provision of services.

Realising that telecommunications markets are more and more operating in an international context, the German government perceives harmonisation and co-ordination of great importance to achieve the required security measures.

Finally, some German organisations have commented on the EU communication regarding Internet voice telephony (see section 0). German private sector businesses have welcomed interpretations that IVT cannot be considered voice telephony in the telecommunication regulations definition. Further, German industry has voiced the opinion that in the future if telecommunications services criteria are to be fully met, Internet voice telephony should not be governed by telecom regimes. Internet services should be seen as separate services, and thus not be required to provide universal service or be licensed accordingly.

5.3.4. United Kingdom

5.3.4.1. Classification and Convergence

With regard to the classification of new services, the UK's independent telecommunications regulator, OFTEL, has thus far taken relatively few steps in view of the fact that telecommunications is already extensively liberalised. Moreover, the Governments' representatives have explicitly disavowed

181 Telekommunikationsgesetz, chapter 2, par. 17
182 Kubicek, H. Multimedia: Germany's Third Attempt to Move to an Information Society
183 See for a description and discussion of the appropriate legal articles, the section on Harmful and Illegal Content.
184 As expressed in two public announcements in response to the EU positioning on IVT, July 1997.
any plans to reclassify Internet services as broadcasting. Recently, the outgoing telecommunications 
regulator (D. Cruikshank) has suggested that a choice be made between subsuming the functions of 
OFTEL into the Office of Fair Trading (OFT) as originally envisaged when OFTEL was created, or 
expanding its remit to include cable, digital and analogue broadcast, and Internet services under a 
homogeneous regulatory regime.

5.3.4.2. Universal Service

In line with the discussion of IVT (see next section) IVT operators and other ISPs are not 
required to contribute to Universal Service funds for voice telephony. If universal service ever spreads 
to include Internet access/services, or ISPs are reclassified as reserved service providers there may be a 
mechanism for obtaining contributions from them. In the current situation, however, this constitutes one 
more competitive advantage for the “non-voice telephony” providers of voice telephony services. Our 
OFTEL contacts saw a very real danger that this might undermine the viability of the Universal Service 
Fund and/or lead to pressures for a reduction in the scope and coverage of services.

Beyond this issue, in July 1997 OFTEL completed a consultative process on redefinition of 
universal service. A number of those consulted suggested that the required fixed network connection 
should be capable of providing high capacity data transmission and access to the Internet. OFTEL 
concluded that the universal service requirement should not be upgraded beyond “low speed data and 
fax transmission” at present. OFTEL does not see universal service as a means of rolling out new 
technologies, but as a means of ensuring that services, which the market has provided to most people 
and which have become essential, become generally available to everyone. The capacity of the fixed 
network connection will be examined in the 1999 review.

5.3.4.3. Treatment of Service Providers

ISPs in the UK are virtually unregulated. The JANet backbone is co-ordinated through 
government offices, but there is no specific legislation. One outstanding legal issue is the access of ISPs 
to the market over the regulated backbone. In this connection, OFTEL has conducted an extensive 
investigation of the impact of continuing telecommunications deregulation on the competitive health 
of the industry, including the provision of value-added (including Internet) services. Measures recently 
announced include (emphasis added):

"An updated classification of BT’s Systems Business and Supplemental Services 
Business will be brought into effect as of April 1998. This change is vital in the new 
digital world, where developments in technology must be taken account of to ensure that 
the increasingly complex array of services can be classified effectively. The change is 
also important because it is that which underpins the prices which BT charges itself for 
network services and it is therefore necessary to enable the policing of anticompetitive 
behaviour between BT and independent service providers.

Another measure set out in the Statement will give BT greater flexibility to offer lower 
prices to independent service providers in order to promote competitively priced 
services at all levels in the value chain, although access to cost-based interconnect prices 
will for now be limited in the main to those installing networks.

A third measure provides for the enhancement of the information required to be

---

185 United Kingdom OFTEL, Universal Telecommunications Services, July 1997.
186 They operate under a Telecommunications Services Class Licence that does not require registration, 
according to the UK Permanent Representation to the EU.
187 United Kingdom OFTEL, Promoting Competition in Services over Telecommunication Networks, July 
1997.
published in the Financial Statements relating to the divide between BT's Systems Business and its Supplemental Services Business. This will help to provide greater transparency in the relationship between BT and independent service providers for the benefit of everyone in the market. Additionally, independent service providers will be entitled to allocations of numbering capacity without the need for individual licences.

[OFTEL will also] set up an Independent Service Provider Forum [to] bring to the forefront issues which are important to them and which may not yet have been fully explored.”

There have also been some discussions (both official and unofficial) of the treatment of Internet voice telephony (IVT). They reflect a number of factors: emergence of commercial IVT services in the UK; reported plans for an IVT-PSTN gateway to allow interoperability between IVT and “ordinary” telephony; rapid expansion of alternative (cable, cellular, tight-beam radio, etc.) voice telephony services; and the European Commission notice (see section 0). At the moment, the general authorisation under which ISPs operate authorises “international data services” that include IVT. The official position of the UK government is that, while IVT currently does not fit the definition of voice telephony this only reflects the current failure to attain “real-time” exchange. This is expected in the near future, but the Government remains committed to minimal regulation in any case. The independent telecommunications regulator, OFTEL, took a stronger position, expressing concern that the EC position may be based on legalisms to the neglect of telecommunications and competition policy. With regard to the four reasons given as to why IVT was not “voice telephony,” they responded:

- IVT is being offered commercially, either separately or as part of certain ISPs service bundles;
- The EC might have done better to ask whether IVT was “provided” than whether it was provided to “the public.”
- IVT may well connect switched network termination points on the fixed telephony network if users connected to ISP by modem call each other. The EC goes on to suggest that IVT via leased lines or cable modems could never be considered voice telephony, something the UK’s cable telephony operators will no doubt be relieved to hear.
- While IVT does not involve direct transport and switching of speech in real time, some PSTN protocols do not actually function in real time; moreover the delay in IVT may be undetectable given adequate “bandwidth.”

With regard to the consequences of the determination, OFTEL note that cable operators appear to be subject to special conditions, and that the matter will need to be revisited in light of the desire to level the playing field between digital and satellite providers of digital communications and broadcast services. Another problem is that IVT may use large amounts of the scarce public good of Internet bandwidth. The government has only limited powers to restrict entry or bring prices into line with competing (regulated) wireline and wireless voice telephony, particularly if the position developed by the US FCC (that ISPs should be treated as users rather than service providers for the purposes of access charging) spreads to Europe.

Finally, British Telecom endorsed the EU position (previously discussed), but stress the rapid erosion of the technological basis for this determination. They also point to a precedent for separate treatment (including licensure) of part of an ISPs service package in the form of separate licenses required of value-added service providers when they offer service components that are outside

---

188 At least in the local loop, which is where the “natural monopoly” argument is strongest.
189 A. May, Comment on Notice 97/V 140/06: Voice on the Internet, 11 July 1997.
190 This is based on unattributed interviews with OFTEL personnel.
191 BT (British Telecommunications) PLC, Internet Voice Telephony - comments on Draft Notice 97/C 140/06, 2 July 1997.
the scope of the original license. On this basis, they do not believe that ISPs offering IVT will remain outside license requirements. They also point out that, if technological changes result in reclassification, IVT providers would become subject to the interconnection obligations of the proposed Interconnection Directive.

The only other legal problems that have arisen outside other specific areas mentioned in this report have to do with allegations of illegal cross-subsidy between BT’s voice telephony and ISP operations. These are routine matters being investigated and dealt with squarely within the framework of existing law.

5.3.5. United States

To understand the legal issues in the US it is necessary to briefly consider the joint evolution of the industry and the law that applied to it, since they differ from those found in Europe. When the Telecommunications Law of 1934 was passed, the distinction between telecommunications and broadcasting and the applicable regulatory structures were quite clear, as shown in the following table:

<table>
<thead>
<tr>
<th>Medium</th>
<th>Telecommunication</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis for regulation</td>
<td>Wires</td>
<td>Wireless</td>
</tr>
<tr>
<td>Regulatory structure</td>
<td>Natural monopoly</td>
<td>Scarce public good (spectrum)</td>
</tr>
<tr>
<td>Nature of communication</td>
<td>Common carrier</td>
<td>Competition</td>
</tr>
<tr>
<td>Content control</td>
<td>Private</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>PCC control</td>
</tr>
</tbody>
</table>

The regulatory structure that evolved was an extensive patchwork of barriers to entry and diversification, both between telecommunications and broadcasting and within the horizontal and vertical structure of each. These restrictions were an attempt to deal with two issues:

- fear of predatory behaviour (vertical market foreclosure, anticompetitive cross-subsidy, denial of interconnection, etc.); and
- desire to protect socially-beneficial firms and services from the ravages of “cream-skimming” competition with subsidies and legal protections.

The difficulties of jointly solving these issues are almost self-evident. For one thing, it is necessary to distinguish anticompetitive and socially-beneficial subsidies, good and bad entrants, innocent competition and monopolisation. Many commentators have pointed out that these problems are not unique to telecommunications and have strongly urged the application of general competition rules, but this approach was not followed. Over the course of time, the effects of the resulting regulatory structure became obvious: high concentration in the broadcast industry despite the potential for competition and a monopolised telecommunications structure. Until recently, the thinking represented by the two bullets above was only modified by the gradual feeling that market forces should be used where feasible in place of overt regulation, and that regulation should concentrate on preserving efficiency and investment incentives and detecting and punishing predation.

---


193 This is a simplification; see section 0 for a more balanced view.
At the same time as the law was creating new divisions that refined the old, technology was working in the opposite direction. Nowadays, most US viewers receive television over wires and many make telephone calls over the air. Interconnection rights and new delivery technologies have weakened the scale and scope economies on which the natural monopoly theory was based, while digital broadcast techniques will shortly do the same for spectrum scarcity. The response to this growing inconsistency was the 1996 Telecommunications Act (TA)\(^{194}\). It was motivated by three perceptions:

- Market forces work better than regulatory insight in managing problems of market convergence and market-splitting;
- Regulatory intervention is needed to control behaviour that damages competition for and in markets; and
- Some services offer social benefits in excess of their costs, which in turn exceed their market value.

The first two played a dominant role in the 1983 Modified Final Judgement that “broke up” AT&T into a long-distance carrier and various so-called RBOCs (Regional Bell Operating Companies). The main difficulty comes in reconciling the third with the competition implied by the first two.

5.3.5.2. Classification and Convergence

The TA stipulates broadly equivalent treatment for broadcast, cable, online services and telecommunications operators (telcos), with a revamped federal regulatory structure. It involves three overall measures: reduction of entry barriers to allow technological forces to overcome legal compartmentalisation; a change of role for the FCC from entry control to guardian of competitive conduct; and protection of vulnerable competitors whose presence is considered beneficial. While the overall mandate is the promotion of competition and the reduction of regulation, the Act requires the Federal Communications Commission to carry out 80 separate rule-making proceedings.

More specifically, the TA relaxes some of the old diversification barriers, notably that between telcos and cable operators; each is now allowed into the other’s market. Letting telcos into the cable market is sensible in one sense: telcos already have lines running into houses, so the inefficiency of multiple lines is reduced rather than increased. Telcos could provide cable before, but only under “video dial tone” rules that ensured that they did not supply telecommunications services to their entertainment customers. The new rules should offer more vertical integration. However, the more interesting competitors are probably the wireless “Multi-Video Program Distributors\(^{195}\).” On one hand, the MMDS enjoy an unfair cost advantage, in many cases using free spectrum (in most cases) instead of costly cables. On the other, the competition they provide may eliminate both the positive (protection for low-income subscribers) and negative (excess profits, reduced consumer surplus) effects of cable price discrimination.

5.3.5.3. Universal Service

Title I (A) of the TA contains the first formal definition of universal service in US law.

- It directs the Board and the FCC to “base policies for the preservation and advancement of universal service on: (1) availability of quality services at just, reasonable, and affordable rates; (2) access to advanced telecommunications and information services to all regions of the nation; (3) access and costs in rural and high cost areas that are reasonably comparable to that provided in urban areas; (4) equitable and non-discriminatory contribution by all telecommunications

---

\(^{194}\) Krattenmaker, T. *The Telecommunications Act of 1996*, 49 Federal Communications Law Journal 1, November 1996. The TA is sufficiently new that only academic assessments of its effects are available outside the area of content control (see section 0).

\(^{195}\) These MVDS include broadcast satellite and Multichannel Multipoint Distribution Services (MMDS).
services providers; (5) specific and predictable support mechanisms; (6) access to advanced telecommunications services for schools, health care, and libraries; and (7) such other principles as the Board and the FCC determine are in the public interest."

- It requires the FCC to redefine "universal service" periodically, taking into account advances in telecommunications and information technologies and services.
- It requires a carrier, upon receiving a bona fide request, to provide telecommunications services:
  1. necessary for provision of health care services to any public or non-profit health care provider that serves persons who reside in rural areas ... at rates that are reasonably comparable to those charged ... in urban areas; and
  2. for universal service educational purposes at rates less than amounts charged to other parties. It lets carriers providing such service write off the discount against its universal service fund obligation, or receive reimbursement.
- It directs the FCC to establish competitively neutral rules to: 
  1. enhance access to advanced telecommunications and information services for all public and non-profit elementary and secondary school classrooms, health care providers, and libraries; and
  2. define the circumstances under which a carrier may be required to connect its network to such public institutional telecommunications users."

Providers will be paid from a fund fed by "equitable and non-discriminatory" taxes on "[e]very telecommunications carrier that provides intrastate ... services." The emphasis on advanced telecommunications is welcomed by many, as are the extension to schools, etc. and the nod in the direction of technological neutrality in the second bullet. However, economics suggests:

- that the tax will distort consumer choices away from services offered by contributing providers;
- that the resulting cost disadvantage could lead to inefficient bypass by those not classed as intrastate "telecommunications carriers;" and
- that the evaluation of non-discriminatory taxes for different types of providers may be very complex.

The approach taken in the TA also begs the questions of how superior new technologies are to be recognised and encouraged and on what basis new services or recipients are to be added to the scope of the program. The former goal could be achieved by auctioning the right to offer universal services, but the latter remains very tricky.

In addition to the fund, Sec. 706 requires the FCC and State telecommunications commissions to encourage deployment of advanced services through utilising price cap regulation, regulatory forbearance, pro-competition measures, or methods that remove barriers to infrastructure investment. In this context, "regulatory forbearance" entails suspension of the TA's other requirements where necessary to promote universal service.

5.3.5.4. Treatment of Service Providers

The TA makes two potentially major changes to telephone provision: allowing "competition in the local loop" by requiring local exchange carriers (LECs) to offer interconnection to all comers on non-discriminatory terms; and allowing RBOCs to compete in all other areas, subject to heavy regulatory constraints. The first of these makes positive use of "interconnection rights," but does little to encourage wireless competitors. LECs are allowed to own local wireless/mobile providers, the TA does not explicitly grant interconnection rights to wireless operators and the PCS spectrum auction system is freighted with special rules that place wireless operators at a distinct cost disadvantage. With regard to the second, it remains unclear why the RBOCs are subjected to so many regulatory burdens (including cross-ownership and diversification restrictions) while other potential competitors are not.

The TA has also changed broadcasting, reducing limits on ownership and extending the term of

\[196\] Cellular and personal communications services (PCS).
broadcast licenses. These are somewhat offset by conditions for high-definition television (HDTV) that double the number of available channels and assign one to each incumbent conventional TV broadcaster. Finally, cable has been opened to new competition, with new entrants being allowed to choose whether they wish to be regulated as broadcasters, common carriers, cable companies or “open video systems” (a new entity similar to the “video dial tone” regime under which telcos used to provide entertainment services.

5.3.5.5. Summary

The TA changes the balance between the “natural experimentation” of state public utilities commissions and the new unified federal apparatus. It may also lose some of the adaptation to local differences that characterised the preceding system. More profoundly, it represents the first systematic attempt to simultaneously rely on market forces to direct technological progress (subject to competition-policy oversight) and to preserve and extend universal service. This is an ambitious goal, and the TA appears to combine good and bad elements. One particular point concerns the application of competition law in this area. As usually practised in the US, antitrust policy is based on a market definition and an assessment of the competitive consequences of its structure and conduct. These may prove difficult to extend to this industry under the onslaught of the electronic highway.

In the first place, market boundaries are blurred and strongly influenced by regulation. Moreover, traditional home delivery markets (local loop telecommunications and most broadcasting/cable) are local, while long-distance services and most Internet services (with the exception of e.g. online grocery shopping) are delivered in national or global markets. Interconnection rights strengthen this global character. The TA seems to recognise this movement in creating a broad national regulatory framework, relaxing radio ownership restrictions, etc. But it leaves the restrictions in place for television and creates new ones for RBOCs venturing into national markets. There seems no obvious reason to suppose their local monopoly power could be easily extended to the national or global stage.

In terms of identifying the players (and the degree of market concentration), the TA seems to favour structure over conduct and formal structure (ownership) over the sort of contractual affiliation that has become the norm in recent years. However, experience with the implementation of the new law and the market’s reaction may well answer these criticisms and produce unforeseen benefits. The new law certainly marks a major break with tradition and is widely cited around the world.

5.4. SUMMARY AND COMPARISON

We begin with a summary discussion that highlights the answers to research questions 1-3. The first part, “Issues Arising,” answers the first research question, while the second, “Initiatives,” sketches the answers to the second two questions, describing legislation and other initiatives. The section concludes with a short comparison of the surveyed countries.

5.4.1. Issues Arising

The issues in this area overlap with those in other areas, and have a strong economic and regulatory flavour, reflecting recent changes in the competitive and regulatory environments. Some general principles are widely regarded as desirable, such as “technical neutrality.” This means that laws and regulations should not be closely tied to characteristics of existing technology and thus liable to produce unexpected effects when technology changes. It can also be taken to favour laws that do not

197 In addition, the TA stipulates a “must renew” presumption in favour of an incumbent licensee.
produce harmful distortions in the development of new technologies. Another broad regulatory issue is the specific form of regulation: integrated or separated; general or industry-specific; service- or facility-based; etc. Finally, as liberalisation proceeds, the issue of whether and how to encourage self-regulation must be continually revisited. Beyond these general issues, our survey concentrated on three more specific topics.

- **Classification and convergence** involves several sub-issues. One is the regulatory and legal treatment of new services - are they handled under telecommunications law, broadcasting law, or new or hybrid forms of regulation? A second is the need for changes in treatment of existing (telecommunications or broadcasting services as their functions converge - this includes the special treatment usually accorded to broadcasters, common-carrier obligations for certain telecommunications operators and “entry barriers” to cross-ownership or cross-operation. A third matter receiving increasing attention is the possibility of delivering existing types of service through novel technological means - this would include digital terrestrial broadcasting and Internet voice telephony.

- **Universal service** issues centre around the common elements of universal service policy. With regard to the **service bundle**, the main questions are: to what extent should advanced services be included; should advanced services themselves be provided, or merely access capable of supporting them; and from where (home, public connection points, etc.) should access be made available? As far as **affordability and entitlement** are concerned, the main issues seem to be the extent to which novel forms of payment are used and the degree to which specific “public access” organisations (schools, libraries, hospitals, etc.) should be given favourable treatment. In terms of the **provider structure**, the issues are: the extent to which competition within the provider structure or bidding to provide “universal service” can be used to increase efficiency, improve functionality and improve incentives; and the impact of bypass technologies on the viability or desirability of current universal service provisions. In terms of the universal service **subsidies**, there are discussions about shifting payments from providers to recipients and creating incentives to reduce or eliminate the need for subsidy. Finally, various alternative funding mechanisms have been considered, including ISP liability and shifting the balance between internal cross subsidy and payments from a central fund.

- **Treatment of service providers** comprises other issues of competition policy and regulatory structure, including licensing of ISPs, conditions under which ISPs may gain access to the telecommunications infrastructure, and the question of whether telecommunications secrecy obligations extend to ISPs providing telecommunications services.

### 5.4.2. Initiatives

#### 5.4.2.1. International

In view of the international character of telecommunications policy, there has been a great deal of activity at the EU level.

**Classification and Convergence**

There are at least 6 enacted or proposed competition Directives that touch on this issue, especially in terms of interconnection, application of the Open Network Provision Principles, reasonable access charge structures and policy justifications for departures from the common requirements. The Directives also promote specific types of regulatory structure, a declaration policy (as opposed to licensing) for new entrants, and procedures to co-ordinate entry approval across the single market.

**Universal Service**

The current service bundle definition is fairly rudimentary, the determination of affordability is left to Member States, who also have considerable latitude as regards funding mechanisms - including use of regulatory forbearance, price caps, etc. At this level, the service bundle serves both as a minimum level that must be provided and as a basis for cost-sharing among market players. Proposals
for expanding the service bundle to e.g. ISDN, “public access” services and contributions from ISPs, governments, etc. are now being discussed.

Treatment of Service Providers

Recent initiatives aimed at broadcasting (“TV without frontiers,” encrypted services) are directed towards harmonisation and elimination of the local obstacles that characterise Member States’ broadcast policies. Internet voice telephony has also been addressed in a notice that finds no basis for treating it as voice telephony under the telecommunications Competition Directive. As noted, this has led to serious concerns among providers and Member State officials that both the competitive provision of telephony and universal service funding may be undercut by bypass competition.

5.4.2.2. France

Classification and Convergence

Telecommunications and broadcasting are handled under distinct legal structures; Internet services are regarded as a hybrid to be treated on a case-by-case basis.

Universal Service

The service bundle follows the EU norm: a minimal level of service provision and access to e.g. modem communications for those who can afford it. Expansion has been discussed but there are no initiatives as yet. Affordability is ensured by price regulation. All licensed telecommunications operators must contribute to a Universal Service Fund that in turn pays subsidies to the designated provider, France Telecom - it is not yet clear which ISPs will require licenses as telecommunications operators and thus incur payment obligations.

Treatment of Service Providers

France endorses the EU position on Internet voice telephony.

5.4.2.3. Germany

Classification and Convergence

The classification issue is being handled by a three-way combination. The TKG handles telecommunications services and concentrates on laying the foundations for competition. The TDG handles services provided over the telecommunications infrastructure, and specifically excludes telecommunications services per se and “broadcast-like” activities (where editorial control is directed towards formation of public opinion). The latter are handled by the Staatvertrag über Mediendienste, which is administered by the Länder. This resolution is only temporary, as further convergence increases the ambiguity of which law and even which level of jurisdiction should take precedence.

Universal Service

The universal service provisions of the TKG match the EU position. It does specify access to ISDN and transmission facilities.

Treatment of Service Providers

The TKG stipulates license requirements for those providing transmission facilities for public use or for those providing public telephone services. Significantly, no license or declaration requirement is imposed for use of others’ networks, regardless of service - this position is motivated by concerns for rapid market growth and service expansion. Moreover, German industry representatives have endorsed the EU position on Internet voice telephony, so it appears that ISPs, more or less regardless of services, will be free of license, declaration and universal service payment requirements. Telecommunications operators bound by the TKG do have obligations to preserve telecommunications secrecy that may give them a competitive edge on their less-regulated competitors, particularly if the
government's desire for extensive international harmonisation is satisfied. However, the TDG establishes ISP liability for content (see section 0 infra).

5.4.2.4. United Kingdom

Classification and Convergence

Telecommunications is extensively liberalised, and there is rapid entry in broadcasting (albeit under government control). Hence there are few regulations dealing directly with the classification issue, and officials have declined to take action in the near term to change existing classifications. Convergence has led to a discussion of whether the existing regulatory structure is appropriate; proposals range from the creation of a new "communications" regulator for telecommunications, broadcasting, cable, Internet services, etc. to the abolition of OFTEL in favour of general competition rules administered by the Office of Fair Trading.

Universal Service

There are no plans to formally expand the basic universal service bundle or to radically change the provision structure. There are major initiatives aimed at improving availability and use of advanced services by “public access” entities. At present, ISPs have no universal service fund contribution requirement; this is viewed by some as a growing risk to the viability of the fund.

Treatment of Service Providers

Internet service providers are unregulated. The major policy issue under discussion is their access to the telecommunications network, especially as the major providers begin offering their own Internet services. Investigations are underway into allegations of access restriction and predatory cross-subsidy that may produce regulatory changes. Finally, the EU position on Internet voice telephony has attracted a generally negative reaction in the United Kingdom, perhaps because this service has been more extensively marketed in the UK than elsewhere.

5.4.2.5. United States

Classification and Convergence

The regulation of telecommunications and broadcasting is based on fear of predation and a desire to support “merit goods.” Over time, this evolved into a regulatory strategy that used competition (entry in particular) in place of regulation and reduced the government role to maintaining incentives and policing behaviour of active market participants. At the same time, the law developed more and more separate categories of services (and barriers between them) while technology and marketing were moving in the opposite direction. This situation led to three perceptions: i) market forces are superior tools for managing convergence; ii) regulation is needed to punish anti-competitive behaviour within markets; and iii) the merit goods argument for subsidies continues to apply. The 1996 Telecommunications Act was the result: it lowered entry barriers; shifted the role of regulators from entry to conduct; and strengthened protections for providers of “merit goods.” It does not wholly resolve the issues raised by convergence and may result in a large number of additional regulations.

Universal Service

The Telecommunications Act was the first to formally define universal service, but the concept had a long history in response to a changing mix of market, technological and policy considerations. It stresses the affordability of basic telephony and the availability of advanced services. It also provides

---

198 Telecommunications is subject to independent regulation under OFTEL, broadcasting is subject to a pastiche of different regulations.

199 This was the original vision for OFTEL, which was regarded as a transitional measure.
for favourable terms for “public access” to advanced services through schools, etc. Funding is to be made available through a contribution tax on all providers of intrastate services, though this may have distortionary economic effects. The service bundle and other components are to be periodically reviewed, and funding may be enhanced through the use of price caps and regulatory forbearance.

**Treatment of Service Providers**

The interconnection provisions of the Telecommunications Act aimed at promoting local competition seem focused on wireline services. Symmetrically, measures to enable local operators to compete in other markets may retain too many of the old regulatory constraints.

**5.4.3. Comparison**

The following Table, based on the country summaries above, briefly summarises the positions of the countries on several broad issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal access to Internet¹</td>
<td>Favoured</td>
<td>No</td>
<td>No</td>
<td>Favoured</td>
</tr>
<tr>
<td>Legal USF²</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ISP USF contribution</td>
<td>Favoured</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Broadcasting redefined</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ISP Liability</td>
<td>Yes³</td>
<td>Yes</td>
<td>Limited</td>
<td>No</td>
</tr>
</tbody>
</table>

¹ As a specific part of universal access definition
² Legally-specified universal service fund with mandated contributions
³ For “audio-visual” content.

The principal differences between the surveyed countries in this area reflect at once the different weights applied to efficiency and equity and the very different nature of industry structure and competition. Systems with entrenched national telecommunications or broadcast infrastructures are structured very differently from those, which have already undergone liberalisation in terms of concentration (of government and market power), transparency, flexibility and the adversarial or cooperative nature of the engagement with industry. In terms of the nature of regulation in telecommunications as opposed to broadcasting, in the United States telecommunications is largely regulated via state public utilities commissions, while broadcasting is handled by the Federal Communications Commission and Constitutional law. In Germany, the situation is reversed, with the Länder controlling broadcasting and the Federal government in charge of telecommunications.

In each of the surveyed countries, the right of universal service right has been explicitly defined in the respective Telecommunications Acts. The UK and France give no indication in statute law of how mechanisms to ensure affordability should be set up, while Germany and the US do. The degree to which universal service continued to be a public good was not revisited until recent debate over the question of universal access to email and the Internet raised the issue of the “wired vs. the unwired.”

Finally, in terms of the treatment accorded market participants, there seem to be fundamental differences between the US and Europe. The following Table is an oversimplification: in each case there is a continuum along which the surveyed countries are ranged. In most respects, the US is at one end and France at the other, with the UK closer to the US end than Germany. The information in this Table is derived from the materials reviewed in writing the country summaries.

---

²⁰⁰ This is a generalisation, since the FCC has dominion over interstate communications and allocation of electromagnetic spectrum for both broadcast and telecommunications.

### Table 5.4. Policy comparison between US and Europe

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>Europe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central as opposed to State control</td>
<td>Weaker</td>
<td>Stronger</td>
</tr>
<tr>
<td>Nature of State control</td>
<td>Very regulated</td>
<td>Variable</td>
</tr>
<tr>
<td>Regulatory power distribution</td>
<td>Diffused</td>
<td>Centralised</td>
</tr>
<tr>
<td>Central-state integration</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Industrial policy</td>
<td>Policy diffusion, passive (antitrust)</td>
<td>Interventionist, active</td>
</tr>
<tr>
<td>Network ownership</td>
<td>Private</td>
<td>Public</td>
</tr>
<tr>
<td>Pre-liberalisation structure</td>
<td>Regulated private monopoly</td>
<td>Public monopoly</td>
</tr>
<tr>
<td>Relation between operator and regulator</td>
<td>Separated, adversarial</td>
<td>Close, co-operative</td>
</tr>
</tbody>
</table>
6. HARMFUL AND ILLEGAL CONTENT

6.1. INTRODUCTION

The issue of harmful content regulation is perhaps the most visible one in the debate surrounding the electronic highway and the one where governments have felt most pressure to act. This chapter takes up those aspects that are generally treated under the rubric of “content regulation.” The harm is associated with the availability of specific types of content on the Internet; the effects of viewing this content; and the social costs of providing the content. We begin with a general discussion of the legal issues surveyed, followed by summaries for each surveyed country. The discussion separates defamation and other intrinsically harmful content. The latter is divided between harmful and illegal content but in view of the fact that the surveyed countries draw the line differently this is done within the section. Finally, the section on other intrinsically harmful content contains some material on other content-based issues; since “content” is such a broad term, this touches on emerging issues having to do with fraud, trading schemes, unsolicited commercial email, etc.

6.2. LEGAL ISSUES

6.2.1. Defamation

Defamation is a general term that covers slander and libel. Its regulation is different in the surveyed countries. The particular aspects arising on the electronic highway concern the placement of liability in terms of persons and acts, and choice of law issues. The basis for most defamation law lies in tort, with liability fixed to both the author of the defamatory statement and other parties who knew or had reason to know of the content and had the power to stop or restrict its dissemination. In particular, liability is fixed on the author because:

- The author’s statement is made more powerful by its publication in a public forum; and
- The victim has limited opportunity to “set the record straight.”

Liability is further fixed on publishers, editors and distributors on the grounds that:

- They have reason to know the content of the statement and power to stop it;
- Their access to the public forum exceeds the victim’s; and
- Their financial resources exceed the author’s.

In the case of Internet defamation, any or all of these assumptions may be violated. Access is so easy that all speech is “cheap talk” and it is difficult to make a convincing case for injury based on content alone. Moreover, the victim typically has equal access to the same forum, and can often reply almost instantaneously. For their part, publishers, editors and distributors in the strict sense may have neither opportunity, reason nor the resources necessary to evaluate every message or even to identify the author or object. Indeed, their access to the forum and financial resources may well be less than those of author or victim.

One persistent problem is the difficulty of fixing identity, and the question of whether liability attaches to a service provider who does not take steps to ascertain his subscribers’ identities or to disclaim their statements. To date, developments that might eventually lead to full-bodied statute law on the topic have occurred in most of the surveyed countries.
6.2.2. Other Intrinsically Harmful Content

There have been many attempts to regulate content on the Internet with respect to pornography; hate speech; terrorist information; sedition; blasphemy; racism, etc. The crucial legal issues are not specific to the electronic highway, although the urgency of the problem is. In particular, the exposure of sensitive populations to offensive material sharpens the conflict between censorship and free speech and the choice of means between technical measures (blocking access), criminal law, “moral suasion“ and liability law.

In analysing this topic it is critical to distinguish between:

- **harmful and illegal** content; and
- **content and viewing**

For example, pornographic material may be viewed as harmful, but is not illegal (obscene) *per se*. However, showing even pornographic material that is not obscene to children is usually illegal.

Table 6.1. Harmful and illegal content

<table>
<thead>
<tr>
<th></th>
<th>Adults</th>
<th>Children</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pornographic</td>
<td>Harmful</td>
<td>Illegal</td>
</tr>
<tr>
<td>Obscene (e.g. child pornography)</td>
<td>Illegal</td>
<td>Illegal</td>
</tr>
</tbody>
</table>

The crux of the legal issue is that an attempt to protect a specific group (children, in this case) by a blanket prohibition on, say, pornographic material on the Internet may be misprised. Indeed, many commentators and much law seems to be moving in the direction of a multi-tiered approach combining legislation, self-regulation and technical means of “content-blocking.” The difficulty of legislation as a sole solution to the problem is compounded by the global nature of the Internet and the fact that the line between pornography and obscenity (or between permitted and illegal types of hate speech) is drawn differently in different countries. Nor is this a simple matter of “leakage” - material located in one jurisdiction may be aimed squarely at subscribers in another, as “pirate radio” stations used to be.

This material is available on the Internet in a variety of media that differ in significant ways. Web pages and ftp sites contain the bulk of pornographic material. Web site operators can demand both proof of age and payment for access to their material, but it is impractical for authorities to restrict access in a wholesale fashion. In addition, as we have mentioned in the discussion of personal data, access to a Web site is potentially a matter of record. Other material is posted to Usenet discussion groups, where access restriction by suppliers is not a practical possibility, no payment is required and there is no record of access. On the other hand, as recent experience in the UK has shown, it may be practicable for authorities to enforce (or request) wholesale restrictions on news-feed suppliers. Finally, some sexual activity takes place on IRC (Internet Relay Chat) connections, which are real-time audio-visual contacts among small groups of users.

CompuServe was ordered to pull all the adult-oriented Usenet newsgroups off its system by German officials who said making them available there was against the law. Because there is no way to stop only German customers from being able to access those newsgroups, the ban was affecting

---

customers worldwide. A key issue in Germany was the availability of content to minors. The suspension was discontinued after CompuServe introduced a number of parental controls and content restriction tools. In its most recent series of legal initiatives on information and communication services, the Jugendsschutz specifications were extended to also cover electronic content harmful to youth but not necessarily prohibited by criminal law. In addition, it stipulates that individual Internet service and content providers should examine whether a youth protection commissioner (whose role it is to advice users and providers about issues relating to the protection of minors) needs to be appointed.

Recent cases in France were decided in favour of the constitutional right of freedom of expression. However, the government prosecuted two ISPs for distributing child pornography in newsgroups. In the 1980s, French Penal Code was amended to regulate this kind of abuses appearing on Minitel services. The new French Telecommunications Law requires ISPs now to provide their clients with technical devices that enable users to block access to certain services. The awareness that this requirement encompasses many practical difficulties still obscures the liability status of ISPs in France. Earlier this year, the French government published a discussion paper on “Netiquette”, defining general rules for Internet use, an explicit step toward the promotion of self-regulation.

The recently-overturned Communications Decency Act, part of the Telecommunications Bill 1996, represented an ambitious attempt to control indecent material on the Internet. The provision was overturned on First Amendment grounds. The most troubling provisions created criminal liability simply for publishing sexual or other material that might somewhere be deemed to be “indecent or patently offensive” over the Internet. It even requires that undefined “effective” steps be taken to protect minors from such materials. Finally, it conflates the terms “indecency” and “obscenity” which have very different meanings in US Constitutional Law203.

6.2.3. Other Content-Based Issues

Much recent attention has been paid to the transmission of fraudulent material over the Internet. One particular problem is the explosion of “pyramid” or Ponzi schemes, such as the MakeMoneyFast chain email letter or its Cashflow.zip successor. The former was a simple chain letter using email, and as such was easily ruled illegal on standard grounds; the only practical question was how to stop its proliferation. The latter attempted to evade the pyramid trading scheme laws204 by selling a “product” in the form of a computer program that contains instructions as to how to prolong the chain; a similar “product” had individuals paying to be added to a mailing list. As currently worded, these schemes evade the Statute of Frauds by mentioning the uncertainties involved, but do fall foul of specific legislation already crafted to deal with such trading schemes.

We also include unsolicited commercial announcements or Spam under this heading. The central issues vary depending on whether the medium is email or newsgroups. The US Federal Trade Commission has begun a major initiative against unsolicited commercial email, and the US has a number of pending bills and important cases. The case of newsgroups is more difficult, since it has all the essential features of the classic “Tragedy of the Commons.” A number of years ago, two attorneys (Canter and Siegel) deluged more than 10000 newsgroups throughout the world with multiple advertisements for their services (the “Green Card Lottery” case). They had to change ISP a number of times, but made a fair bit of money, not least through the sale of a book containing hints for exploiting Usenet as an advertising medium. In an interesting recent development, Canter was recently disbarred.

---

203 Faber, J. at 8 Lex Mundi World Reports 2, July 1996.
204 E.g. the US Postal regulations or the UK Trading Schemes Act.
There are a number of lawsuits regarding this activity, known as excessive multiple posting/excessive cross posting (ECP/EMP) but to date no legislative proposals have surfaced.

6.3. COUNTRY SUMMARIES

6.3.1. International

Perhaps as a result of widely-differing local standards, there are few concrete international legislative initiatives. However, there have been many discussions\(^{205}\) of harmful and illegal content in various international fora. The official recommendations recognise limits to EU intervention in the form of subsidiarity and proportionality\(^{206}\), but nonetheless call for international regulation of access and service provider liability. The recommendations also stress the distinction between harmful and illegal content and urge international co-ordination of the distinction between the two.

Harmful content is regarded as a matter involving national (or local) standards and the resolutions call for common international rating systems, self-regulation and parental control, subject to overall consistency with The principles of the European Convention on Human Rights (ECHR, especially the freedom of speech provisions of Article 10). Legal commentators\(^{207}\) stress the importance of recognising the distinction between provision of content and provision of access, storage, etc. in the open environment of the Internet, and of taking account of recent judgements of the European Court of Human Rights that elucidate the meanings of freedom of expression, its limitations, and the limits of those limitations, as well as the implementation of proportionality. More specifically, they stress the detrimental effects of trying to impose uniform approaches to the distinction between harmful and illegal content or the regulation of the former. With regard to liability, they point out that self-regulation and liability can be made complementary, with self-regulation providing evidence that reasonable efforts have been made to prevent access to harmful content where appropriate. Moreover, they suggest that centrally imposed ratings systems are unlikely to be successful whether they are unilaterally imposed by providers\(^{208}\) or agreed across the communities linked by the Internet\(^{209}\).

Illegal content is viewed as a matter of national law, complicated by the fact that such content is often made available via channels such as Usenet newsgroups or email which are considerably more difficult to monitor, detect, trace and control than Web pages. Inter alia, the EU recommendations call for police training and co-ordination, a minimum number of common rules in criminal law and administrative co-operation to facilitate their enforcement without regard to the location of the content provider, a common framework for self-regulation (in co-operation with authorities), common liability regulation and even the creation of new, even world-wide international legal instruments. In response, legal commentators have pointed out that the primary vehicle for international harmonisation and

---

\(^{205}\) E.g., EU publications such as the Green paper on the protection of minors and human dignity in audio-visual and information services, COM(96) 483, Commission Communication on illegal and harmful content, COM(96) 487, Telecommunications Council Resolution on harmful and illegal content on the Internet, 97/C 70/01, European Parliament Resolution 24 April 1997, and Interim report on initiatives in EU member states with respect to combating harmful and illegal content on the Internet, http://www2.echoluilegal/en/w2ep2en.html.

\(^{206}\) Based on the observation that content regulation touches both free movement of services (First Pillar) and civil liberties and justice (Third Pillar).


\(^{208}\) In which case they unduly restrict parents' freedom of choice and exercise of judgement.

\(^{209}\) In which case they may find that there are no neutral descriptive terms valid across those communities.
enforcement will, in the short run at least, be "appropriate co-operation" between national authorities.

Any EU action will have to respect privacy rights (Article 8 of the ECHR), including the right to anonymity. Similar issues arose in the context of personal data protection, and the Personal Data Protection Directive can be used as a source of criteria for balancing privacy rights and legitimate law or liability enforcement needs.

6.3.2. France

6.3.2.1. Defamation

The 1881 Loi sur la Liberté de la Presse that outlaws defamation is applicable to the Internet. Producing or "holding" defamatory material is not an offence; publication by means of speech, printed words, drawings, paintings etc. is. It should be noted that in order to preserve democratic debate, the law exempts material concerning public figures or matters of clear public interest.

When defamatory information is accessible from French territory, a suit can be filed in France under French law. This means that the de facto jurisdiction is global; French citizens can press charges no matter where the server spreading the defamatory material is located. The real legal problems arise in enforcing the court's judgement.

The issue of who controls the information flow on the Internet and who is liable for harmful or illegal content - or indeed whether it is possible to settle this for a medium as decentralised as the Internet - has not yet been answered by French legislation. It is still unclear whether or not ISPs can block access to certain messages and information sites. The 1996 UEJF case (see following paragraph) exonerated ISPs from certain forms of content liability, stating that ISPs do not provide content, but simply channel content provided by their users. That same year government had to withdraw legislation that installed government content control.

In March 1996, the Association des Etudiants Juifs de France (UEJF) sued nine ISPs in France for providing access to Web sites containing revisionist messages. The court rejected the UEJF's demand for closure of the sites, arguing that ISPs are providers of access and reasonably not of content. Forcing ISPs to control all message content in real time would be impossible to implement.

The debate in France on content liability took an interesting turn later that year when legislation on government content control on the Internet was passed and later withdrawn as unconstitutional, not unlike the CDA debacle in the US. In June 1996, when the Senate examined the new telecommunications bill, the government proposed an a priori exemption from criminal liability for ISPs, provided that some conditions are met. This amendment, known as the Amendement Fillon after the Telecommunications Minister, sought to add 3 articles to clarify the legal status of ISPs and to establish government content control.211

210 For details of the case, see http://www.aui.fr/Groupes/GT-RPS/UEJF/uejf.html. While this case appears to be a major exception to the general principle of ISP liability (e.g., for defamation), the judgement probably depends more on the broad and vague nature of the UEJF allegation than a countervailing assertion of ISP immunity.

211 The Amendement Fillon: Article 43-1. - Toute personne dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle mentionnés au 1° de l'article 43 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est tenue de proposer à ses clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner. Art 43-2. Le comité supérieur de la télématicque, placé auprès du Conseil supérieur de l'audiovisuel, est chargé d'élaborer des recommandations propres à assurer le respect, par les services de communication audiovisuelle mentionnés au 1° de l'article 43 (de la loi n° 86-1067 du 30 septembre 1986), des règles déontologiques adaptées à la nature des services proposés. Le Conseil supérieur de l'audiovisuel adopte, sur proposition du comité, les recommandations qui sont publiées au Journal Officiel de la République Française. Article 43-3. - Les personnes mentionnées à l'article 43-1
Article 1 of the amendment requires ISPs to provide their clients with a technical device to enable them to block access to certain services. The second article grants extensive regulatory competencies to the Conseil Supérieur de l'Audiovisuelle (CSA), the government broadcast agency. The CSA would publish guidelines to ensure respect for ethical rules on the Internet in the Journal Officiel. The third article states that an ISP that provides clients with necessary software to block access to a service against which the CSA had unfavourably decided will no longer be criminally liable for offences resulting from the content of messages in question (unless the ISP has knowingly committed or participated in the offence).

In late June, Parliament accepted the Telecommunications Act together with the Fillon amendment. However, a number of French user associations protested the Internet regulation and alerted public opinion to the matter. In July, a group of 61 Senators asked the French Constitutional Council to review the amendment. The Conseil Constitutionnel struck down articles 43-2 and 43-3 of the Fillon articles (on CSA content control powers and limiting ISP liability) as unconstitutional on the grounds that the articles restricted free communication of thoughts and limited the exercise of the constitutional right to free speech. The obligation for ISPs to provide clients with parental control software was left in force. However, the liability status of ISPs is still obscured by the awareness that this requirement encompasses many practical difficulties. (E.g., how to deal with non-French ISPs with French customers?)

Since the partial withdrawal of the Fillon Amendment, the French government has taken a more pragmatic stance and leans towards the self-regulation of content: “Netiquette”.

In October 1996, France proposed a charter for international co-operation on Internet issues on the OECD level. The object of the proposal is to harmonise the different national bodies of Internet legislation on the basis of the self-regulation of content. Also, the proposal contains suggestions for international police and judicial co-operation to deal with criminal use of the Internet by international terrorists, drug traffickers and organised crime.

In March 1997, the Beaussant Commission of the responsible Telecommunications department launched the Charte de l'Internet, a national discussion paper that is intended to serve as a declaration of intent for future regulation of Internet etiquette. The document defines general ethical principles applying to the Internet, like the protection of minorities, human dignity and intellectual property. The government’s intention is to have a public debate on the content-orientated rules and customs on the Internet, in order to gain adherence of the French Internet community to the Charte.

Most recently, in August 1997, PM Jospin confirmed the governments' focus on self-regulation of content:

“La préservation du droit de la propriété intellectuelle - sans lequel il n'y a pas de création -, les garanties des consommateurs, la protection des mineurs, la répression de ce qui l'on appelle aujourd'hui la "cyber-criminalité", la lutte contre la propagande raciste ou révisionniste, le respect de la vie privée sont autant d'impératifs. Internet n'est pas, comme on a pu le dire ici ou là, une zone de non droit. [...] Il appartient d'abord aux acteurs d'Internet de prendre en charge eux-mêmes ce qui peut relever d'une régulation préventive du réseau. Celle-ci, en s'appuyant sur des règles de conduite et une déontologie, doit concilier la lutte nécessaire contre les déviations auxquels Internet... ne sont pas pénalem tement responsables des infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle sauf si elles n'ont pas respecté les dispositions de l'article 43-1, ou si elles ont donné accès à un service ayant fait l'objet d'un avis défavorable publié au Journal officiel en application de l'article 43-2, ou s'il est établi qu'elles ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission.

212 E.g., the influential French organisation of Internet users AUI described the amendment as 'hasty, useless, unjustified, technically inapplicable and dangerous to democracy and freedom of expression'.
peut donner lieu et le respect de la liberté de communiquer qui fait sa richesse.”

Internet is a medium like all other means of communication. In the absence of specific regulation of criminal content, court decisions have established the scope. The Yves Rocher case of April 1996 extends defamation law to the Internet. The Yves Rocher company was ordered to remove defamatory remarks about two other companies from the Internet. The cosmetics giant claimed that given the character of the Internet, it could not control access to and distribution of any information it had put on the Net. The judge rejected this argument, fixing liability on the author on the grounds that if one can put defamatory material in a public place, one can also remove it from there213. In the April 1997 ESIG vs. l’EXPRESS Case it was confirmed that defamation law extends to the Net. Publisher L’Express had to pay damages to the ESIG company for publishing a defamatory article on its Web site, as well as in the magazine itself.

6.3.2.2. Other Intrinsically Harmful Content

Article 227-23 of the Code Penal stipulates that the production and distribution of a pornographic image of a child by whatever means constitute an offence punishable by one year of imprisonment and a fine of FF 300,000. Penalties increase to 3 years imprisonment and a fine of FF 500,000 when the child is less than 15 years old.

Article 227-24 of the same Code outlaws the distribution, by whatever means, of violent and pornographic messages which may be seen by children, specifying penalties of 3 years imprisonment and a fine of FF 500,000. The offence does not require that a minor has actually seen the material; it suffices that minors are “likely to see” it.214

These two articles, known collectively as the Jolibois Amendment, were passed in the 1980’s to fight abuses on the Minitel network. They specifically state that distribution of illicit pornographic material is punishable regardless of the medium used for distribution.

In May 1996, two French ISPs were charged with the distribution of paedophile material because some of their Newsgroups contained pornographic pictures of children, which were posted outside of France. The ISPs’ appeal is still under consideration.

In France, communication inciting to hate, discrimination and violence is considered harmful content, along with the specific offences of Holocaust denial and incitement to the consumption of drugs. Below, the acts that constitute the offence are described, along with their applicability to the Internet if this has been determined by a specific case.

Article 24 of the 1881 Loi sur la Liberté de la Presse punishes the direct incitement to discrimination, hate or violence against a person or a group of persons. Article 24 only applies to writing or speech explicitly intended to encourage discrimination, hate and crimes of violence.

Article 24 bis punishes the act of contesting the reality of crimes against humanity. This article especially concerns the denial of WW II crimes215. In 1990, the Paris Appeals Court decided that the

---

213 This may not be applicable on Usenet (newsgroups) as opposed to the Web.
214 Article 227-23: Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image d'un mineur lorsque cette image présente un caractère pornographique est puni d'un an d'emprisonnement et de 300 000 F d'amende. Le fait de diffuser une telle image, par quelque moyen que ce soit, est puni des mêmes peines.
215 However, in 1992 a British academic, Bernard Levin, was convicted for denying the Turkish genocide of the Armenians. The case was based in part on material republished in Usenet newsgroups by an “artificial
publication of any written revisionist statement aiming to deny Jewish genocide constitutes a statutory offence. Revisionist messages posted to newsgroups or exposed on neo-nazi Web sites are likely to conflict with article 24 bis.

Article 24 refers to article 23, which in its turn proscribes the act of expressing litigious speech, whatever medium is used, provided that culpable intention exists. The term “medium in use” implicitly includes the Internet in its definition (“any other medium for written words, speech, picture”).

Article 227-18 of the Penal Code punishes the illicit consumption of drugs, mainly in order to protect minors. In addition, Article 630 of the Code de la Santé Public punishes the acts of inciting or aiding the consumption of drugs. The promotion, by any means, of the use of certain drugs (including marihuana) is forbidden. Thus advertising or promoting the use of marihuana on the Internet (as some Dutch Web sites do) is an offence in France.

6.3.3. Germany

A number of German laws deal with the dissemination of harmful and illegal content. Within the German Strafgesetzbuch (Criminal Code), various categories of content are declared punishable. Paragraph 184 applies to different forms of pornography (providing pornography to underage persons (184 (1); containing violence, sexual abuse of children or sodomy), paragraphs 185-200 address the issue of defamation, and a number of sections in the StGB deal with criminal offences related to racism, glorification (131) of and incitement to war (80a), violence, and crime (111, 130a) incitement to hatred against parts of the population (130), and holocaust denial, approval or minimisation (130 (3)). Each of these offences can be punished with either imprisonment or fines if they take place through the dissemination of publications as defined in paragraph 11 (3). The definition of “publication” in this paragraph has recently been extended to also cover “data storage devices” as means of publication. The various general and specific administrative acts and the Criminal Code have been amended to include “data storage devices.” In addition, the methods of providing information are not just limited to dissemination of materials, but also making materials publicly available and accessible by means of electronic information and communication services (Art. 86 (1) Criminal Code, Art. 119 (1) Administrative Offences Act, Art.3 (1) of GjS). This makes these laws explicitly applicable to electronic highway activities.

Moreover, there are specific provisions in administrative laws that serve the protection of children and young persons from potentially morally harmful information. The most important laws in this respect are the Gesetz über die Verbreitung jugendgefährdender Schriften (GjS), the Ordnungswidrigkeitsengesetz, and the Gesetz zum Schutz der Jugend in der Öffentlichkeit. These administrative laws require the appointment of commissioners to oversee and consult on issues regarding publications potentially morally harmful to youth, and regulate procedures that will assess whether publications (on an individual basis) are or are not harmful. There is a requirement for the appointment of Jugend commissioners for those who provide “electronic information and communication services which are based on transmission by means of telecommunication (...) and (...)

- which services are generally available

\footnote{Article 227-18: Le fait de provoquer directement un mineur à faire un usage illicite de stupéfiants est puni de cinq ans d'emprisonnement et de 700 000 F d'amende. Lorsqu'il s'agit d'un mineur de quinze ans, l'infraction définie par le présent article est punie de sept ans d'emprisonnement et de 1 000 000 F d'amende. Article 227-18-1: Le fait de provoquer directement un mineur à transporter, détériorer, offrir ou céder des stupéfiants est puni de sept ans d'emprisonnement et de 1 000 000 F d'amende. Lorsqu'il s'agit d'un mineur de quinze ans, l'infraction définie par le présent article est punie de dix ans d'emprisonnement et de 2 000 000 F d'amende.}
The commissioners occupy a dual role: they act as a point of contact for users of teleservices; and advise providers about the offering and dissemination of potentially harmful content. These requirements can be also be met if a provider involves a self-regulatory organisation to conduct these activities.

The two main legal issues that have been and are still being addressed are the applicability of current law provisions to the information and communication dissemination on the Internet, and the fixation of responsibility and liability of the different parties involved in these communication processes. Both in Article 1, the Teledienstegesetz, and Article 6, the Amendment to the Gesetz über die Verbreitung jugendgefährdender Schriften, of the new Information- und Kommunikationsdienstegesetz, these issues have been partly tackled.

The fixation of provider's legal responsibility; considering the fact that the placement of responsibility for content in the context of the electronic highway (esp. with regard to service providers) has been subject to different interpretations, the German legislature has dedicated a specific act to deal with the liability issue. Paragraph 5 of Article 1 of the IuKDG states the three (decreasing) levels of responsibility of providers as follows:

"(1) Providers shall be responsible in accordance with general laws for their own content, which they make available for use.

(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.

(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.

(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telekommunikationsgesetz and if blocking is technically feasible and can reasonably be expected. "

According to the Begriindung (explanation) to the IuKDG these provisions should be interpreted in the following way. Providers (and authors) remain fully responsible for their own material and material that they have acquired; in these cases, they should be considered the author of the material. They bear co-responsibility if they have knowledge of the content of those materials to which they provide access and have the capability to block access to the information. These duties are limited to the exercise of "minimum care" (i.e., examine content only if there is a reason to suspect it contains illegal information) and is only applicable if a provider continues to provide access to content which he consciously knows is illegal. This provision does not apply if information is only temporarily (i.e., hours, not days!) or automatically stored for technical support reasons (e.g., cache) on the providers' servers. In that case, they are not considered to be able to manage that information. The legal consequences of current criminal and administrative laws apply if co-responsibility has been determined according to these provisions. Providers will be treated in the same manner as network operators with regard to telecommunications services: they will not be held accountable for information to which they only provide access.
In short, these provisions hold service providers liable for (parts of) content stored on their own server that they themselves have provided or for which they could be reasonably expected to be aware of containing illegal information and for which they could have blocked access. However, general provisions as laid down in the aforementioned bodies of laws have not been revised and could be applicable to activities regarding teleservices. Therefore, we will first address those provisions before discussing the new elements of the luKDG related to content.

All of the offences mentioned above, (which are individually and specifically defined in the Criminal Code and described below), refer to paragraph 11 (3) in which publications were previously defined as sound and visual recordings, pictures and other illustrations. In the most current amendment, introduced in Article 6 of the luKDG, “data storage devices” are included as well.

6.3.3.1. Defamation

Current defamation provisions in the Criminal Code relate to different situations in which defamation can occur: statement of facts that are false, statement of facts that are true; criminal consequences if defamation takes place publicly or privately. In any case, full responsibility of authors is presumed, although they might be calling on free speech provisions of GG in conjunction with pleading justification on the basis of the protection of legitimate interests if the author has complied with “his duty to take care as stated in (Art. 193).”

6.3.3.2. Other Intrinsically Harmful Content

The law distinguishes several categories of offence relating to pornography:

- pornographic works offered or made accessible to persons under the age of 18, and importing pornographic works (this refers to “simple” pornography which may be distributed to adults);
- broadcasts of pornographic performances;
- pornographic works that show violence, sexual abuse of children or sexual activities with animals.

Many activities involving hate speech, holocaust denial, discrimination, racism, incitement to violence and war fall under a special section in the Criminal Code dealing with issues of public order and state security. German law enforcement authorities believed that these provisions were certainly applicable to information disseminated on the electronic highway even before the enactment of the provisions of the luKDG. They required access providers to block their subscriber’s access to illegal content. This was done on a case-by-case basis. Two of those will be briefly described here.

CompuServe was ordered to pull all the adult-oriented Usenet newsgroups off its system by German officials who said making them available there was against the law. Because there is no way to stop only German customers from being able to access those newsgroups, the ban was affecting customers worldwide. A key issue was the availability of content to minors. The suspension was discontinued after CompuServe introduced a number of parental controls and content restriction tools.

A second case regarded the availability of pages containing criminal information (with respect to art 129a and 130a; see above) that could be called up via provider’s access points and network nodes. In September 1996, German criminal law enforcement officials sent out notification to service providers that they would run the risk of criminal investigations by continue to provide access to a Web page of a magazine that is banned in Germany, Radikal. The access also consisted to providing links to a Dutch Web site containing this Web page. They could be indicted of aiding and abetting criminal activities allowing this page to be called up via their access points and network nodes. German Internet
providers, joined in the Internet Content Task Force (ICTF), had to block access to the Dutch Web site, containing 3100 personal and commercial home pages. Following protests on the blocking included widespread mirroring of Radikal. Without an agreement or verdict about the liability of providers, many networks continue to provide access in the Spring of 1997.

There are more cases that apply to publications containing harmful and illegal content which were not disseminated on the electronic highway, but in print media, radio and televisions or by post and telecommunications networks. The consequences of these cases could possibly apply to activities conducted on the electronic highway.

The IuKDG aims to provide further stimulus to self-regulatory measures by parties involved in the dissemination of content over the Internet. These would be add to those already conducted by the German Internet Content Task Force (ICTF) of the Internet Media Council. The ICTF includes most commercial providers in Germany, users, lawyers, politicians, etc. The ICTF believes that providers bear a moral and legal (co-) responsibility for information disseminated on the electronic highway. Therefore, their objective is to develop and manage strategies, to establish guidelines that make it possible to integrate Internet services into the larger context of society, and to adopt a set of uniform standards that would avoid abuse in conducting business on the electronic highway. For example, the ICTF has developed proposals to establish of a hot-line for reporting harmful and illegal content, and to co-ordinate technical measures for blocking access.

6.3.4. United Kingdom

6.3.4.1. Defamation

In the UK, defamation law is a common law artefact of over 400 years of evolution, balancing conflicting principles of freedom of speech and press on one side and protection of individual dignity on the other. The pace and nature of this common law evolution is slowed by the rules of *stare decisis*, so that periodic legislative adjustments have been made. The *Defamation Act 1996* is the first such adjustment since 1952, and takes particular account of electronic highway developments. The intervening years have seen two marked trends in case law: an increase in the ability of plaintiffs to establish defendants' liability and a rapid growth in the size of judgements. In addition, the reach of the law has expanded greatly with the growth of information networks, with large judgements being granted against foreign publishers on the basis of very small exposure within the UK. The new Act does not make fundamental changes, but does attempt to modernise some existing defences to liability in order to reflect difficulties created by new technologies and media globalisation.

The underlying principles of English common law allow a *prima facie* assertion of liability against a defendant who voluntarily communicates a (direct or indirect) defamatory statement to a third party. There is a rebuttable presumption that the statement is false, and the plaintiff need not

---

217 In recent case law, the *Norwich Union, Hallam-Baker v. Godfrey*, and *Asda* cases all involved allegations of defamation over email or Usenet. In each case, the defendant settled out of court with the plaintiff.


220 *Belt v. Lawes*, 1882 LIT 359, 361.
demonstrate the defendant's intent to defame or had faith. In cases where the publication is written or recorded (libel), the plaintiff need not demonstrate proof of actual harm.

The normal defences are: "justification" (proof that the statement is substantially true); "fair comment" (non-malicious opinion, based on provable facts, on matters of public importance or the conduct of officials); "absolute privilege" (applicable to Parliamentary statements and fair and accurate court reports); "qualified privilege" (non-malicious publication that advances a "legal, social or moral duty"). Others that will be revisited below are "innocent dissemination" and "unintentional defamation." These defences are very complex in practice, and the costs of litigation are greatly increased by the need to resolve their convolutions. This trend seems likely to increase as the situations in which defamation occurs depart further from the experience behind the common law principles. It should also be recognised that the costs create uneven protections, since neither contingency fee arrangements nor legal aid are available in defamation cases in the UK. It is also noteworthy that English law does not recognise a "public figure" defence.

The law was heavily weighted in favour of the plaintiff. This reflects history; libel did not develop as an action on the case (in which case proof of damage would be required) but as a derivative of criminal libel laws intended to deter speech that threatened to cause a breach of the peace; the truth of the statement or its importance to the public at large was thus beside the point. Defences that protect free speech rights were a later development that modified but did not replace this basic position.

The standard defences may be of limited utility to electronic highway defendants. For example, a justification defence must be supported by evidence of the truth of the statement that will satisfy a court of law. This certainly excludes hearsay, and it may prove significant that electronic documents, even with digital signatures are still classed as hearsay in the UK system. By contrast, in the US a plaintiff must prove the falsity of defamatory statements in matters of public interest, and the German Constitutional Court has similarly held that the Basic Law precludes press liability for non-negligent publication of erroneous factual allegations in matters of public interest. Finally, the European Court of Human Rights found that requiring defendants to prove the truthfulness of their allegations in cases involving public figures contravenes the free speech protections of Article 10 of the ECHR. Attempts to reverse the burden of proof in the UK have failed for lack of support.

The Defamation Bill 1996 redefines the responsibility for publication of defamatory statements to explicitly exclude secondary distributors (such as access providers, ISPs, carriers, newsagents, booksellers, libraries, etc.) who "did not know, and were not negligent in not knowing" about the defamatory content of the material they distributed. This is known as the defence of innocent dissemination. The Act does not clarify the circumstances under which users are beyond the

---

221 Cassidy v. Daily Mirror Newspapers, 1929 2 KB 331, 354.
224 Robertson and Nichol, op. cit. p. 86-93.
225 E.g., Johnson, A. and C. Dyer, 'Scapegoat' Doctor Wins Libel Damage of 625,000, The Guardian, 24 Feb. 1996 - the defendant was also liable for legal costs of 500,000.
229 Lingens v. Austria, 8 EHRR 407, 1986.
231 For an analysis of this Bill, see Akdeniz, Y. Recent Developments on UK and U.S. Defamation Law concerning the Internet at La Letter de l'Internet Juridique, June 1996.
"effective control" of operators. This question will need to be revisited over time, since even with current technology it is theoretically possible to screen all messages and users.

When the Defamation Act was first introduced in the House of Lords, the Parliamentary Under-Secretary of State indicated that ISPs would be specifically covered by Sec 1(3)(e). In the House of Commons, Sec. 1(3)(c) was amended to cover those who "operat[e] or provid[e] any ... system or service by means of which the [defamatory] statement is ... made available in electronic form." This change was urged by press agencies to ensure that they were covered by the Act, but would seem to cover ISPs as well.

Another development during the drafting process was an abortive attempt to make the plaintiff bear the burden of proving that the defendant acted unreasonably in distributing a defamatory document, on the grounds that the necessary knowledge would only be available to the defendant. This seems at odds with the identical burden of proof of negligence in personal injury cases.

6.3.4.2. Other Intrinsically Harmful Content

The Obscene Publications Acts of 1959 and 1964 form the main legislative weapon against obscene material, defined as follows:

"For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."

It is an offence to publish or possess an obscene article for profit. Publishing includes:

"(a) Distributing, circulating, selling, letting on hire, giving or lending, offering for sale or for letting on hire.

(b) Where the article contains or embodies matter to be looked at or a record, showing, playing or projecting."

Computer disks are “articles,” but electronic transfers are not. The Criminal Justice and Public Order Act 1994 (CJPOA) added the words “or, where the matter is data stored electronically, transmits that data” to (b) above.

Under the 1964 OPA, it is an offence to “have an obscene article in ownership, possession or control with a view to publishing it for gain.” Again, the new definition of “publishing” covers Web or ftp sites that charge for access to obscene materials.

Sec. 43 of the Telecommunications Act 1984 proscribes sending “by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.” The significant term is “public telecommunications system,” which is not limited to the PSTN telephone system. However, it does not apply when a public telecommunications system outside the UK is used to send a message into the UK, even when the transfer has been initiated from inside the UK. It also exempts local area network and leased line

232 House of Lords Debates, v. 570, col. 605, 8 March 1996.
233 House of Commons Standing Committee A col. 4, 6 June 1996.
234 Obscene Publications Act 1959, Sec. 1(1).
235 Obscene Publications Act 1959, Sec. 1(3).
236 See reports of R. v. Arnolds; and R. v. Fellows, London Times, 27 September 1996. Also, the author of the Internet Bible, Jason Manger, was sentenced in March 1996 to one year’s imprisonment (suspended), £1000 costs, and forfeiture of computer equipment and pornographic material for selling hardcore pornographic material to customers all over the world.
transmission unless the message "touches" a public telecommunications system.

The offence of child pornography is not grounded simply in the obscenity of the material itself, but in the abuse involved in its production. The Protection of Children Act 1978 proscribed the use of children in pornographic photography even when they were not otherwise abused. The CJPOA amended the definition of "photograph" to cover electronic images, including "simulated" child photography produced by purely electronic means from legal source materials. The CJPOA provides:

"it is an offence for a person (a) to take, or permit to be taken or to make, any indecent photographs or pseudo-photographs of a child; (b) to distribute or show such indecent photographs or pseudo-photographs."

This redefinition appears to depart from the original motive. It may reflect a belief that those who produce such simulated images will go on to abuse children or to eliminate a difficult evidentiary hurdle in the introduction of apparent photographs at trial.

Finally, the Criminal Justice Act 1988 is affected by the CJPOA redefinition of "photograph" in that it makes possession of a (simulated or real, photographic or electronic) pornographic image of a child an offence. These laws have been used successfully in a number of different cases of Internet distribution and possession in computer files.

Despite these legal changes, in August 1996 the Clubs & Vice Unit of the Metropolitan Police wrote to all Usenet News nodes in the UK enclosing a list of newsgroups felt to contain obscene or dangerous materials and suggesting that voluntary blocking of these groups would obviate the need for expensive police investigations. In almost every case, the groups were dropped. Discussing this initiative, the Unit Commander, Mike Hoskins stated that he was obliged to do something about illegal material on the Internet, and saw three options:

- do nothing;
- prosecute ISP under the Protection of Children Act 1978 and the Criminal Justice Act 1988; or
- work with ISPs towards a self-regulatory solution.

The same office subsequently established a contact point where citizens could report new newsgroups containing inappropriate content. UK ISPs have subsequently sanitised this approach through a voluntary Code of Conduct. Similar "voluntary" procedures have been tried in the United States, while Germany has used more direct case-by-case blocking measures with mixed success. The legal issue is one of free speech. At one level it is argued that this amounts to censorship without public debate (in the US the issue of prior restraint would also be raised), but the police action was simply a request.

Pyramid schemes conducted over the Internet are specifically prohibited under the Trading Schemes Act. An interesting jurisdictional issue has arisen with regard to the Titan stock-trading scheme, which fell foul of UK law and moved to the Netherlands, continuing to target UK citizens via

---

238 Williams Committee, Obscenity and Film Censorship, HMSO, Cmd 7772, 1979.
240 "Operation Starburst" (1995), a world-wide paedophile ring exchanging images over the Internet; R. v. Arnolds and R. v. Fellows, a paedophile site at Birmingham University in which the judge ruled for the first time that a file stored on a hard disk was the same as a photograph and R. v. McLeish, a case stemming from Operation Starburst in which the defendant dispatched pictures documenting his own abuse of children.
241 R. v. Sharp, the first Internet pornography case in the UK and R. v. Crumpton, the first UK jail sentence involving Internet pornography.
the Internet. The *Computer Misuse Act* specifically states that its jurisdiction extends to any country provided the UK has some contact with the crime.

6.3.5. United States

6.3.5.1. Defamation

The UK defence of innocent dissemination closely resembles the exemption found in the 2nd *Restatement of Torts* in the US that exempts those who only "deliver or transmit" defamatory statements unless they "know or have reason to know" of their defamatory character. Recent US cases have begun to clarify the situation. In the *Cubby* case, the common law of libel, holding that "republication" of defamatory material triggers liability, was reversed because the judge viewed the ISP as "more like a bookseller than a publisher." Thus, the ISP could not be expected to know what its users were posting and had no editorial control over them. Judge Leisure based his reasoning in part on *Smith v. California*, an obscenity case, creating an interesting parallel that suggests across-the-board limits to ISP liability. He also made much of the fact that the private forum in which the alleged defamation occurred stood in contractual relationship to the ISP; contracts tend to limit tort liability compared to other sorts of relationship. However, the reasoning in the *Smith* case did not depend on this.

The *Stratton Oakmont* case was dropped, but the judge declined to reverse an interim ruling that Prodigy could be held liable for comments posted on its bulletin boards because it held itself out as a 'family service,' actively censored material appearing on its fora and provided its moderators with software tools to facilitate screening posts for 'offensive' words. The recently-overturned *Communications Decency Act* contained a clause specifically aimed at overturning this decision by including a "good faith" defence and specifically stating that ISPs are not republishers.

A related aspect of defamation law in the US concerns the position of public figures. Following Justice Brennan’s decision in *New York Times v. Sullivan* (1964), public officials can win defamation suits only by proving actual malice. The motivation is the preservation of vigorous public debate, with its inevitable errors of fact. Over the years, this was applied to "public figures," people who satisfy Justice Powell’s definitions in *Gertz v. Robert Welch, Inc.* (1974):

"In some instances an individual may achieve such pervasive fame or notoriety that he becomes a public figure for all purposes and in all contexts. More commonly, an individual voluntarily injects himself or is drawn into a particular public controversy and thereby becomes a public figure for a limited range of issues. In either case such person assume special prominence in the resolution of public questions."

Almost everyone on the Internet is (or can easily become) a "public figure" according to the second of these definitions. While these people may not be "important" in an objective sense, they also have another characteristic essential to the diminished protection accorded them: easy access to self-help commensurate with the injury they suffered.

6.3.5.2. Other Intrinsically Harmful Content

Liability typically depends on the legal analogy applied to computer information systems. With regard to obscene material there are two significant differences between the US and other countries.

First, *obscenity* is measured against a *patchwork of local standards*. The determinate test comes

---


from *Miller v. California*; material is obscene if:

(a) "the average person, applying community standards would find that the work, taken as a whole, appeals to the prurient interest,

(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and

(c) whether the work, taken as a whole, lacks serious literary, artistic, political or scientific value."

Courts have generally refused to develop or apply national standards and have warned carriers to be wary of differences between the states - the legal rule seems to be that the standards (according to the famous *Miller v. California* "local standards" test) of any jurisdiction where the material can be received may be used.

Second, mere possession is not a crime. As Thurgood Marshall put it in *Stanley v. Georgia*:

"Whatever may be the justification for other statutes regarding obscenity, we do not think the privacy of one's home. If the First Amendment means anything, in means that a State has no business telling a man, sitting alone in his own house, what books he may read, to what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."

The individual only leaves this "zone of privacy" when he connects his computer to a network or telephone system, and the State may legitimately regulate movements of material. In *US v. Orito*, the Supreme Court held that Congress had the power to prevent obscene material "entering the stream of commerce either by public or private carrier."

Speech that is not obscene may be regarded as indecent. Indecent speech is protected by the First Amendment, though it can be regulated in the face of "overriding government interest." In the *Pacifica* case on which this reasoning is based, the Court upheld the diversion of indecent material to time periods when children were less likely to be exposed (like the 9 PM "watershed" in UK broadcasting). This suggests a clear precedent for sites demanding proof of age.

As regards child pornography, the Supreme Court held in *New York v. Ferber* that it lay outside the First Amendment protections because:

- the use of children to produce the material can harm their physical and mental well-being;
- the *Miller* standard is unsatisfactory;
- the financial gain involved in selling and advertising this material provides incentives to engage in activity (production) prohibited throughout the states;
- the value of permitting minors to perform or appear in lewd exhibitions is negligible at best; and
- earlier Court decisions are compatible with classifying child pornography outside First Amendment protections.

The US Code (Title 18, Sec. 2252) forbids "knowing foreign or interstate transportation to reception by any means including, for example, visual depictions of minors engaged in sexually explicit conduct which have been converted into a computer-readable form." It goes on to proscribe knowing possession of "3 or more books, magazines, periodicals, films, video tapes or other matter which contain any depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or

---

247 In *US v. Thomas*, a couple who ran a BBS in California were convicted according to the standards of Tennessee. This case is felt to be determinate as regards liability and jurisdiction.

transported, by means including computer.” Even an individual who did not have the requisite 3 images
might be caught using system backups or restoration of erased files provided the individual could also
have restored those files. In the former case (backups) the system operator would probably escape
liability under the “knowing” requirement, unless he or she had reason to believe (e.g. through having
received a complaint from another user) that the backups contained illegal materials, in which case she
may be regarded as having “constructive knowledge” of their contents.

The most noteworthy development in legislation concern the Telecommunications Act of 1996,
which contains the Communications Decency Act (recently struck down in Reno v. ACLU):

“Title V: Obscenity and Violence - Subtitle A: Obscene, Harassing, and Wrongful
Utilisation of Telecommunication Facilities - Communications Decency Act of 1996 -
Revises provisions of the Communications Act prohibiting obscene or harassing
telephone calls and conversation to apply to obscene or harassing use of a
telecommunications facility and communication. Increases the penalties for violations.
Prohibits using a telecommunications device to: (1) make or initiate any communication
which is obscene, lewd, lascivious, filthy, or indecent with intent to annoy, abuse,
threaten, or harass another person; (2) make or make available obscene communication;
(3) make or make available an indecent communication to minors.

Provides that no person shall be held to have violated such prohibition solely for
providing access or connection to a telecommunications facility, system, or network not
under such person's control. Provides employers with a defence for actions by employees
unless the employee's conduct is within the scope of employment and is known,
authorised, or ratified by the employer. Establishes as a defence to prohibited
communications that a person has taken, in good faith, reasonable, effective, and
appropriate actions to prevent access by minors or has restricted access by requiring use
of a verified credit card, debit account, or adult access code or personal identification
number.

(Sec. 504) Requires cable operators, upon request, to fully scramble or block
programming to which the subscriber does not subscribe.

(Sec. 505) Requires a multi-channel video programming distributor: (1) to fully
scramble or block sexually explicit adult programming so that non-subscribers do not
receive it; and (2) until it complies with such requirement, to not provide such
programming during the hours of the day when a significant number of children are
likely to view it.

(Sec. 506) Allows cable operators to refuse to transmit any public access or leased
access program, which contains obscenity, indecency, or nudity.

(Sec. 507) Amends the Federal criminal code to specify that current obscenity statutes
prohibit using a computer to import or transport in interstate or foreign commerce, for
sale or distribution, obscene material, including material designed, adapted, or intended
for producing abortion or for any indecent or immoral use.

(Sec. 508) Prohibits using any facility or means of interstate or foreign commerce to
persuade, induce, entice, or coerce a minor to engage in prostitution or any sexual act for
which any person may be criminally prosecuted.

(Sec. 509) Provides that no provider or user of an interactive computer service shall be
held liable for any voluntary action taken to restrict access to, or to enable information
content providers to restrict access to, material that the user or provider considers to be
objectionable, whether or not such material is constitutionally protected.

Subtitle B: Violence - Directs the FCC, if it determines that video programming
distributors have not, within one year, voluntarily established rules for rating programming that contains sexual, violent, or other indecent material about which parents should be informed before it is displayed to children and voluntarily agreed to broadcast signals that contain such ratings, to: (1) establish an advisory committee to recommend guidelines and procedures for rating such programming; (2) prescribe such guidelines and procedures; and (3) prescribe rules requiring programming distributors to transmit such rating to permit parents to block inappropriate programming. Directs the FCC, not less than two years after enactment of this Act, to require apparatus designed to receive TV signals that are shipped in interstate commerce or manufactured in the United States and that have a picture screen of 13 inches or greater (measured diagonally) to be equipped with a feature designed to enable viewers to block display of all programs with a common rating. Authorises the FCC to allow apparatus manufacturers to comply with such requirement using alternative technology that meets certain standards of cost, effectiveness, and ease of use.

(Sec. 552) Encourages broadcast television, cable, satellite, syndication, and other video programming distributors to establish a technology fund to encourage electronics equipment manufacturers to facilitate the development of technology which would empower parents to block programming deemed inappropriate for children and to encourage availability of such technology to low income parents.”

The most troubling aspects of this Act, from the viewpoint of civil libertarians are:

- it criminalised transmission with intent to annoy, threaten or harass;
- it criminalised transmission to individuals known to be under the age of 18; and
- it criminalised transmission that may be received by individuals under the age of 18.

Suits were filed the day the Act became law. On June 26, the U.S. Supreme Court, 7-2, decided Reno v. American Civil Liberties Union, striking down several provisions of the CDA. The majority opinion by Justice Stevens held that the provisions of the CDA concerning “indecent transmissions” and “patently offensive displays” constituted undue prior restraint in violation of the First Amendment. The Court afforded the highest level of First Amendment protection to Internet speech. Justice O’Connor, joined by Chief Justice Rehnquist, dissenting in part, found that the “indecency transmission” and “specific person” provisions of the CDA are constitutional “as applied to a conversation involving only an adult and one or more minors.” The government argument was based three “free speech” precedents. Ginsberg allowed restrictions on the right of minors to choose what sexual material they may read and see. However, the judge pointed out that Ginsberg allowed parents to provide access to pornography to their children, which the CDA did not. The Pacifica case turned on the ease with which minors could gain access to the medium in question. The Reno decision contrasts the “intrusive” nature of the broadcast medium with the more deliberate action required to obtain access over the Internet. Renton concerned a zoning ordinance designed to exclude adult theatres; the majority in Reno pointed out that this decision was based on property values and crime rates rather than permissible speech.

In view of the discussion of telecommunications and broadcasting above it is highly significant that the distinction between the Internet and broadcast is central to the Reno decision. Regulation of broadcasting is justified by frequency scarcity and the “invasive” nature of broadcasting. The Court failed to find these elements on the Internet and thus found “no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.”


The government also cited the CDA’s “Good Faith” defence to prosecution if one “has taken, in
good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent
access by minors.” The lack of “effective” means of limiting access undermines this defence. The Court
cited the availability of software-based parental control mechanisms offered by most ISPs and proposed
legislation that would make it mandatory to offer them. The software is not always effective in
screening for sexually explicit images, and there is no effective mechanism to verify a user’s age. Since
there is no practicable way to screen out minors while still permitting adults to access materials, the
dissent found the CDA to be unconstitutional because it was “akin to a law that makes it a crime for a
bookstore owner to sell pornographic magazines to anyone once a minor enters his store.” The only
way to avoid liability is to refrain completely from indecent speech; this forced silence impinges on the
First Amendment right to make and obtain this speech and, for all intents and purposes, “reduces the
adult population [on the Internet] to reading only what is fit for children.”

After this decision, several prospective bills have surfaced. The “Internet Freedom and Child
Protection Act” (H.R. 774) requires ISPs to provide screening software. The “Family-Friendly Internet
Access Act of 1997” (H.R. 1180) would require Internet Access Providers to supply screening software.
The “Child Safe Internet Act of 1997” (not yet introduced) would also provide parents with access to
screening software, protect minors from sexual or violent on-line content, create a felony for posting
indecent material in a “child-safe” chat room, shield providers who implement rating systems and
require warning labels on browser software. The Administration’s A Framework for Global Electronic
Commerce finds that, to the extent filtering technology is available, content regulations traditionally
applied to the broadcast media would not be applied to the Internet. The Administration supports self-
regulation, ratings systems and technical solutions and states that “unnecessary regulation could cripple
the growth and diversity of the Internet.”

What has surprised many is that the court did not simply strike down the CDA on the grounds of
breadth but held that “indecent speech” is too vague to be criminalised on the Internet and granted the
Internet full First Amendment rights. While the Administration seems to feel that Internet speech may
be free from broadcast standards, others feel that cable and broadcast itself will be the next to have First
Amendment protections restored.

Other Content-Based Issues

There are some cases and statutes that deal with Internet fraud. At the federal level, Virgin
Atlantic Airways were fined $14000 in November 1995 for “misleading advertising” - in the event, they
simply failed to update an airfare reported on their Web site. The FTC has been considering an
extension of advertising standards to the Internet as well. In a case with implications for jurisdictional
questions, Georgia Institute of Technology was sued in France for a description of its French program -
the description was in English, while French law requires all advertising (seen) in France to be in
French (the suit was dropped). Finally, the A Framework for Global Electronic Commerce envisages a
variety of anti-fraud measures. In addition, California has an Internet Fraud Statute.

By far the most important category of “fraud” is unsolicited commercial solicitation (junk email,
Spam, etc.) As noted above, the FTC is carefully investigating the legal and economic issues in a series
of workshops. Beyond this, a number of important cases and a scattering of laws are beginning to map
out the boundaries of public and private interest in this area.

The major case is CompuServe v. CyberPromotions, Inc. in which an ISP is suing a client for
trespass to chattel based on the latter’s persistent sending of unsolicited commercial email. Subscribers

251 The majority opinion was even more pointed. As Justice John Paul Stevens noted, this would be “like
burning the house down to roast the pig.”
pay for time spent on-line, so the processing of the messages imposed real costs on the recipient. The ISP asked the client to desist, and implemented software screening when this was ignored. The client circumvented the screening by falsifying its identity. Eventually, the ISP other customers began to complain. On 3 February Judge Graham (US District Court, Southern Ohio) issued an injunction against the client, finding the latter’s actions raised a viable claim for trespass to chattel.

This relied on Ohio law and the Restatement (Second) of Torts. Section 217(b) of the Restatement provides that a trespass to chattel may be committed by “intentionally using or intermeddling with chattel in possession of another.” ‘Intermeddling’ is defined as “intentionally bringing about physical contact.” The court found that electronic signals generated and sent by CyberPromotions' computers were sufficiently tangible to support a trespass cause of action, citing decisions recognising hacking as trespass. The response that the defendants had not physically dispossessed or interfered with the plaintiff’s use of its equipment was rejected on the grounds that the value may be impaired even if the physical condition is not damaged. The defendant’s concealment of its identity forced CompuServe’s computers to store undeliverable messages, diminished the value of CompuServe’s equipment and supported a claim of financial injury based on cancelled subscriptions.

The defendant mounted three defences, all of which were rejected:

• By allowing its subscribers to receive email, CompuServe had consented to use of its property - the plaintiff's request the defendant cease sending the bulk email disposed of this.

• CompuServe was a public utility - under Ohio law, this means that it provides a “public service” and its operations are a matter of “public concern.” The judge found that CompuServe's operations were not essential to society (since alternatives existed) and were thus not a public service. Moreover, since consumers can choose among many ISPs the operations were not a matter of public concern.

• Unsolicited email is protected by the First Amendment - the judge held that the First Amendment protects citizens against the government rather than each other. Moreover, he noted that “[t]here is no constitutional requirement that the incremental cost of sending massive quantities of unsolicited advertisements must be borne by the recipients.”

At the legislative level, Nevada and Connecticut have pending bills252 that would prohibit the use of unsolicited email for consumer marketing without a pre-existing business relationship (Nevada) or prior consent (Connecticut). A federal precedent is the Telephone Consumer Protection Act of 1991 that prohibits sending unsolicited facsimile advertisements (from facsimile machines or computer fax modem boards). The basis for the law was a desire to prevent the shifting of costs to recipients, and it makes exemptions for pre-existing relationships and express consent.

Finally, the Senate has begun consideration of the Unsolicited Commercial Electronic Mail Choice Act of 1997 that would require advertisers to label their emails in a manner that would permit users to request ISPs to screen them out.

6.4. SUMMARY AND COMPARISON

We begin with a summary discussion that highlights the answers to research questions 1-3. The first part, “Issues Arising,” answers the first research question, while the second, “Initiatives,” sketches the answers to the second two questions, describing legislation and other initiatives. The section concludes with a short comparison of the surveyed countries.

6.4.1. Issues Arising

In each of the surveyed countries the issue of harmful content regulation is the most visible one

252 Nevada Senate Bill 13, Connecticut House Bill 6558.
in the debate on the electronic highway and the one were governments have felt most pressure to act. The harm is associated with the availability of specific types of content on the Internet; the effects of viewing this content; and the social costs of providing the content. The distinction between what is harmful and what is illegal content is drawn differently in the different countries.

The legal issues that arise on the electronic highway are defamation, other forms of intrinsically harmful content and the transmission of fraudulent material over the Internet. Defamation, covering both slander and libel, is regulated differently in each country. The particular aspects of defamation over the Internet concern the placement of liability in terms of persons and acts and the choice of law forum. Specific problems arise with defamatory material on the Internet because while liability is normally fixed on the author, the ease of access to the medium and the difficulty of fixing identity on the Internet make the situation less transparent.

Other intrinsically harmful content includes pornography, hate speech, terrorist information, sedition, blasphemy and racism. The exposure of sensitive populations to offensive materials brings out the conflict between censorship and free speech. However, laws in all countries seem to be moving, at different rates, from blanket prohibition on specific content into the direction of a multi-tiered approach combining legislation, self-regulation and the introduction of technical means of content-blocking.

Other content-based issues are illegal trading schemes and Spam and more specifically, how to stop the proliferation of these unsolicited commercial emails and gambling chain letters on the Internet.

6.4.2. Initiatives

6.4.2.1. International

As mentioned, there are few international legislative initiatives. With regard to harmful content, there have been calls for international regulation of liability and co-ordination with regard to the distinction between harmful and illegal content, as well as somewhat more controversial calls for common ratings systems. For illegal content, the proposals stretch to adoption of a certain minimum set of common criminal law standards. One particular difficulty in this respect concerns the difference between nations where mere possession is an offence and those where certain types of transmission are required to create criminal liability. However, the calls for international police co-operation for specific types of illegal content (e.g. child pornography) do seem likely to bear fruit.

6.4.2.2. France

The applicability of existing legislation to the Internet has been largely settled by case law. The distribution of defamatory and illicit pornographic material is punishable regardless the medium used for distribution. For public debate's sake, an exception is made for defamation concerning public figures. Hate, litigious and discriminatory speech and the denial of crimes against humanity are punishable as well when expressed on the Internet. The issue of who is liable for harmful or illegal content has not yet been resolved by French legislation. In 1996, the French government had to withdraw legislation on government content control on the Internet. It had proposed an a priori exemption from criminal liability for ISP's as long as the ISP's provided their clients with a technical content control device and blocked access to sites deemed unethical by the government. While the latter aspect was ruled by the Conseil Constitutionnel to be against the constitutional right to free speech, the obligation for ISP's to provide parental control software was left in force. However, the status of ISP's is still obscured by the awareness that this requirement encompasses many practical difficulties. Recently, the French government pragmatically leans towards self-regulation of content: "Netiquette".
6.4.2.3. Germany

The two main legal problems are the applicability of laws to the Internet and fixing content liability. The German criminal code and other legislation outlaw the dissemination of various categories of harmful and illegal content, like defamation, pornography, racism and holocaust denial, while these laws recently have been made explicitly applicable to the electronic highway. In addition, the German Jugendschutz monitors the electronic highway for content harmful to children and young people. The new Information- und Kommunikationsdienstegesetz holds ISP's liable for both content they themselves stored on their server and for content users stored there if the ISP could reasonably be expected to be aware of any illegal content. Also, the new law sets standards for self-regulation of content.

6.4.2.4. United Kingdom

Publishing defamatory material on the Internet is punishable, except for the defense of innocent dissemination, as has been settled through case law and the Defamation Bill 1996. Also, law provisions on the distribution medium for child pornography and the act of “publishing obscene material” have been redefined to fit the electronic highway. ISP's in the UK have come up with a Code of Conduct to deal with harmful content on their servers. Pyramid schemes conducted over the Internet are specifically prohibited under the Trading Schemes Act.

6.4.2.5. United States

Defamation on the Internet is punishable, with two exemptions: the notion of innocent dissemination and defamatory material concerning public figures. Case law has set standards on when obscene material on the electronic highway is illegal to balance privacy concerns. Child pornography is punishable, regardless the medium used for distribution. In 1996, the Supreme Court made the government withdraw several provisions of the Communications Decency Act that applied to the Internet. The provisions criminalised transmissions on the Internet with intent to annoy, harass and threaten and transmission to individuals known to be under 18, or which might reach individuals under 18. These provisions were found to be in violation of the First Amendment. Both Access Providers and ISP's are now required to provide parental control software. Internet fraud and Spam dealt with by case law and Federal and State statutes.

6.4.3. Comparison

The following Table, drawn from the country summaries above, briefly summarises the positions of the countries on several broad issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defence of innocent dissemination</td>
<td>No</td>
<td>Yes¹</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Private lines OK?</td>
<td>Unclear</td>
<td>Unclear</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Mere possession OK?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Revisionism OK?</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Spam OK?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Speech protection?</td>
<td>Declaration of the Rights of Man, Art. II</td>
<td>Constitution, Art. 5</td>
<td>No</td>
<td>Constituion, 1st Amendment</td>
</tr>
</tbody>
</table>

¹. Specifically, this is based on the "responsibility" paragraph 5 of Article 1 of the IuKDG.
7. COPYRIGHT

7.1. INTRODUCTION

The electronic highway has radically changed in both quantitative and qualitative ways access to intellectual property, and has therefore challenged various concepts in the different bodies of law (e.g., copyright, patent, trademark) encompassing intellectual property rights (IPR). When faced with such challenges, the first tendency of legal scholars, lawmakers and regulators is to ask how the new circumstances might be reconciled within the existing legal frameworks; only if this first approach does not resolve the issue is there movement towards revising the legal frameworks themselves. As with earlier technological developments such as computer programs, cable television, copy machines, etc., the electronic highway is proving recalcitrant to approaches that fit within the existing framework. This is because of the qualitative changes not only in the intellectual property under consideration, but the surrounding context as well: new actors enter and old ones converge; technologies and activities converge; and the intent behind individual acts and the ability of individuals to control, understand and shape their actions in even their own interests may require different approaches. Although the electronic highway challenges standard concepts in various aspects of IPR, nowhere is this more important than in the realm of copyright law. In this chapter, therefore, we address those issues arising in terms of the widespread access the electronic highway affords within the field of copyright.

In the following section, we will focus on a more general description of the legal issues. We have distinguished among issues occurring in the redefinition of terms and scope, the protected works, and the types of right protected. The description of individual countries surveyed carries this distinction forward, supplemented by extended presentations of efforts, especially in the UK and US, to revise copyright legal concepts in light of the electronic highway.

7.2. LEGAL ISSUES

In general, copyright laws address a number of issues. These can be categorised as follows:

- Protection of works and of people. What are the acts covered by copyright protections? What constitutes a protected work on the electronic highway? Does copyright extend to all works created on the electronic highway? Do new works enjoy the same rights as more traditional ones?

- The type of rights that are protected and the limitations and exceptions to those rights. What is the scope of protection? What rights assign to specific works? Are the same limitations to general copyright applicable on the electronic highway?

Beside these specific issues, some other questions emerge that also appear within other subject areas: what is the applicable law, and how can protected works and rights be enforced on the electronic highway. In our research, we have encountered a wide variety of perspectives on all of these issues, partly as a result of a specific disciplinary approach taken or because of differences in copyright traditions. These differences should to a certain extent come forward in the by-country discussions, below.
7.2.1. Protection of Works and People: Actors and Acts

Copyright laws written before the advent of the electronic highway invoke terms whose definitions have become unclear or inappropriate. Among the important terms requiring redefinition are:

- The actors involved. These include authors, publishers, distributors, users, etc. whose roles and interests have converged or shifted. This is important both in defining rights and in fixing liability; the person who causes an infringement may not be the person best placed to avoid it or to obtain the necessary transfer of rights.\(^{253}\)
- The acts themselves. These include creating works, viewing, copying,\(^{254}\) publication, public display, etc.\(^{255}\)

7.2.1.1. Actors

The people covered or affected by copyright law include: authors; publishers of original works; service providers, broadcasters and network operators; librarians, teachers and scholars; users and “re-users” - multimedia creators, publishers and distributors, authors of web pages, etc.

Service providers and network operators face particularly tricky problems - as with defamation, there are reasons to believe that they cannot practically guard against copyright infringements occurring via their systems and further that they rarely benefit in any direct way from such infringements.\(^{256}\)

Broadcasters, on the other hand, may have technological abilities to limit reception. The ability to limit reception and therefore control content could increase their copyright liabilities. The convergence between broadcasters and other services, set in motion by satellite broadcasts, deregulation (especially relaxation of cross-ownership rules), Web broadcast, etc., will undoubtedly change this position.

Traditional publishers and librarians will find their interests hurt by the advent of new technology due to their relatively high costs and inefficiency. It is possible in the future\(^{257}\) that publishers may produce or libraries stock a single master copy of a document, to which users will be granted access. This raises questions of:

- who should have access and under what terms?
- how and how much authors should be compensated?
- who should participate in collective licensing; how the moral rights of authors should be protected?
- how the administrators of the grid should enter the copyright “value chain?”

---

\(^{253}\) For example, one who publishes a Web page containing links to copyright material has himself made no copies: those who view that page will have made copies, but in all innocence.

\(^{254}\) Should private digital copying be fully subject to copyright, authorised, or prohibited beyond a single copy?

\(^{255}\) For instance, on the Web the act of viewing a work necessarily entails making at least a transitory copy (in the user’s RAM) and, with caching browsers a durable copy on the user’s hard disk.

\(^{256}\) There are legal initiatives aimed at protecting these parties: The US House of Representatives is considering the Online Copyright Limitation Liability Act which exempts online services and ISPs from copyright liability when they have neither knowledge of nor financial interest in such violations. This includes links to illegal material unless they constitute endorsement of that material. The bill is opposed by software publishers who fear an explosion of pirated material and threaten to reduce online sales. The December 1996 conference of the World Intellectual Property Organisation dropped a treaty provision that would have held ISPs, libraries and telephone companies liable for all infringements over their services.

\(^{257}\) This is reflected in e.g. the US National Research and Education Network “Digital Library” idea - cf. Perritt, H. at [ref. To be added]. For the transfer of rights issue in this context, see the discussion of “permission headers” in Section 0.
In addition to those holding primary copyright, the interests of those with neighbouring rights will need to be considered as well.

7.2.1.2. Acts

The other critical element is to define covered works. The principal problems for standard documents are those associated with any new copy and distribution technology. Special problems attend copyright protection for databases; CD-ROMs, user interfaces and web sites.

The facts and information contained in databases are normally not protected in themselves. As compilations, they receive some protection²⁵⁸, though their contents require separate copyright. Databases differ from compilations in three respects: they are indifferent as to what is stored in them; they permit data to be reconfigured at will; and they offer the ability to manipulate, retrieve and otherwise use quantities of data that would not be handled in any other way. The first of these means the selection of material may be irrelevant; the second that the arrangement of material is arbitrary and the third that even a failure to locate material (from a truly comprehensive database) may be of material value. Taken together, this means that selection and arrangement no longer provide an adequate basis for copyright. Another problem of great difficulty and importance is the ownership²⁵⁹ of a database - does it belong to the author, or the owner of the media? A database compiled from one or more separate "works" may be regarded as an adaptation of them. If it has no "off-line" counterpart, it may have no clear author at all. It is even possible to assemble "hyper-databases" from data held (and structured) in different locations - do these have "distributed" owner/authorship? What acts infringe copyright? Such issues have led to sui generis database protection rules. User interfaces belong more to the copyright issues surrounding computer programs than the electronic highway; they are only mentioned here because they arise in the area of Web page design as well as in the more "fixed" arena of software in the ordinary sense.

CD-ROM materials or multimedia products raise special copyright issues because they combine works by many authors, developed under (potentially) different types of copyright protection, and are contained within a single medium with particular means of access and use. They thus share database and user interface characteristics. The degree to which they are regarded as duplicating other specific protected media²⁶⁰ determines the ownership, scope and presumed transfer of rights. As with user interfaces, their connection to the electronic highway is indirect.

Web pages are directly connected to the Internet, and raise some particular issues²⁶¹. In the first place, they are computer programs as well as documents. Moreover, one can create a Web document consisting entirely of inline images and other links to copyright material held elsewhere. The linked material does not appear on the creator's computer and, in the case of inline images, the viewer of the page (who does make a copy) is not even aware that the material is coming from a remote location. The analysis of whether these activities infringe on copyright is complex and goes beyond the scope of this document. There are some questions to which uniform answers have not emerged, in part because the straightforward application of existing law produces unintended effects:

²⁵⁸ In the UK, compilations are covered by the Copyright, Designs and Patents Act 1988. In the US, and the European Commissions proposed Council Directive on Databases, this protection is only available to compilations representing the author's creative endeavour and not mere 'sweat of the brow' (see e.g., Feist Publications Inc. v. Rural Telephone Service Co. Inc. 111 S Ct. 1282 (1991)).

²⁵⁹ For example: a scholar stores the results of a survey in a database to which others have contributed on a University computer. Can the University sell the data; can the scholar take the data to a research institute; who own copyright in the database; and who is the 'author' for the purposes of determining the term of copyright?

²⁶⁰ E.g., films, sound recordings, printed documents, databases.

• Does the creation of a Web page containing links to copyright material violate copyright?
• Does the “publication” of such a page violate copyright?
• Does the user violate copyright?
• Can a Web site owner prevent others from linking to it or its contents?

The answers turn on the scope and intended effect of the implied licence involved in exposing material on a Web site and any difference in law between that exposure and publication. In different countries, the issue may be resolved by appeal to moral rights (not to have the material viewed outside the intended context), inverse passing-off (the right not to have someone claim credit for your work), explicit limitations on the scope of implied licence, flexible notions of fair dealing or even laws against unfair competition. The basic point is the conflict between “use” and “copying.” This is far from resolved.

7.2.2. Type of Rights Protected and Infringement to the Rights

Not only do terms referring to people and to acts require reconsideration, the very legal terms defining the types of rights protected and what constitutes infringement of those rights come into question. Among the terms familiar to copyright law whose meanings might change are included fair use, implied license, de minimus copying, originality, fixation, etc. These need to be adapted to the new environment; their definitions strongly affect the protections available and their impact on creative activity.

Rights are still mainly determined by means (media) of fixation. The main issue in their evolution is the balance of economic, moral and social rights, as expressed in specific rights such as: reproduction, modification, distribution, public performance, public display. Other rights have been suggested: digital transmission or digital broadcast, downloading, partial reproduction, and data extraction; combined or collective rights for multimedia works. Important considerations are:

• Which acts infringe these rights?
• Are these rights appropriate to the authors’ and others’ interests?
• Can they be defined and enforced in practical ways?
• Will their exercise in fact serve the parties interests?

The existing set of rights may not match the uses to which material may be put; without adequate means for transferring and acquiring them, exploitation can be skewed. It is also important to establish limitations, exceptions and co-ordination with other laws and jurisdictions. What may be permissible as fair use in one country may be a copyright infringement in another.

Whatever the rights and their scope, it is the mechanism by which they are acquired and transferred that will determine their effectiveness. The general thrust, whether in contractual terms or not, seems to favour a combination of new technologies and new legal instruments and techniques. On the technology side, new coding schemes are being developed to ensure identification and authentication, and to construct large “clearinghouse” databases of rights, fees, and even protected works to supplement or even replace collecting societies, though the latter would retain important

262 France
263 UK
264 US
265 e.g. Smith, G. op. cit.
266 Dreier, op. cit.
267 To cope with the anticipated glut of "user-defined" works.
functions, especially for substitutable subject matter. Perhaps the ultimate expression of this trend is the "digital library concept" built around three elements: permissions headers; queries; and a procedure for matching the two. All three contain information about the contents of desired and existing documents and the economic terms on which the information can be used. Legally, the permissions header is an offer, the query a solicitation of offers, and the match an acceptance. The legal definitions and status of these objects remain to be settled but their advent is certain. The principal legal issues concern the legal effect intended by the header - outright transfer requires a signed writing, and recordation may provide valuable protections to the conveyance; the grant or transfer of limited permissions must confirm to applicable contract law as to formation, enforceability, repudiation and interpretation.  

7.3. COUNTRY SUMMARIES

In this section, we provide an overview of the legal initiatives in the surveyed countries, looking particularly at the redefinitions of terms involving actors and their acts, and the types of rights protected. Before looking at individual countries, we summarise recent multinational agreements.

7.3.1. Multinational Agreements

The Berne Convention was recently amended by the WIPO Copyright and Performances and Phonograms Treaties. They were hotly contested during the drafting process. At one stage, the draft copyright treaty contained a provision (Article 7) that would have made provisions for a right of reproduction extending to temporary storage in computer memory; it would have effectively precluded Web browsers that improve performance by means of caching. An early version of Article 10 would have held ISPs responsible for all copyright violations over their services by creating a new exclusive right of "communicating to the public." This was vigorously opposed by ISPs, the American Library Association and telephone companies, and was modified at the last minute. Indeed, Article 10 now provides that responsibility for copyright infringements will lie with users rather than ISPs.

The basic thrust of the treaties is to make it easier to pursue copyright violators internationally by applying copyright regimes to non-physical environments. The WIPO copyright treaty determines that reproduction rights and its exceptions fully apply to the digital environment and that storage of a protected work constitutes a reproduction. In addition, it introduces a new right: the right of communication to the public, guaranteeing the exclusive right of an author to authorise access to, or usage of his or her work in any form of electronic transmission. Finally, it prohibits unauthorised removal or alteration of "rights management information" and requires implementing legislation to enforce the treaty provision. Significantly, it also provides (in Article 11) for redress against deliberate circumvention of copy protection and rights management arrangements. The performance treaty is the first to apply to digital transmission of sound recordings, protecting performers and producers. It requires equal treatment of citizens and foreigners and creates a 50-year protection on performance reproduction, distribution and rental.

The European Union has developed several initiatives and directives that relate to copyright in the Information Society. Although these fall beyond the scope of our survey, the Database Directive and the Green Paper on Copyright and Related Rights in the Information Society and its follow-up are setting the rules for many of the initiatives conducted on the national level.

268 See the discussions of digital signatures in Section 0.
269 WIPO Copyright Treaty adopted by the Diplomatic Conference on December 20, 1996; Agreed Statements Concerning the WIPO Copyright Treaty adopted by the Diplomatic Conference on December 20, 1996.
270 Information identifying ownership rights.
7.3.2. France

7.3.2.1. Actors and Acts

The *Code de la Propriété Intellectuelle* (CPI) is the primary law governing property rights in France, as harmonised in July 1995 by EU Directive 93/98. Although the Internet is not explicitly mentioned in the CPI, several court cases have placed the electronic highway within it. The legal definition of works of art includes literary, graphic, audio-visual and photographic works (a definition fitting Web pages), or combinations such as CD-ROMs. French law does not grant (multimedia) works on the Internet different terms of protection than other works or than any other EU country. Databases *sui generis* (i.e. not only their contents) will be protected when the EU Directive on databases is implemented in France.

The *Affaires Brel et Sardou* of August 1996 extended copyright protection to the Internet as a medium for publication and distribution. The Paris *Tribunal de Grande Instance* ruled on 14 August 1996 that French students who put the lyrics of several *chansons* by Brel and Sardou on their personal Web sites violated copyright on two counts: unauthorised reproduction and distribution of protected works. The decision established that Web pages are considered accessible to the public and that works to be found on them can never be limited to private use only. The students were ordered to remove the material. The judges set a clear standard:

[...\] toute reproduction par numérisation des œuvres musicales protégées par le droit d'auteur susceptible d'être mise à la disposition de personnes connectées au réseau Internet, doit être autorisée expressément par les titulaires ou cessionnaires des droits.

One unresolved multimedia definition in France is the status of multimedia works. The CPI distinguishes two classes of works: collective works owned by all of the authors (*œuvres de collaboration*) and collective works owned by the 1st among equal authors (*œuvres collective*).\(^{271}\) The *œuvre de collaboration* is protected for a period of 70 years after the death of the last living author, while the *œuvre collective* becomes public property 70 years after its 1st publication. Authors (or, more properly, their heirs) clearly benefit more by owning an *œuvre de collaboration* but multimedia works do not automatically fall into either legal category.

7.3.2.2. Types of Rights and Infringements

The ease with which copyrighted works are used on the Internet and the scale on which this takes place concern the government and authors. This problem is complicated by the extent of the legal protection authors enjoy in France. However, to date no initiatives to adapt the extent of protection offered by moral rights have surfaced in France.

French authors currently hold a variety of copyrights on the Internet. According to articles L 121-1 to 121-9 of the CPI, authors enjoy *droits moral et droits patrimonial* over their works. Each of these rights has to be respected on the Internet. There is a set of economic rights: the author disposes of the right to authorise reproductions of the work (*droit producteur*), the right to authorise public representations of the work (*droit diffuseur*) and the right to authorise adaptations to the work (*droit*...)

\(^{271}\) Art. L. 113-2. Est dite de collaboration l'œuvre à la création de laquelle ont concouru plusieurs personnes physiques. Est dite composite l'œuvre nouvelle à laquelle est incorporée une œuvre préexistante sans la collaboration de l'auteur de cette dernière. Est dite collective l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé.
In addition, the author is entitled to equitable remuneration for public use of his work. This means that no representation, reproduction or modification of the work may take place without the author's permission. In addition to these rights, French authors enjoy moral rights over their work: the right to assert authorship, the right of first diffusion to the public and the right to respect for the integrity of the work. These moral rights are clearly not economic rights; their goal is to guarantee that the author's work will not in any way be deformed and that the artist will always receive credit for his creation.

When French copyright is infringed on the Internet and this act can be perceived from French territory, the CPI applies. In practice, this means that French authors or their heirs can sue anybody when their copyright has been violated on the Internet, no matter where the server is located. The CPI established a special government agency, l'Agence pour la Protection de Programmes (APP) charged with monitoring media, including Internet sites lacking non-password protection, for copyright infringements, focusing on software programs. French courts have decided numerous cases on the basis of testimony by APP agents, most recently the Brel and Sardou case (see above). Based on this case law, we can distinguish a number of acts on the Internet that constitute copyright infringement in France:

- Diffusion of an unpublished or published work. The use of a copyright protected work on a Web page, in an e-mail, in a Newsgroup, etc, infringes on CPI Article L 121-2 which gives the author the sole right to determine the process and timing of the publication of his work.

- Modifying the work without permission. Digitising a work constitutes an infringement per se under French law. So, when somebody's personal Web site is illustrated --without authorisation-- with a picture of a protected work of art, this act not only constitutes a breach of the reproduction right but also of the right on integrity of the work, because the work has inevitably been transformed into binary format. 272

- A potential violation is triggered by the interactive nature of the Internet. The use of hypertext links on the Net could constitute an infringement of moral rights. By establishing a direct link with another page there is a risk of dislocating that page from its real context, hurting the integrity of the work. So far the issue has not been brought to court.

All unauthorised use of copyright protected works is illegal and as a contrefacon subject to either civil or criminal prosecution by the author or his right-holders. The 1992 CPI subjects contrefacons to criminal prosecution with a maximum punishment of 2 years detention and a fine of FRF 1 million. Article L 122-5 of the CPI formulates two exemptions:

- The droit de citation allows for certain limited forms of reproduction of copyrighted works if certain detailed conditions are met, e.g., when a clear mention of the author's name is made and the work is cited for scientific purposes. However, jurisprudence indicates that French judges are not too keen on sanctioning citation. Citing too much of a work is often deemed to be a form of copying while citing fragments is judged as damaging the work's integrity.

- A second exemption is made for the reproduction of a work for private use only, la copie privée. So, downloading a Web page for non-commercial, personal use is not considered to be a breach of copyright.

The limitations of these exemptions may be illustrated by the Queneau case of May 1997. In that case, a Parisian student was ordered to remove a poem by R. Queneau from his Web site. The student called upon the right of citation and the right of private use, but the court ruled both options out by stating that putting a work up on the Internet means making it accessible to the public. The poem

272 Compare with the 1991 copyright Huston case (Civ. 1o 28.05.91 JCP 91 II no21732) in which the unauthorised conversion of a black and white movie into colour was judged to constitute a breach of the integrity of the work.
was reproduced and made public without the author's right-holders' prior permission and the transformation into binary format constituted an infringement of the work's integrity.

7.3.2.3. Summary

While many of the legal issues described before are experienced in France as well, no specific legal initiatives have been undertaken in this country. The legal issues are dealt with primarily using the current *Code de la Propriété Intellectuelle*. French law has not significantly changed to tackle specific electronic highway issues. Some questions have been resolved by court cases. Here as well, the general tendency is to strictly apply current law in the same spirit as it has been done to more traditional copyright-related issues.

7.3.3. Germany

Similar to other countries, Germany has specific laws dealing with each separate area of Intellectual Property Rights. Although there has been some discussion of revision of the law, copyright and related rights—including author rights and neighbouring rights—are governed by the 1965 *Gesetz über Urheberrechte und verwandte Schutzrechte* (*Urheberrechtsgesetz*, or UrhG). In the beginning of 1996, the Parliamentary Inquiry Commission *Zukunft der Medien in Wirtschaft und Gesellschaft -- Deutschlands Weg in die Informationsgesellschaft*\(^{273}\) started to consider a number of areas where changes in information and communications technology would potentially have great consequences with respect to governance and society as a whole. In its *Zweiten Zwischenbericht*, it dealt with the area of copyright and multimedia.\(^{274}\) The main recommendation of this Commission is not to reform the UrhG in a very far-reaching manner. Rather, legislation should be reactive to technological developments. The June 1997 report of the Commission resulted in the statement of a number of concrete recommendations. Many of these recommendations directly relate to the legal issues described in this report in the section above.

7.3.3.1. Actors and Acts

In the past, several alterations have been made to the UrhG to adapt to the changing circumstances. Most of the recent changes have been initiated on the EU level, such as the protection for computer programs. Directive 91/250/EEC on the legal protection of computer programs provided that computer programs shall be protected by copyright as literary works.

Paragraph 2 of the UrhG indicates the kind of works that are protected. Among these works are, for example, literary, spoken, linguistic works, and computer programs. The listing that is given in this paragraph of the law is not meant to be exhaustive, but is meant to illustrate the different works of creation that are protected. Their common aspect is that they have to be personal intellectual creations. Modification of works and compilation of works are in their turn creative works as well and receive protection. Because of this inconclusive definition and its technology-independent character, no redefinitions of works have been required in Germany. A new or adjusted definition of protected works does not provide any benefits; the current formulation of paragraph 2 of the UrhG\(^{275}\) is broad and flexible enough to also include multimedia products. Yet, there other changes in the environment that have not been deemed necessary a change in legal status. For instance, changes that related to the

\(^{273}\) The commission consists of Members of Parliament, business representatives and academic scholars.

\(^{274}\) *Zweiten Zwischenbericht der Enquete-Kommission Zukunft der Medien in Wirtschaft und Gesellschaft -- Deutschlands Weg in die Informationsgesellschaft: Thema Neue Medien und Urheberrecht.*

\(^{275}\) "(1) Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere... (...) (2) Werke im Sinne dieses Gesetzes sind nur persönliche geistige Schöpfungen."
introduction of CDs or scanners (encompassed by the term “equipment”) could be interpreted in existing law. The most recent major change to the UrhG has been the double legal protection to databases (see below), again initiated at the EU level.

Within the Informations und Kommunikationsdienste Gesetz (IuKDG), article 7 addresses amendments to the UrhG. These amendments cover the incorporation of the EU database directive into German law. This provides databases with a double legal protection. The first covering databases as an intellectual creation by itself, the second giving databases a sui generis protection (paragraph 87a). In that case, a database is not an intellectual creation per se, but has required a substantive investment to be constructed.

A number of issues still remain unclear, among which are the status of Internet links (the report questions whether this is covered by “citation right” stated in paragraph 51), frames and web-sites. In these cases, the inclination is see whether how current copyright can deal with these issues. In that context, the German government believes that actually coming forward with legal initiatives exclusively in the national sphere should not be the first line of action. Both WIPO Treaties already set out a limited need for legal intervention as does the EU Green Paper mentioned earlier. Whether Germany should refrain from modifying its copyright law and await EU harmonisation is will depend on the speed of development and substantive design of these EU proposals.

7.3.3.2. Types of Rights and Infringements

Authors, performing artists, and broadcasting organisations all enjoy various rights as described in the Urheberrechtsgesetz. Most of these are determined by international conventions, indicated earlier in this section. Among the most common ones are moral rights, publication rights, reproduction rights (including sound and visual recordings), distribution rights, public performance rights, broadcasting rights, performers’ rights, broadcasters’ rights, rental and lending rights, etc. There are fair use of works and other limitations to rights mentioned as well that provide users with the opportunity to make use of works without receiving approval or having to compensate the creators. The limitations to right relate to the use of works for

- private use;
- use of short excerpts in connection with the reporting of current events;
- ephemeral fixation by a broadcasting organisation by means of its own facilities and for its own broadcasts;
- use solely for the purposes of teaching or scientific research.

A change related to extension of rights has been formulated in the Rental Right and Lending Rights Directive (92/100/EEC) and has been incorporated in paragraph 27 of the UrhG.

The Zweiten Zwischenbericht of the Parliamentary Enquiry Commission also explored issues related to new media and different rights. Below, we summarise their discussion points.

International copyright presumes the principle of homeland territory. This means that the applicable law is determined by the country in which the copyright and its protection were being used. In many digital transactions, it is difficult to determine where copyright infringement took place. In much the same manner, it is difficult to determine where databases reside. This is complicated by automatic data transport and temporary storage of data. Regarding copyright, general principles (such as free choice of law, forum) should apply.

If an author has given permission for distribution of a creation, he cannot deny subsequent request. However, this exhaustion of rights principle, which traditionally require a physical format, should not be extended to electronically transmitted services.
Private use provisions, formulated in paragraph 53 of UrahG, will also cover the use through digital technologies. A general levy on equipment, similar to blank tape and recording equipment levies, could be considered.

Beside the criminal liability of service providers, one should also consider civil, copyright and press liabilities as well. The responsibility of service providers with respect to copyright infringements is appropriately provided in article 1, paragraph 5 of the new luKDG. However, the practical consequences of this provision should be critically observed in order to perceive legal caveats to this provision with respect to copyright among other legal issues.

The simple electronic download will constitute a public reproduction as indicated in paragraph 15 (3) of the UrahG. Copyright on the digital download of copies from libraries for scientific and educational purposes should not be restricted.

As agreed in article 14 of the WIPO Performances and Phonograms Treaty, producers of sound recordings should be granted an exclusive right to reproduction.

The ease of distribution and quality of copies of original works will only improve in future. This could result in a decrease of compensation for creative works, while at the same time the use of the performance will increase. From the perspective of authors this is obviously not a beneficial development. From the point of view fast and efficient distribution is in the general interest. Compensation methods could be devised that incorporate the value of different uses of creative performances. However, digital request of copies from libraries for scientific and educational purposes should not be restricted.

Producers of sound recordings should, referring to article 5 of the WIPO Performances and Phonograms Treaty, be granted moral rights with respect to be identified as the performer of his or her performances. General provisions of moral rights to this group should not be extended.

7.3.3.3. Summary

The German government's main position is that legislation should be reactive to technological developments. It does not consider radical changes to current law desirable. Current formulation of German copyright law is broad and flexible enough to deal with many challenges that the electronic highway is providing. The most recent amendment to copyright law covers the incorporation of the EU database directive into German law. Most prominent issues yet unresolved relate to jurisdictional issues. In this area, Germany awaits international developments in EU and WIPO fora before developing any national initiatives.

7.3.4. United Kingdom

The basic law providing copyright protection in the UK is the Copyright, Designs and Patents Act (CDPA) of 1988. Interpretation and enforcement rest primarily with the Patent Office. Debate and consultation are still going on about implementation of the WIPO Treaties and the EU Database Directive.

7.3.4.1. Acts and Actors

Under UK law the broadcast "takes place" where it is made, not received, so a French broadcast, for example, cannot violate UK copyright. This is not the case with cable - c.f. CDPA, sec. 6 (3,4 - broadcast, 20 - cable). With regard to databases, the CDPA covers them as compilations (details...
in the discussion of "treaty implementation" below).

More generally, the Patent Office has stated:

"Under UK law (the position in other countries may differ) copyright material sent over
the Internet or stored on web servers will generally be protected in the same way as
material in other media. So anyone wishing to put copyright material on the Internet, or
further distribute or download such material that others have placed on the Internet,
should ensure that they have the permission of the owners of rights in the material."111

With regard to the definitional issues, the then Minister for Trade and Industry, Ian Taylor,
commented in a Commons Debate on 7 November 1996 that he was unwilling to broaden the definition
of "broadcasting" to extend to all forms of digital transmission:

"I am cautious about broadening that definition. The hon. Gentleman will well
understand that I believe that there will eventually be convergence. Even the BBC has
openly announced plans for broadcasting over the Internet. There will be a convergence
of all means of transmission--including cable, telephone and satellite. Broadcasters and
other content providers, including the music industry, will come together in the new
multimedia age.

As I mentioned in the Command Paper issued yesterday in response to the report of the
House of Lords Science and Technology Committee on the information society, we
envisage looking at the regulatory environment in the context of changing industries.
The time is not yet right for that. We have made some pre-emptive moves--for example,
through the regulation by the Office of Telecommunications of conditional access as a
result of the Broadcasting Act 1996. We are well apprised of the changes and well aware
of their significance. It is not sensible to move too far or too fast. We are watching
carefully to see where technology leads."

The proposed EU database directive has led to some discussion in the UK about what
constitutes a database. Some databases, which at present qualify for copyright protection in the United
Kingdom, may no longer do so. However, all databases will be eligible for the newly created "database
right", whether or not they qualify for copyright protection. The new right is aimed at protecting the
investment of money, time and effort that goes into compiling databases, even if they do not qualify for
copyright as "intellectual creations." The new right will last for fifteen years from the completion or
publication of the database, and gives the maker the ability to control extraction and re-utilisation of all,
or a substantial part, of the contents. Existing databases up to 15 years old will qualify for the new right.
Databases currently protected by copyright will retain that protection for the remainder of the copyright
term. This is ambiguous as regards the inclusion of public information, the impact of updates on the
term of protection and the meaning of the term "substantial." It is also silent on matters of (in the case
of databases with interface mechanisms that may be regarded as computer programs) fair dealing.
Current exceptions - for example research, education and library use - continue to apply except where
the Directive specifically requires otherwise (the research exception is limited to non-commercial
research). Certain similar exceptions will apply to database right, but this remains unclear and will need
clarification in the implementing legislation.

In terms of the specific plans for implementation, we note that at present databases are
protected as a "compilation" in accordance with established principles for protection of original literary
works under the CDPA provided that they are recorded (in writing or otherwise). Protection does not
depend on the medium and is given to printed and electronic databases, whether supplied on-line or on

111 At http://www.patent.gov.uk
111 Based on interviews with Patent Office and the BBC Multimedia Centre.
carriers such as CD-ROMs.

Section 1(1) and section 3(1) of the CDPA provide that:

"1(1) Copyright is a property right which subsists in accordance with this Part in the following description of work -(a) original literary, dramatic, musical or artistic works, ..... 3(1) In this Part "literary work" means any work, other than a dramatic or musical work, which is written, spoken or sung, and accordingly includes -(a) a table or compilation."

There is no specific provision for databases in the CDPA, and the term "compilation" is not defined. It has been left to the courts to decide what constitutes a compilation and in what circumstances copyright is deemed to subsist in such a work as an original literary work.

A compilation is protected provided that it is original. The CDPA does not define "originality" but courts have held this to mean that the author did not copy the work from elsewhere, but created it independently by the expenditure of his own skill, knowledge, mental labour, taste or judgement.

The CDPA gives exclusive United Kingdom rights to prohibit or authorise reproduction, translation and adaptation of original literary works (including compilations). There are a number of exceptions including: research; private study; education; libraries and archives; public administration; criticism, review, and news reporting and incidental inclusions.

Implementing the copyright provisions of the Directive may limit the protection, which has in the past been given to databases in which a substantial amount of labour, but little or no intellectual effort, has been invested. Instead, they would be protected them by the sui generis right, which is a new right in English law. Pre-existing databases, which fail to qualify for copyright protection under the Directive, will continue to be protected by existing copyright until the end of the term of that protection.

All databases will be eligible for the new right including those, which are also eligible for copyright protection, provided there has been a sufficient investment in the making of the database.

Articles 6(2) and 9 of the Directive permit exceptions to copyright and to the sui generis right (within certain limits) to be applied at the discretion of Member States. Since many electronic databases are licensed with stringent conditions on use, this raises the question of whether there should be any exceptions to copyright and the new right, particularly in the fields of education and research where licensing appears to be common. There has been no decision on the optional exceptions. Singling out databases for special treatment by providing no exceptions would be seen by the user community as an unwarranted step backwards, and right-holders in other works as unfair.

7.3.4.2 Types of Rights and Infringements

Issues regarding the types of rights and infringements in the UK have arisen with respect to Web pages and the WIPO Performances and Phonograms Treaty. We discuss each of these in turn.

With regard to Web pages, the critical open questions seem to be whether linking and frames constitute infringement, whether links are in any sense preferable to local mirrors, and especially whether using the source code or linking to a portion of a Web page (rather than the page itself) constitutes infringement. On one side, the computer copies involved in viewing and downloading certainly infringe in the ordinary interpretation of the CDPA. However, a key observation seems to be that Web pages may be regarded as computer programs. If so, Sec 50b of the CDPA permits (for certain purposes) what would otherwise be obvious infringing acts of "decompilation." Certainly viewing the page or a portion thereof should be OK. If the computer program analogy is accepted, Sec 50c of the CDPA may even moot the entire question of implied licence. A related question is whether viewing a graphic "out of context" (e.g. by linking directly to that graphic rather than the page

279 Smith, G. op. cit.
containing it) is an infringement. If the implied licence to copy the graphic for viewing purposes is not restricted, this would seem to be permitted. Even if the license is restricted (for instance, by a notice on the site), one might still ask whether it constitutes protected "fair dealing," in which case the implied license is irrelevant. This is laid down in Sec. 29 of the CDPA, but the question of what acts of viewing are "fair dealing" is not resolved. To sum up the Web issue, it seems to be the case that publishing a virtual document (containing links to other documents) does constitute infringement under current law. It is also the case, however, that Web site owners cannot prevent other sites from using links to itself (in whole or part) in their virtual documents. Moreover, no express assertion of rights on the first site can be brought to the attention of a user of the second site, who may be the only person who actually makes a copy of material on the first site. There is some case law suggesting that a withdrawal of implied license could be viewed instead as a derogation from grant. In the UK, arguments based on moral rights (in this case, the right to control the context in which the image is viewed) or inverse passing-off (the right to be protected against other's claims to your work).

In developments related to the issue of Web links, one newspaper (The Shetland Times) obtained an injunction against another (Shetland News) preventing the latter from providing links to articles on the former's Web site. The court held that the headline text used in the link violated the CDPA.

The WIPO Performances and Phonograms Treaty triggered discussion with regard to its requirement for equitable treatment of domestic and foreign performers. In response to a Parliamentary question, Ian Taylor said:

"To my knowledge, our performers are not being treated differently from all other performers. There are variations within the EEA, from country to country. Many of the ways in which our performers feel they might be treated differently in fact relate only to traditional broadcast materials. To that extent, we are attempting to provide a flexible way for performers--while still protecting them--to pursue their interests and get equitable remuneration, without specifying that in statute. As we move forward to new distribution mechanisms, we shall quickly find that the 50:50 split is not tenable. It is in the long-term interests of performers for their material to be distributed more widely rather than for it to be carefully restricted and used less. Content will be king in the new age, putting performers in a much better position."

In commenting on the Performances and Phonograms Treaty, the Patent Office drew particular attention to the following points:

- The failure to reach agreement on provisions that would have clarified the scope of the reproduction right under Article 9 of the Berne Convention and the Performances and Phonograms Treaty in relation to temporary reproductions (e.g. held in a computer memory or on a network server). This was reportedly one of the most contentious issues both leading up to the Conference and at the Conference itself. The Conference eventually agreed that electronic storage "is covered" by Article 9 of Berne and by the Performances and Phonograms Treaty.

- The agreement to limit the scope of the Performances and Phonograms Treaty to aural performances only (i.e. not audio-visual performances), following a failure to agree on the conditions under which audio-visual performances might be included. However, the Conference agreed to adopt a protocol to the Treaty covering audio-visual performances no later than in 1998.

- The deletion of a proposed 'modification right' from the Performances and Phonograms Treaty.

7.3.4.3. Summary

In the UK, the Copyright, Designs and Patents Act of 1988 governs copyright. Interpretation of the meaning of this Act for the Internet rests with the Patent Office, which falls within the portfolio of

---

the Minister for Trade and Industry. The status of the Internet has been evolving through interchanges between Parliament and the Patent Office. A good deal of those interchanges concern provisions of the WIPO treaties and EU directives, especially with regard to performers in the first instance and databases in the second.

7.3.5. United States

In the US, there is a general agreement that copyright law requires a thoroughgoing reform. However, there is less agreement on the nature of those reforms. A major effort in 1995 was withdrawn, the debate surrounding it generated considerable insight into how the US views copyright and the electronic highway.

7.3.5.1. Actors and Acts

Section 2 of the proposed National Information Infrastructure Copyright Protection Act of 1995 (H. R. 2441, S. 1284, henceforth referred to as the NII) made four separate but related amendments to the Copyright Act. First, the distribution right in section 106(3) would have been amended to add the phrase “or by transmission” to the list of methods by which copies of a work can be distributed. Second, the definitions of “publication” and “transmit” in section 101 would have both been amended. The phrase “or by transmission” would have been added to the end of the definition of publication. A new sentence would have been added to the end of the definition of “transmit,” reading: “To 'transmit' a reproduction is to distribute it by any device or process whereby a copy or phonographic record of the work is fixed beyond the place from which it was sent.” Finally, section 602 would have been amended to specify that the rules governing importation into the United States apply to any importation “whether by carriage of tangible goods or by transmission.”

The Copyright Office argued that “the transmission of a work over a communications network should be included within the scope of the copyright owner's exclusive rights. At this point in time, it appears likely that transmission may soon become the primary method of exploitation for works of authorship. If authors are to continue to have meaningful and adequate incentives for creation, it is therefore critical that they be able to control such uses of their works.

We believe that the Copyright Act in its present form can and should be read to encompass within the author's exclusive rights the right to transmit the work electronically to individual members of the public. The handful of courts that have addressed the issue so far have come to that conclusion. Such a use of a work has been held to involve the creation of a copy of more than transitory duration in the recipient’s computer, implicating the reproduction right. If such copies are sent to members of the public, it will implicate the distribution right. And if the work is made visible or audible on the recipients’ computers, it may implicate the rights of public display or public performance.

Others advanced different interpretations of the law. Since it may take years for the courts to establish a definitive position on this issue, and since the development of the NII is already well underway, it was thought beneficial to clarify the law in order to remove uncertainty. The amendment simply clarifies existing rights.

As technology evolves, in order to preserve adequate incentives for creation, the governments position was that it must ensure that the copyright owner will continue to control the basic means of

281 Statement of Marybeth Peters, Register of Copyrights and Associate Librarian for Copyright Services to House Subcommittee on Courts and Intellectual Property and the Senate Judiciary Committee, 104th Congress, 1st session, November 15, 1995.
exploitation of works of authorship—whatever they may be at a given point in time. This requires the development of appropriate concepts and language to track changing means of exploitation without the need for constant legislative reworking. For example, if technology allows transmissions without creation of a reproduction in the receiving computer's memory, the amended definition of "distribution" would no longer suffice.

A certain degree of controversy surrounded the choice to clarify the law through the distribution right. Some felt that all transmissions involve public performances of works; others that every transmission produces a reproduction and should be addressed solely through that right. Any approach to transmission will be vulnerable to criticism when separate markets exist for the licensing of different rights. The NII copyright bills attempted to minimise market disruption by amending the distribution right rather than creating a new right. In the view of the framers, other rights may also be implicated in transmission, making it necessary to obtain authorisation from the appropriate licensing source.

The amendment did not change existing law, create any new liability, or shift the locus of responsibility for infringing transmissions. It did, significantly, attempt to prohibit "the manufacture, import or distribution of products which would avoid, bypass, remove or otherwise circumvent any process, treatment, mechanism or system that prevents or inhibits the protection of copyright." This was seen as penalising current equipment used for legitimate purposes and chilling future technological development.

Other areas of concern that were not addressed include the fact that under current technology and legal interpretation, every transmission over a network produces a potentially large number of reproductions, and therefore constitutes an act of prima facie infringement. Perhaps some of these should be privileged, particularly where they are incidental and transient. Online service providers are also greatly concerned about their potential liability for every infringing transmission through their services, no matter how responsibly they act. These problems could entail changes in the law that significantly shift the balance between owners and users.

Ultimately, the Bill failed because no compromise could be reached on issues of fair use, ISP liability and anti-circumvention.

Shortly before the NII bill was introduced, another law (Public Law 104-39) was passed that created an exclusive right to perform sound recordings publicly by means of digital transmissions.

The Clinton Administration has introduced a new bill specifically aimed at implementing the WIPO treaties, and has raised the possibility of reintroducing the NII. The implementing legislation (H.R. 2281, S. 1121) takes a piecemeal approach to these treaties. It has been opposed by activist groups (e.g. Digital Futures Coalition, Electronic Freedom Foundation) on several grounds.

Section 1201 contains the treaty prohibition on circumvention of copy protection devices. This is felt to stifle innovation, in much the same way as last year's failed attempt to ban "black box" digital decoders. During the drafting process, a similar version that would have affected the design of future computers and other recording products was withdrawn in favour of the more modest requirement that nations should provide "adequate legal protection ... against the circumvention of effective technological measures." The implementing legislation reverts to the broader "capabilities" approach. It is felt that this would: i) harm education and research by allowing copyright owners to "fence off" public domain works and frustrate fair use rights; ii) frustrate encryption research that helps secure networks; iii) prevent legitimate "reverse engineering" to the detriment of software development; iv) force redesign of existing devices with

---

282 Since transmission was not defined as an exclusive right, an intermediary would not be directly liable. Only those who by means of the transmission distribute copies of the work to the public are direct infringers. (The intermediary might be subject to indirect liability through the doctrines of contributory infringement or vicarious liability.)
substantial non-infringing uses; v) give judges authority to bless or deny computer design decisions; vi) limit parental capability to monitor and control children’s on-line activity; and vii) penalise consumers who resist efforts to track their on-line usage on privacy grounds. These groups further note that the sanctions in Sec. 1201 are “not tied to infringement of any intellectual property right held by a copyright owner.” They thus do not exempt “circumvention” in exercise of fair use rights or access to public domain or non-copyrightable material; while these restrictions and exemptions remain in place, their exercise becomes more difficult.

- Section 1202 is concerned with rights management information. It provides for criminal and civil penalties, again without any need to show intent to infringe, promote infringement or further another’s infringement.

- The proposed Bills also omit certain key provisions of the Treaties. While other legislation (see above) effectively addresses the liability of ISPs, no current bills take up the issues of fair use, first sale, library archiving, distance education or non-negotiated licence terms.

The Electronic Futures Foundation and other groups raise similar objections to the proposed database treaty. In particular, they point out that:

- The treaty seems to undermine the long-standing US position that facts cannot be copyrighted or otherwise removed from the public domain. This new property right for facts is seen as particularly troubling in countries where public databases have been “farmed out” to private contractors, as it may restrict public access to public information. In the US, this might conflict with government obligations under the Freedom of Information Act.

- There are several definitional problems, particularly no clear enunciation of a “fair use” right.

- Databases need periodic maintenance; as it stands, such maintenance “resets the clock” for protections.

- Finally, the 1996 draft contained the same troubling language about third party liabilities and circumvention of copy protection as the copyright treaty.

### 7.3.5.2. Types of Rights and Infringements

There is a bill (Online Copyright Limitation Liability Act, H. R. 2180) pending in Congress that limits the liabilities of online service providers with respect to software pirates or copyright thieves among their clientele. It exempts transmitters or access providers from certain copyright liabilities.

---

283 See Sony Corp of America v. Universal City Studios, Inc., 464 US 417 (1984), that was instrumental in the explosive growth of the VCR market.


285 These include “shrink-wrap” or “click-on” licences developed to overcome the lack of privity between developers and ultimate users.


287 See for instance, Feist Publications, Inc. v. Rural Telephone Service, in which the Supreme Court rejected a copyright claim for a telephone directory’s white pages on the grounds that facts cannot be copyrighted and obvious organisational schemes (alphabetical order in this case) are insufficiently creative.

288 A representative of the UK Copyright Office expressed a similar reservation.

289 "A person shall not be liable: for direct infringement, or vicariously liable for the infringing acts of another, based solely on transmitting or otherwise providing access to material on-line, if the person— (A) does not initially place the material on-line; (B) does not generate, select, or alter the content of the material; (C) does not determine the recipients of the material; (D) does not receive a financial benefit directly attributable to a particular act of infringement; (E) does not sponsor, endorse, or advertise the material; and (F)(i) does not know, and is not aware by notice or other information indicating, that the material is infringing, or (ii) is prohibited by law from accessing the material; or (2) in the case of a finding of contributory infringement based solely on conduct for which a person is exempt from liability for direct infringement or vicarious liability.
Transmitters are not liable if they do not know that the material is infringing, and do not profit directly by the infringement, moreover, they have no duty to find out whether it is. They are not liable for links to pirated material either unless the linking endorses the material. Moreover, if they respond to notice of infringement by removing or blocking the offending material, they have no consequent liability, even when the removal was based on another party’s misrepresentation of the character of the material. The Bill is opposed by software publishers (fearing an increase in illegal copying and distribution) and those who fear a resulting reduction in the amount and quality of on-line software.

Another proposed bill, (Fairness in Musical Licensing Act of 1997) provided that:

"communication by electronic device of a transmission embodying a performance or display of a non-dramatic musical work by the reception of a broadcast, cable, satellite, or other transmission shall not be a copyright infringement unless an admission fee is charged to see or hear the transmission or the transmission is not properly licensed.

[The Bill] Excludes as a copyright infringement the performance of a non-dramatic musical work: (1) by a commercial establishment at no charge when a purpose of the performance is to promote audio, video, or other devices utilised in such performance; and (2) at an organised children’s camp if the children in attendance sing, dance, or participate in all or a portion of such work, or when the performance is of an instructional nature."

7.3.5.3. Summary

The US differs from France and Germany in according only limited recognition to moral rights.

There are a number of legislative actions pending that address both the definition of acts and actors and the rights and liabilities regarding copyright infringement. The most far-reaching recent legislative initiative was the National Information Infrastructure Copyright Protection Act of 1995; it was withdrawn, but may be re-introduced in the wake of the WIPO treaties.

7.4. SUMMARY AND COMPARISON

We begin with a summary discussion that highlights the answers to research questions 1-3. The first part, "Issues Arising," answers the first research question, while the second, "Initiatives," sketches the answers to the second two questions, describing legislation and other initiatives. The section concludes with a short comparison of the surveyed countries.

7.4.1. Issues Arising

As with other subject areas, legal activities with respect to copyright on the electronic highway focus primarily on how to deal with occurring issues making use of existing legal frameworks. Many of these issues are the result of the convergence of media, telecommunications and content industries, and the facilitated distribution of creative works. The general legal problem is how to redefine law to reduce its dependence on specific technologies. More specific issues may be broadly categorised along the following lines:

- Issues regarding protection criteria for types of works (e.g., what constitutes a protected work on the electronic highway) and actors involved (e.g., do authors, producers, service providers still take the same roles and interest). New works have been created as a result of developments on the

under paragraph (1), for any remedy other than injunctive relief under section 502, except that such injunctive relief shall be available only to the extent that all acts required by such relief are technically feasible and economically reasonable to carry out. Nothing in clause (i) of paragraph (1)(F) shall impose an affirmative obligation to seek information described in such clause."
electronic highway. The exact status of these works and their associated level of protection are sometimes ambiguous. These issues emerge particularly with databases, CD-ROM materials, and Web-pages (including frames and links): whether they can be interpreted as, for instance, compilations or citations; whether they have characteristics of several pre-existing types of works, etc.

* Issues regarding the type of rights that are enjoyed and limitations and exceptions to these rights. Rights are still largely determined by their media of fixation. Existing rights may not match the uses to which the materials may be put; without adequate means of exploiting them, protection can be skewed. In the same context, questions arise with respect to digital copies. These copies are indistinguishable from the originals. This leads to discussion about the free use of copies analogous to that often allowed in the traditional environment for personal use or special interest groups.

Other prominent issues are related to jurisdiction (what law is applicable if a work is produced in one country and the rights are infringed in another), enforcement of laws, and the liability for the infringement of copyright.

### 7.4.2. Initiatives

#### 7.4.2.1. International

The two main multinational fora with a dominant role in the field of copyright as applicable to the surveyed countries are the United Nations World Intellectual Property Organisation (WIPO, to which all surveyed countries subscribe) and the European Union, which enacts regulations that apply to three of the four surveyed countries.

**Protection of Works and People**

The EU Database directive was adopted by the Council in 1996 and will have to be implemented in the Member States before 1 January 1998. It provides two types of protection for databases: copyright protection with respect to the selection and arrangement of their contents (as opposed to the contents themselves); and a *sui generis* right that protects the database in cases where a qualitative or quantitative investment in the establishment of the database has been made.

**Types of Rights**

The Berne Convention was recently amended by the WIPO Copyright Treaty. Subsequently, the Rome convention was amended by the WIPO Performances and Phonograms Treaty. The WIPO copyright treaty stipulates that reproduction right and its exceptions fully apply to the digital environment and that storage of a protected work constitutes reproduction. In addition, it introduces a new right of communication to the public, guaranteeing the author's exclusive right to authorise access to or usage of his or her work in any form of electronic transmission. Finally, it prohibits unauthorised removal or alteration of "rights management information," and requires implementing legislation to enforce its provisions.

#### 7.4.2.2. France

**Protection of Works and People**

The legal definition of works of art includes literary, graphic, audio-visual and photographic works (a definition fitting Web pages) and compilations such as CD-ROMs. French copyright law does not grant (multimedia) works on the Internet different terms of protection than any other works.

**Types of Rights**

To date, no initiatives have surfaced in France to change the extent of protection offered by French copyright with respect to electronic highway activities. The types of rights stipulated by French copyright law are applied in much the same manner to Internet activities. Although no specific legislative initiatives have been undertaken, recent court cases have shed light on some interpretations
of law. The main thrust has been continued strong protection of authors and their rights

7.4.2.3. Germany

Current German policy initiatives involve only slight modification of German copyright law. The main approach seems to be that legislation should be reactive to technological developments.

Protection of Works and People

German copyright law defines works in a broad sense as personal intellectual creations and does not limit the types of works protected. It has therefore a technology-independent character. Given that, no changes have been considered necessary to adapt to changing circumstances initiated by developments on the electronic highway. In its most recent legislative initiative (implementation of the Informations- und Kommunikationsdienstegesetz as of 1 August 1997), Germany's only change to copyright law relates to incorporation of the EU Database Directive, providing databases with double legal protection.

Types of Rights

Although no actual changes in law are currently put forward, the Parliamentary Inquiry Commission Zukunft der Medien in Wirtschaft und Gesellschaft -- Deutschlands Weg in die Informationsgesellschaft has explored issues related to new media and different rights in its Zweiten Zwischenbericht. Its recommendations aim to clarify some of the ambiguities with respect to copyrights on the electronic highway. For instance, the commission stated: that private use provisions will also cover use through digital technologies (albeit in return to a general levy); that simple electronic download of material constitutes public reproduction as indicated; and that the exhaustion of rights principles which traditionally require a physical format should not be extended to electronically transmitted services.

Special attention has been paid in Germany to the liability of Internet service and access providers. Specific stipulations with respect to the responsibility of service providers in the Informations- und Kommunikationsdienstegesetz has been perceived as a temporary measure to deal with liability issues with respect to copyright infringement on the Internet.

7.4.2.4. United Kingdom

Protection of Works and People

While implementation of the EU Database directive is still under discussion, under the current Copyright, Designs and Patents Act (CDPA) of 1988 databases are still considered compilations. Protection does not depend on the medium and is given to printed as well electronic databases, provided they meet the "originality" standard required of literary compilations. With regard to transmission as a means of distribution, the CDPA establishes different presumptions for broadcast (where potential infringement occurs where the broadcast is made) and e.g., cable (where potential infringement occurs where the transmission is received). The Government has specifically declined to broaden the definition of broadcast to cover all forms of digital transmission.

Types of Rights

With the exception of the provisions of the CDPA, no specific legal initiatives have been undertaken in the UK with respect to types of rights. On the issue of Web pages, the central issue is the extent to which they are viewed as computer programs. If they are, the CDPA permits what would otherwise be obvious acts of infringement, and may even moot the question of implied licence. With regard to links, the general position of the CDPA and case law is that links can create infringement.
Licence to view may be irrelevant under the CDPA’s definition\textsuperscript{290} of “fair dealing,” but the application of the definition is unclear. Also, it may happen that a copyright owner’s assertion of rights or limitation of implied licence may be invisible to third-party users of links. The approach taken in recent cases is to view withdrawal of implied licence as derogation from grant. Another current topic of discussion is the question of equitable treatment of domestic and foreign performers, and in particular the mechanisms by which performers obtain remuneration. The government’s position favours wider distribution over careful restriction.

7.4.2.5. United States

In the US, there is a general agreement that copyright law requires thoroughgoing reform. A number of pending legislative actions address both the definition of acts and actors and the rights and liabilities regarding copyright infringement. The most far-reaching recent legislative initiative was the National Information Infrastructure Copyright Protection Act (CPA) of 1995 which was withdrawn by the US government when no compromise could be reached on issues of fair use, ISP liability and anti-circumvention.

Protection of Works and People

In the proposed and withdrawn CPA of 1995 the definition of publication was to be extended to include publication by means of transmission as well. The Copyright Office position was that “it appears likely that transmission may soon become the primary method of exploitation for works of authorship.”

Types of Rights

Most issues in the US have focused on how to provide authors with meaningful protection by extending their rights. Most significant was an amendment to the CPA of 1995 that would have amended the distribution right to add transmission as a means by which copies can be distributed.

The liability issue has been addressed by one specific legislative initiative. The currently pending Online Copyright Limitation Liability Act limits the liabilities of online service providers with respect to acts of software piracy or copyright theft by their clientele. It exempts transmitters or access providers from certain copyright liabilities. Transmitters are not liable if they do not know that the material is infringing, and do not profit directly by the infringement, moreover, they have no duty to find out whether it is.

7.4.3. Comparison

The following Table briefly summarises the positions of the countries on several broad issues.

<table>
<thead>
<tr>
<th>Issue</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redefinition of terms</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Moral rights</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Limited</td>
</tr>
<tr>
<td>Remote jurisdiction</td>
<td>Yes</td>
<td>depends</td>
<td>depends</td>
<td>No</td>
</tr>
</tbody>
</table>

In both the US and UK, there are active efforts to redefine terms, through legislation and through interpretation by the governing executive agencies. In France and Germany, by contrast, there is little initiative towards redefinition as current copyright protection is considered sufficient. In all of the countries surveyed, it is proving difficult to arrive at a definitive position with regard to copyright and the electronic highway. The European countries all regard moral rights as an element of copyright and are incorporating these rights into their reframing of copyright for the electronic highway; the US is much more limited in that regard. There are stark differences among the countries in whether or not

\textsuperscript{290} CDPA, Sec. 29.
remote jurisdiction is claimed. France claims it in toto while the US rejects it. Germany and the UK are in the middle, with Germany leaning towards the French position and the UK leaning towards the US position.
8. IMPORTANT OBSTACLES TO DEVELOPMENT OF AN INFORMATION SOCIETY AND CONCLUDING REMARKS

8.1. INTRODUCTION

This section discusses what we have perceived to be "the most important legal obstacles to the developments of an information society", thus addressing research question five. We should stress that this is our perception, based on the materials we have reviewed and the interviews and discussions in which we have participated. It does not represent either the results of a scientific survey or the consensus judgement of authorities. In our view, this would be difficult to achieve and of dubious value.

This section also serves as an abbreviated overview of the issues discussed in the main body. They have been selected because they seem to us as important, difficult and in need of fairly prompt legislative action. This list is provided largely as a summary and for guidance in narrowing the scope of future efforts.

8.2. OBSTACLES

The "information society" whose development is being urged has many different aspects. To some, the most important aspect is the removal of obstacles to communication - they look forward to a degree of free speech and government accountability that libertarians like Thomas Paine could scarcely have conceived. To others, the information society is a means of dissolving the isolation of individuals, communities and nations and of reorganising social structures. Still others view it as a means of realising the full power of the global economy.

Originally, we intended to describe issues that "were considered to be the most important legal obstacles to the development of an information society." The immediate questions are:

- Considered by whom?
- What does "important" mean?
- What is an "obstacle"?
- What is "the information society"?

With regard to the first question, we soon discovered though interviews and the opinions expressed by members of our network of contacts that each person's area of expertise or responsibility determined his or her view of the "importance." Indeed, many people were concerned primarily with broad themes such as privacy or electronic commerce that had a vague or ambiguous representation in terms of concrete legal issues. Specifically, a technological/economic development like Web commerce could be seen as the ultimate forum for effective competition or an unstoppable opportunity for the accretion and exercise of market power. Next, it became evident that "one person's obstacle was another's opportunity." This owed something to politics, something to nationality and something to discipline. Finally, even a casual reading of the public discussion of the electronic highway reveals that individuals have widely differing visions of the information society. It would not be possible to represent their views of important obstacles without eliciting, comparing and articulating their visions.

At the same time, it did not seem to us that this could be a particularly useful exercise in terms of the rest of the material. Instead, we present a listing of those issues which, in our judgement:

- pose a major threat to the realisation of the full potential of the new technologies to contribute to human welfare;

291 Economists tended to see few obstacles, or at least few requiring legislative intervention.
are unlikely to be resolved without some form of collective action; and
do not seem to be effectively addressed at the moment.
For ease of exposition, we consider them in order of the areas.
In the area of encryption, the largest obstacle seems to be the difficulty of assessing and balancing legitimate needs for access and legitimate fears of access. This should clearly distinguish among access to plaintext of encrypted material, decryption keys and encryption hardware, software and algorithms. Legitimate needs for access mainly reflect:
- law enforcement and national security needs of governments;
- dispute resolution requirements;
- recovery of one's own information in case of key loss or deliberate withholding; and
- access to asset records by spouses, etc.
Legitimate concerns about encryption restriction:
- privacy invasion;
- loss of anonymity;
- compromised privilege against self-incrimination;
- weakened business confidentiality;
- loss of competitive advantage;
- trust and security of financial networks and network transactions;
- computer system security against unauthorised access or modification
In striking this balance, it is also necessary to take account of: evolving technological possibilities for encryption and/or code-breaking; the availability, legitimacy and practical enforceability of legal tools for restricting encryption or compelling the use of specific types; the simultaneous developments in other nations and international fora; and the essential overlaps between encryption and other areas (digital signatures, electronic commerce, data protection, illegal content, copy protection) and legal themes (esp. liability, reliability, privacy, enforcement and anonymity).
In the area of digital signatures, there is wide consensus on the need for legal certainty regarding the validity, scope and evidentiary value of electronic signatures and documents in relation to written ones. There is a separate need to take advantage of the particular advantages of public-key encrypted digital signatures and especially certificates and the reliance that should be placed on them. This may well be a matter for legislation: the large number of US state laws and emerging national law in Germany (as well as actual and proposed TTP laws in the other countries) suggest that a legislative resolution may be in the offing. In addition to establishing the legal status of these certificates, it is necessary to establish the rights and duties of certifying authorities (CAs) as providers of authentication services. This will probably need to involve some degree of legislation to establish license conditions and otherwise aid the development of a public "infrastructure of trust." There are also opportunities for the government to undertake or support special certificates that further other purposes, such as access to government services, electronic driver licenses or passports and the like. In this area, too, it is necessary to take account of other areas and concerns, and particularly of the confusion surrounding the distinction between encryption providers, key recovery/escrow agents, public key infrastructure agents, certification authorities and trusted third parties. As indicated, these are all different entities and perceptions of the need for and desired nature of government intervention will reflect particular views as to what is being discussed. This is an area where particular attention should be paid to international harmonisation, because electronic documents, digital signatures, certificates and electronic cash are
likely to be most useful in cross-border trade. It seems especially important to establish conditions for mutual recognition of these instruments and the organisations involved in their creation and use.

In the area of personal data, there appear to be rapid movements aimed at comprehensive and internationally-harmonised bodies of law. The adequacy of these measures remains doubtful. Specific obstacles concern: data subjects' notification and consent; preservation of "privacy rights," control of transborder data flows and the particular problems associated with offshore data havens; and the intrusive possibilities created by data-sharing and data-matching. Of these, it is transborder flows that currently seem to be receiving most attention in the international arena. The related problem is the fact that European protections in this area differ substantially from those in the United States, being oriented towards protection of privacy from private parties. Perhaps for this reason, issues of on-line consumer privacy and employee privacy rights are currently receiving more attention in the US. Ultimately, however, the two different approaches will have to be reconciled in view of the importance of trade and information flow across the Atlantic. At a deeper level, there is a real danger of a tragedy of the commons in which unfettered access to and expanding use of personal data ultimately debases their utility.

The area of telecommunications and broadcasting appears to be coping with the new changes as it coped with the old ones - by making incremental changes within a very comprehensive legal and regulatory structure. This structure has already come under irresistible pressure through a combination of technological change and market liberalisation, and is changing rapidly - the Internet is another source of impetus for these changes. We have three specific observations to make. First, the degree to which specific aspects of Internet communication are portrayed as telecommunication, broadcasting publishing, etc. will profoundly affect the legal resolution of associated issues. Second, the possibilities for using the Internet to substitute for or complement traditional broadcasting or telecommunications may create pressures for change in their bodies of law. Finally, telecommunications and broadcasting law will be the vehicle used to implement solutions to Internet problems. It is important to ensure that this use of these laws does not undermine their primary or ostensible function. Beyond this, it appears likely that progress in the area of interconnection will need to be completed. In addition, policies with regard to universal service may need to be modified in light of new technologies. The obstacles to continuation of existing policies are largely due to the fact that these policies were designed to solve problems of infrastructure creation and interconnection that have largely been dealt with. There are new problems and new possibilities, but they should be worked out by: revisiting the policy basis for universal service; making an explicit separation between access and usage; reducing the linkage between access and fixed residential lines; changes to the service bundle, recipients, notion of affordability, funding mechanism and structure of the service providers. These modifications could take several directions, including:

- reduction of universal service bundles and obligations on the grounds that the access infrastructure is now largely in place and the market may be a more appropriate means of dealing with usage issues;
- expansion of the universal service bundle to encompass new services;
- specific provisions for subsidised access for specific public access points (e.g. schools, etc.) offering particular external benefits;
- imposing universal service payment obligations on ISPs, at least to the extent that they provide telecommunications services;

292 A good example is the US Telecommunications Act of 1996, which contains separate sections of telecommunications, broadcasting, cable, and Internet services, as well as including the Communications Decency Act.
• funding universal service subsidies from outside the telecommunications sector in recognition of convergence;
• developing compensation mechanisms that encourage technological and service developments that may remove the need for subsidies; and

Defamation seems to be regarded as a contentious issue. It may be an obstacle if intemperate online speech slows or reduces peoples' willingness to make best use of new possibilities or to co-operate in developing collective self-regulatory solutions (e.g. Netiquette). Formal legal principles regarding ISP liability seem to be converging around a model that connects liability to knowledge of content, willingness to exercise editorial control, and technical ability to restrict access or compel removal. There remain some technical matters, such as the fact that defamatory material may be available at a number of sites throughout the world long after it has been removed or disclaimed by the author or the author's ISP. This places it somewhere between written and spoken material for legal purposes. There also remain serious problems of defining the applicable jurisdiction and the scope for damage assessment. To the extent that these problems prove insurmountable or slow to resolve in the electronic highway context they may give rise to an increase in defamation on the Internet or a migration of defamatory material to the new environment. On the other hand, as individuals come to terms with the eased barriers to public speech the Internet affords, it may be the case that on-line defamation attracts even less weight than spoken defamation. Traditional distinctions (e.g. between slander and libel or public and private figures) are eroded by technology and are disappearing at least from the legal and social discussion of this area. There may thus be some need to recodify some parts of defamation law.

For harmful or illegal content, other serious issues arise. They are viewed as obstacles to the development of the information society because this material surmounts barriers already in place for physical manifestations with seeming ease. Combined with the prominence they receive in the popular press, this makes cyberspace seem an unfriendly and dangerous place. This prominence has also been associated with some fairly ambitious attempts to limit or roll back existing speech protections (e.g. the Communications Decency Act). On the other hand, it has been argued that obscenity, in particular, has been associated with many previous social advances in respect of publishing, cinema and other forms of communication - perhaps it will serve the same 'test bed' role here. Perhaps the gravest of the specific obstacles are: i) the need to deal simultaneously with illegal material as opposed to illegal access or exposure to harmful material; and ii) the differences between national laws regarding the boundary between harmful and illegal material, ISP liability and the illegality of mere possession, transmission or transmission over public networks. Recent cases such as Reno v. ACLU make much of the question of access in particular, how to protect young people from exposure to indecent material. It has been noted that "filtering" software can help parent to protect their own children, but that its abilities are strictly limited. From the liability point of view, a Web site operator may find that his attempts to ascertain the age of those who gain access to his material are not effective enough to protect him from liability. In this regard, it seems an attractive option to have the government issue digital proof of age certificates that would serve a function analogous to driver licences in the US. Their use to control access to indecent material could provide a safe harbour against ISP liability. Hate speech is largely a matter of differing standards across jurisdictions, a feature that it shares with obscenity. However, its regulation is also based on the possibility of damage to innocent third parties, a characteristic that it shares with child pornography. The main difference is the near-universal illegality of the latter. The emerging consensus on matters of harmful and illegal content is that a multi-tier approach combining legislation with self-regulation and technical devices is called for. At a deeper level, it remains to be seen whether the Internet consists of 'communities' capable of forming and enforcing their own standards of what is acceptable or a sea of disparate and largely powerless individuals. In either case, there is a role for
government assistance, albeit in different form. Unsolicited commercial email or news posting is viewed\textsuperscript{293} as a growing and serious threat to the development of electronic commerce and more generally to the cost-effectiveness and utility of online resources. This area will certainly attract legislative attention in the near term. Again, the perception is that a tragedy of the commons is developing, in which the volume of unwanted and irrelevant commercial solicitation will reduce the utility of email, newsgroups and other means of communication. Among the legal initiatives needed is an extension to the new environment of laws regarding advertising, fair dealing and consumer protection. This may raise some interesting liability questions. The judgement against Virgin Atlantic for misleading advertising was predicated on outdated information on their Web site. Currently, many Web browsers use cache files to speed their operations. As a result, the user may not be aware that he or she is not seeing the most recent version of a page. In some countries, caching also occurs at the national level - for instance the Hensa cache site that serves the UK. It is an interesting question as to how liability can be assigned in this area without imposing large time-stamping costs.

8.3. IS LEGISLATION NEEDED?

In general, there seem to be seven generic reactions to this sort of issue and to the general question of Internet governance.

• \textit{Laissez-faire}: the belief that competitive and other forces will lead to a satisfactory outcome.

• \textit{Inactivity as a counsel of despair}: the belief that the technological, jurisdictional, enforcement and other problems are ultimately intractable.

• \textit{Slight modifications of existing law in the same area}. For instance, some aspect of the validity of digital signatures can be handled simply by a reinterpretation of statutes specifying written signatures.

• \textit{Adopting and adapting existing law from other areas}. Some problems occurring on the electronic highway can be simplified by an appropriate choice of legal metaphor. For instance, the counsel of despair that the Internet is a "virtual space" which makes a mockery of geographically-based jurisdictions can be partially answered by the observation that it may equally be considered a network of relationships of precisely the sort that international telecommunications law has grown accustomed to dealing with.

• \textit{Confronting problems in other areas for which the Internet substitutes}. Regulation is often used as an aid to or surrogate for open competition in situations of "natural monopoly" associated with restricted market access or large minimum efficient scale. To the extent that head-to-head competition between electronic enterprises occurs across a much broader front, the need for regulation or its appropriate form may need to change. Some have argued, for instance, that laws of libel or copyright are based on presumptions specific to printed media. In a world of electronic communication, these presumptions may be undermined or reversed.

• \textit{New laws owing little or nothing to previous laws}. This is a popular position among those favouring restrictions on encryption.

• \textit{Creation of a new "Cyberspace" jurisdiction} Some believe that the non-geographical, non-physical nature of the Internet poses tremendous challenges that can be drastically simplified by a new sovereignty, with its own, initially self-regulatory, legal structure and regular relations with other, geographically-based jurisdictions.

It is also important to consider the issue of timing. There are several reasons why a rush to legislate may be dangerous.

• Technology and practice evolve at a rapid pace, and laws may well be obsolete before they take

\textsuperscript{293} Primarily in the US, though the problem may be growing across the world.
effect.

- Likewise, the public understanding of the impact of new developments and the political decisions that emerge from public debate may be premature.
- Reciprocally, the development and deployment of new technologies and the structure and utility of new services will often respond strongly to legal developments, raising the possibility that an early law may threaten the very industry it was intended to regulate. Put slightly differently, a solution to today’s pressing problem may jeopardise tomorrow’s golden opportunity.
- Often, legislation is used to provide clarity and unify case law, or to support self-regulatory or contractual solutions to problems. Clearly, this cannot happen until the case law is developed and/or the nature of contractual problems understood in terms of experience.
- As a pragmatic matter, since much Internet activity is global in scope, passing national legislation in advance of the development of international arrangements may create further problems. However, there are certain considerations favouring early legislation.
- Legislation resolves uncertainty. Taking a clear stand may encourage private parties by giving them a clear sense of the future legal environment they will face. This is the motivation behind early digital signature laws such as those in Germany and the US State of Utah.
- As mentioned above, legislation can influence the pace and direction of technological and practical evolution. It can thus be used to forestall unfortunate developments and inefficient decentralised “solutions” to problems. It has been argued that the current problems with unsolicited commercial messages in telephony, email and newsgroups could have been headed off by forthright enforcement of existing law or addition of minimal new powers. Now, however, these problems are widely regarded as intractable and persistent since the “telemarketers” and their economic interests are well entrenched.
- Finally, the passage of relatively vague early laws can create a sort of “natural experiment” whereby valuable information about the future severity of legal problems or the extent of necessary trade-offs between apparently-conflicting public policy objectives can be assessed. Various US state digital signature laws can be seen in this light.

8.4. STEP TOWARDS THE INFORMATION SOCIETY

A message that has permeated this report is the uncertainty of the future. In each of the areas we examined, there is uncertainty how the technology will be developed, what uses will made of the technology, what benefits and harms may accrue from these uses, and what governments can do to promote the good and impede the bad. Simple long-term forecasting to set equally long-term laws and regulations does not appear to us to be a good idea; the uncertainties swamp the assessments, and there is no clear single best solution. This becomes clear if we examine the history of the Internet to date. From its beginnings in the U.S. defence establishment, even the most far-seeing of prophets did not envision the way in which the Internet has revolutionised not only information flow, but even the societies, which use that flow.

The best strategy thus appears to be an adaptive one, in which planning is relatively short-term, legislation is crafted that is adaptive to changing circumstances, and--perhaps most difficulty--the authors of legislation can remain sufficiently detached from their works to be able to change course when such a change is indicated. A proper adaptive strategy seeks signposts, which foretell the future, and invoke a set of policies suited to that future.
9. BIBLIOGRAPHY

Note: These materials were consulted in preparing this study. In addition, we used parliamentary reports, case records and law statutes. These are referenced where appropriate in the text. Publications by national official bodies are prefaced by the name of the country. European Union documents are prefaced by "EU" regardless of which organisation issued them, since they are available from collective sources. The first part of this bibliography refers to materials consulted in written form. The second part provides a bibliography of on-line resources.

9.1. WRITTEN MATERIALS


6. Akdeniz, Y. The Regulation of Pornography and Child Pornography on the Internet, 1997 The Journal of Information Law and Technology 1


17. Blakesly, J. Jurisdictional Issues and Conflicts of Jurisdiction, in Bassiouni, ed. Legal Responses
to International terrorism: U.S. Aspects.


26. BT (British Telecommunications) PLC, Internet Voice Telephony - comments on Draft Notice 97/C 140/06, 2 July 1997.


38. Charles, R. and J. Zamansky Liability for Online Libel After Stratton Oakmont, Inc. v. Prodigy
Services Co., 28 Conn. L. Rev. 1173, 1996.


58. Egan, P. Virtual Community Standards: Should Obscenity Law Recognize the Contemporary


61. EU, Abolition of the restrictions on the use of cable television networks for the provision of already liberalised telecommunications services, 95/51/EC.

62. EU, Citizens' access to public sector information, (Study by Tilburg and Leiden Universities), 1997.


64. EU, Communication on A European Initiative in Electronic Commerce, IP/97/313.

65. EU, Convention on the Law Applicable to Contractual Obligations, 80/934/EEC.

66. EU, Directive 95/46 of 24/10/1995 for the protection of individuals with regard to automatic processing of personal data.

67. EU, Directive on Cross border credit transfers, IP/97/19.

68. EU, Directive on the Protection of Consumers in Respect of Distance Contracts, 97/7/EC.

69. EU, Financial services: meeting consumer's expectations, IP/96/432.

70. EU, Implementation of full competition in telecommunications markets, 96/19/EC.

71. EU, Mobile and personal communications, 96/2/EC.


73. EU, On a common framework for general authorisations and individual licenses in the field of telecommunications services, 97/13/EC.

74. EU, On competition in the markets for telecommunications services, 90/388/EEC.

75. EU, On the application of open network provision (ONP) to voice telephony, 95/62/EC.

76. EU, On the protection of minors and human dignity in audiovisual and information services, COM(96) 483.

77. EU, Telecommunications Council Resolution on illegal and harmful content on the Internet, 97/C 700/1.

78. EU, Communication on illegal and harmful content on the Internet, COM(96) 487.

79. EU, European Parliament Resolution on the Commission communication on illegal and harmful content on the Internet,

81. EU, On universal service for telecommunications in the perspective of fully liberalised environment, COM(96) 73.

82. EU, Recommendation Concerning Problems of Criminal Procedure Law Connected with Information technology, Committee of Ministers to Member States, R (95) 13 September 1995.


84. EU, Satellite communications, 94/46/EC.


86. Faber, J. Indecency and the Internet: where does the First Amendment Fit In?, VIII Lex Mundi World Reports VIII, No. 2, July 1996.


89. Fixler, M. CyberFinance: Regulating Banking on the Internet, 47 Case Western Res. L. Rev. 81, 1996.

90. Florida Attorney General, Formal Opinion 95-70.


156. Kim, T. C. Taming the Electronic Frontier: Software Copyright Protection in the Wake of United States v. LaMacchia, 80 Minn. L. Rev. 1255, 1996.


164. Kubicek, H. Multimedia: Germany's Third Attempt to Move to an Information Society


167. Lalande, P. *L'Internet, a vrai défi pour la France*, report to the Prime Minister, April 1997.


182. Massachusetts Digital Signature Page at [http://www.magnet.state.ma.us/itd/legal/pollaw.htm](http://www.magnet.state.ma.us/itd/legal/pollaw.htm)


208. Note: Conflicts on the Net: Choice of Law in Transnational Cyberspace, 29 Vand. J. Transnatl


222. Post, D. The First Internet War: Scientology, its Critics, Anarchy, and Law in Cyberspace, Reason, April 1996.


228. Reidenberg, J. Governing Networks and Rule-making in Cyberspace, 45 Emory L.J. 922, 1996.


251. Shiff, S. The Good, the Bad and the Ugly: Criminal Liability For Obscene and Indecent Speech on the Internet, 22 William Mitchell L. Rev. 731, 1996.


254. Smedinghoff, T. Online Law, 1996.


258. Sperti, A. The Public Forum Doctrine and Its Possible Application to the Internet, UCLA Online Institute for Cyberspace Law and Policy, Spring 1997.


290. United Kingdom Williams Committee, Obscenity and Film Censorship, HMSO, Cmdnd 7772, 1979.


9.2. ON-LINE SOURCES

The following tables contain alphabetical listings of the titles and Web addresses (URLs) of some on-line archives and other resources used in this study. This listing is not complete, and the addresses may have expired by the time this document is read. The listing of an address does not constitute endorsement of the contents by the authors of this report or endorsement of this report by the authors of those sites.

The first part of the listing contains the home pages of various organisations, divided by type. The second part contains sites oriented to specific topics. These topics are not necessarily the same as the subject areas considered in this report, and many of the topics listed here go beyond the scope of this document. In many cases, the title of the page indicates the source of the material. In some of the others, the identity of the organisation can be inferred from the Web address in the right-hand column.
9.2.1. By Organisation Type

### France
- D.I.S.S.I. Delegation Interministerielle pour la Securite des Systemes d'Information
- Internet en France
- Le paysage réglementaire et économique
- Ministère de l'économie, des finances et de l'industrie / Secrétariat d'Etat chargé de l'industrie
- Minitel Web
- Mission interministerielle sur l'Internet, Rapport de Mme Isabelle Falque-Pierrotin

### Germany
- Deutscher Bundestag - German Parliament
- Die Bundesregierung informiert
- Fakten, Trends und Meinungen
- Global Inventory Project - Germany
- Info 2000: Deutschlands Weg in die Informationsgesellschaft
- News-Ticker Onlinerecht
- Overview of home pages of German ministries
- Rechtsberater -- German Law Index
- Speech of German Minister Ruttgers on the IuKDГ
- Willkommen beim Server zur Initiative Informationsgesellschaft Deutschland

### United Kingdom
- Acts of Parliament
- DTI Information Superhighways Command Paper
- Information Society Initiative
- Lord Chancellor's Department Home Page (UK)
- Parliamentary Office of Science & Technology
- The Law Commission (UK)
- UK Government Pages Organisation Index
- UK parliament publications database

### United States
- U.S. Congress on the Internet (Thomas)
- U.S. House of Representatives - Internet Law Library - Computers and the law
- US FDA 21 CFR Part 11 - Electronic Records; Electronic Signatures
- US Information Infrastructure Task Force

---

Table 9.1. Governments

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>France</strong></td>
<td></td>
</tr>
<tr>
<td>D.I.S.S.I. Delegation Interministerielle pour la Securite des Systemes d'Information</td>
<td>gopher://gopher.urec.fr/00/Securite/Docs/Lois/DISSI_SCSSI.txt</td>
</tr>
<tr>
<td>Internet en France</td>
<td><a href="http://www.telecom.gouv.fr/francais/activ/techno/technweb.htm">http://www.telecom.gouv.fr/francais/activ/techno/technweb.htm</a></td>
</tr>
<tr>
<td>Le paysage réglementaire et économique</td>
<td><a href="http://www.telecom.gouv.fr/francais/activ/telecom/telecpay.htm">http://www.telecom.gouv.fr/francais/activ/telecom/telecpay.htm</a></td>
</tr>
<tr>
<td>Ministère de l'économie, des finances et de l'industrie / Secrétariat d'Etat chargé de l'industrie</td>
<td><a href="http://www.telecom.gouv.fr/">http://www.telecom.gouv.fr/</a></td>
</tr>
<tr>
<td>Minitel Web</td>
<td><a href="http://www.minitel.fr/index_fr.html">http://www.minitel.fr/index_fr.html</a></td>
</tr>
<tr>
<td>Mission interministerielle sur l'Internet, Rapport de Mme Isabelle Falque-Pierrotin</td>
<td><a href="http://www.telecom.gouv.fr/francais/activ/techno/rapfalq00.htm">http://www.telecom.gouv.fr/francais/activ/techno/rapfalq00.htm</a></td>
</tr>
<tr>
<td><strong>Germany</strong></td>
<td></td>
</tr>
<tr>
<td>Deutscher Bundestag - German Parliament</td>
<td><a href="http://www.bundestag.de/">http://www.bundestag.de/</a></td>
</tr>
<tr>
<td>Die Bundesregierung informiert</td>
<td><a href="http://www.bundesregierung.de/inland/index_d1.html">http://www.bundesregierung.de/inland/index_d1.html</a></td>
</tr>
<tr>
<td>Global Inventory Project - Germany</td>
<td><a href="http://www.bmwi-info2000.de/gip/index_e.html">http://www.bmwi-info2000.de/gip/index_e.html</a></td>
</tr>
<tr>
<td>News-Ticker Onlinerecht</td>
<td><a href="http://www.netlaw.de/newstick/index.html">http://www.netlaw.de/newstick/index.html</a></td>
</tr>
<tr>
<td>Overview of home pages of German ministries</td>
<td><a href="http://www.government.de/inland/index_d4.html">http://www.government.de/inland/index_d4.html</a></td>
</tr>
<tr>
<td>Rechtsberater -- German Law Index</td>
<td><a href="http://www.rechtsberater.de/">http://www.rechtsberater.de/</a></td>
</tr>
<tr>
<td>Speech of German Minister Ruttgers on the IuKDГ</td>
<td><a href="http://www.iid.de/rahmen/rede130697.html">http://www.iid.de/rahmen/rede130697.html</a></td>
</tr>
<tr>
<td>Willkommen beim Server zur Initiative Informationsgesellschaft Deutschland</td>
<td><a href="http://www.iid.de/">http://www.iid.de/</a></td>
</tr>
<tr>
<td><strong>United Kingdom</strong></td>
<td></td>
</tr>
<tr>
<td>Information Society Initiative</td>
<td><a href="http://www">http://www</a> isi.gov.uk/isi/welcome.html</td>
</tr>
<tr>
<td>Lord Chancellor's Department Home Page (UK)</td>
<td><a href="http://www.open.gov.uk/lcd/lcdhome.htm">http://www.open.gov.uk/lcd/lcdhome.htm</a></td>
</tr>
<tr>
<td>Parliamentary Office of Science &amp; Technology</td>
<td><a href="http://www.parliament.uk/post/Home.htm">http://www.parliament.uk/post/Home.htm</a></td>
</tr>
<tr>
<td>The Labour Party - Information Superhighway (UK)</td>
<td><a href="http://www.labour.org.uk/views/info-highway/content.html">http://www.labour.org.uk/views/info-highway/content.html</a></td>
</tr>
<tr>
<td>The Law Commission (UK)</td>
<td><a href="http://www.gtnet.gov.uk/lawcomm/homepage.htm">http://www.gtnet.gov.uk/lawcomm/homepage.htm</a></td>
</tr>
<tr>
<td>UK Government Pages Organisation Index</td>
<td><a href="http://www.open.gov.uk/index/orghome.htm">http://www.open.gov.uk/index/orghome.htm</a></td>
</tr>
<tr>
<td>UK parliament publications database</td>
<td><a href="http://www.parliament.the-stationery-office.co.uk/cgi-bin/tso_fx">http://www.parliament.the-stationery-office.co.uk/cgi-bin/tso_fx</a></td>
</tr>
<tr>
<td><strong>United States</strong></td>
<td></td>
</tr>
<tr>
<td>U.S. Congress on the Internet (Thomas)</td>
<td><a href="http://thomas.loc.gov">http://thomas.loc.gov</a></td>
</tr>
</tbody>
</table>
Table 9.2. Interest groups

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA Electronic Commerce Division</td>
<td><a href="http://www.abanet.org/scitech/ec/home.html">http://www.abanet.org/scitech/ec/home.html</a></td>
</tr>
<tr>
<td>Association CyberlexNet</td>
<td><a href="http://www.grolier.fr/cyberlexnet/">http://www.grolier.fr/cyberlexnet/</a></td>
</tr>
<tr>
<td>AUI, Association des Utilisateurs d'Internet</td>
<td><a href="http://www.aui.fr/">http://www.aui.fr/</a></td>
</tr>
<tr>
<td>Bonn Declaration (Cyber-Rights and Cyber-liberties)</td>
<td><a href="http://www.leeds.ac.uk/law/pgs/yaman/bonn.htm">http://www.leeds.ac.uk/law/pgs/yaman/bonn.htm</a></td>
</tr>
<tr>
<td>CELOG, Centre d'Expertises</td>
<td><a href="http://www.celog.fr/">http://www.celog.fr/</a></td>
</tr>
<tr>
<td>CITADEL EFF France</td>
<td><a href="http://www.citadeleff.org/">http://www.citadeleff.org/</a></td>
</tr>
<tr>
<td>CommUnity (UK)</td>
<td><a href="http://www.community.org.uk/">http://www.community.org.uk/</a></td>
</tr>
<tr>
<td>Digital Future Coalition</td>
<td><a href="http://www.dfc.org/dfc/">http://www.dfc.org/dfc/</a></td>
</tr>
<tr>
<td>Droit et Nouvelles Technologies (LexNet, Be.)</td>
<td><a href="http://www.lexnet.be/Droit-Technologies/">http://www.lexnet.be/Droit-Technologies/</a></td>
</tr>
<tr>
<td>Electronic Commerce Association (ECA)</td>
<td><a href="http://www.eca.org.uk/">http://www.eca.org.uk/</a></td>
</tr>
<tr>
<td>Electronic Frontier Foundation (EFF)</td>
<td><a href="http://www.eff.org">http://www.eff.org</a></td>
</tr>
<tr>
<td>eTRUST Home Page</td>
<td><a href="http://www.etrust.org">http://www.etrust.org</a></td>
</tr>
<tr>
<td>European Electronic Messaging Association</td>
<td><a href="http://www.eema.org">http://www.eema.org</a></td>
</tr>
<tr>
<td>Internet Law and Policy Forum</td>
<td><a href="http://www.illp.org">http://www.illp.org</a></td>
</tr>
<tr>
<td>Internet Privacy Coalition</td>
<td><a href="http://www.privacy.org/ipc">http://www.privacy.org/ipc</a></td>
</tr>
<tr>
<td>La Cnejita, Compagnie nationale des experts en</td>
<td><a href="http://www.axinet.com/cnejita/">http://www.axinet.com/cnejita/</a></td>
</tr>
<tr>
<td>informatique et techniques associées</td>
<td></td>
</tr>
</tbody>
</table>

Table 9.3. International

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARIES Programme (EU)</td>
<td><a href="http://www.poptel.org.uk/aries/">http://www.poptel.org.uk/aries/</a></td>
</tr>
<tr>
<td>Asia Pacific Policy and Legal (APPLE) Workshop</td>
<td><a href="http://www.glocom.ac.jp/esa/APPLE/APPLETOC.html">http://www.glocom.ac.jp/esa/APPLE/APPLETOC.html</a></td>
</tr>
<tr>
<td>DGXII HOME PAGE (EU)</td>
<td><a href="http://www.cec.int/enkomm/dg12/dg12tst2.html">http://www.cec.int/enkomm/dg12/dg12tst2.html</a></td>
</tr>
<tr>
<td>Electronic Commerce (EU)</td>
<td><a href="http://www.ispo.cec.be/Ecommerce">http://www.ispo.cec.be/Ecommerce</a></td>
</tr>
<tr>
<td>European Current Research Information Systems</td>
<td><a href="http://www.uib.no/nsd/eucris/">http://www.uib.no/nsd/eucris/</a></td>
</tr>
<tr>
<td>IM - EUROPE Home Page (EU)</td>
<td><a href="http://www.echo.lu/home.html">http://www.echo.lu/home.html</a></td>
</tr>
<tr>
<td>Watch-CORDIS (EU)</td>
<td><a href="http://www.cordis.lu/cordis/watchc.html/">http://www.cordis.lu/cordis/watchc.html/</a></td>
</tr>
</tbody>
</table>
### Table 9.4. Journals, etc.

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BBC Multimedia Centre Index</td>
<td><a href="http://www.bbc.co.uk/the_centre/">http://www.bbc.co.uk/the_centre/</a></td>
</tr>
<tr>
<td>Internet Legal Practice Newsletter</td>
<td><a href="http://www.collegehill.com/ilp-news">http://www.collegehill.com/ilp-news</a></td>
</tr>
<tr>
<td>Journal of Information Law &amp; Technology (JILT)</td>
<td><a href="http://elj_warwick.ac.uk/elj/jilt/default.htm">http://elj_warwick.ac.uk/elj/jilt/default.htm</a></td>
</tr>
<tr>
<td>NetWatchers Cyberzine</td>
<td><a href="http://www.emitech.com/netwatchers/front.htm">http://www.emitech.com/netwatchers/front.htm</a></td>
</tr>
<tr>
<td>Journal of Electronic Publishing (JEP)</td>
<td><a href="http://www.press.umich.edu/jep/">http://www.press.umich.edu/jep/</a></td>
</tr>
<tr>
<td>Net Magazine</td>
<td><a href="http://www.futurenet.co.uk/netmag/net.html">http://www.futurenet.co.uk/netmag/net.html</a></td>
</tr>
<tr>
<td>Expertises des systèmes d'information</td>
<td><a href="http://www.celog.fr/expertises/">http://www.celog.fr/expertises/</a></td>
</tr>
<tr>
<td>Netizen</td>
<td><a href="http://www.freenix.fr/netizen/">http://www.freenix.fr/netizen/</a></td>
</tr>
<tr>
<td>Planète Internet</td>
<td><a href="http://www.club-internet.fr/planete/">http://www.club-internet.fr/planete/</a></td>
</tr>
<tr>
<td>Le Monde Informatique</td>
<td><a href="http://www.lmi.fr/">http://www.lmi.fr/</a></td>
</tr>
<tr>
<td>JurisNet</td>
<td><a href="http://www.jurisnet.org/">http://www.jurisnet.org/</a></td>
</tr>
<tr>
<td>Law-France</td>
<td><a href="http://www.rencomp.com/law-france/">http://www.rencomp.com/law-france/</a></td>
</tr>
<tr>
<td>Droit de l’Informatique et des Télécoms</td>
<td><a href="http://www.legalis.net/dit/">http://www.legalis.net/dit/</a></td>
</tr>
<tr>
<td>Journal Officiel</td>
<td><a href="http://www.jura.uni-sb.de/france/JORF/index.html">http://www.jura.uni-sb.de/france/JORF/index.html</a></td>
</tr>
</tbody>
</table>

### Table 9.5. Law firms

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberLaw</td>
<td><a href="http://www.cyberlaw.com/">http://www.cyberlaw.com/</a></td>
</tr>
<tr>
<td>FarisLaw France</td>
<td><a href="http://www.farislaw.com/">http://www.farislaw.com/</a></td>
</tr>
<tr>
<td>Fenwick &amp; West (Publications)</td>
<td><a href="http://www.fenwick.com/pub/pub.html">http://www.fenwick.com/pub/pub.html</a></td>
</tr>
<tr>
<td>FindLaw - LawCrawler</td>
<td><a href="http://www.lawcrawler.com/">http://www.lawcrawler.com/</a></td>
</tr>
<tr>
<td>German law firms on the Internet</td>
<td><a href="http://www.beck.de/rsw/kuner/">http://www.beck.de/rsw/kuner/</a></td>
</tr>
<tr>
<td>Law Circle</td>
<td><a href="http://www.lawcircle.com/issues.html">http://www.lawcircle.com/issues.html</a></td>
</tr>
<tr>
<td>Netlaw Germany</td>
<td><a href="http://www.netlaw.de/desetze/">http://www.netlaw.de/desetze/</a></td>
</tr>
<tr>
<td>Perkins Coie</td>
<td><a href="http://www.perkinsoe.com/">http://www.perkinsoe.com/</a></td>
</tr>
<tr>
<td>Rechtsanwaltskanzlei Emmert Schurer Buecking &amp; Koll.</td>
<td><a href="http://www.kanzlei.de/">http://www.kanzlei.de/</a></td>
</tr>
<tr>
<td>The Law Society - swarbco database</td>
<td><a href="http://chianti.ipl.co.uk/lawsoc/swarbco.html">http://chianti.ipl.co.uk/lawsoc/swarbco.html</a></td>
</tr>
</tbody>
</table>
Table 9.6. University resources

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bert-Jaap Koops Homepage (KUB, NL)</td>
<td><a href="http://cwis.kub.nl/~frw/people/koops/bertjaap.htm">http://cwis.kub.nl/~frw/people/koops/bertjaap.htm</a></td>
</tr>
<tr>
<td>Columbia University Law School</td>
<td><a href="http://www.ctr.columbia.edu/">http://www.ctr.columbia.edu/</a></td>
</tr>
<tr>
<td>Cyberspace Law Institute</td>
<td><a href="http://www.cli.org">http://www.cli.org</a></td>
</tr>
<tr>
<td>Cyberspace Law Resources (UCLA)</td>
<td><a href="http://www.gse.ucla.edu/el/ip/resources.html">http://www.gse.ucla.edu/el/ip/resources.html</a></td>
</tr>
<tr>
<td>German Cyberlaw Project</td>
<td><a href="http://stud-www.uni-marburg.de/~koch2/gcp/">http://stud-www.uni-marburg.de/~koch2/gcp/</a></td>
</tr>
<tr>
<td>Institut für Rechtsinformatik der Universität Hannover</td>
<td><a href="http://www.lri.uni-hannover.de/">http://www.lri.uni-hannover.de/</a></td>
</tr>
<tr>
<td>Juristische Informationen im Internet</td>
<td><a href="http://www.jura.uni-sb.de/internet/">http://www.jura.uni-sb.de/internet/</a></td>
</tr>
<tr>
<td>Legal WWW-Server Saarbrücken</td>
<td><a href="http://www.jura.uni-sb.de/eng/minternet/index.html">http://www.jura.uni-sb.de/eng/minternet/index.html</a></td>
</tr>
<tr>
<td>Literaturservice Excerpta Informatica (KUB, NL)</td>
<td><a href="http://cwis.kub.nl/~frw/schrijf/kri/index.htm">http://cwis.kub.nl/~frw/schrijf/kri/index.htm</a></td>
</tr>
<tr>
<td>National Centre for Legal Education: Journals</td>
<td><a href="http://www.law.warwick.ac.uk/ncl/html/journals.html">http://www.law.warwick.ac.uk/ncl/html/journals.html</a></td>
</tr>
<tr>
<td>NetLaw Library</td>
<td><a href="http://www.uni-muenster.de/jura/im/netlaw/">http://www.uni-muenster.de/jura/im/netlaw/</a></td>
</tr>
<tr>
<td>Oxford University Networked Information System</td>
<td><a href="http://www.ox.ac.uk/">http://www.ox.ac.uk/</a></td>
</tr>
<tr>
<td>Rich's Home Page (Stanford)</td>
<td><a href="http://www.erland.stanford.edu/~llurch/">http://www.erland.stanford.edu/~llurch/</a></td>
</tr>
<tr>
<td>Stanford Law and Technology Policy Center</td>
<td><a href="http://www.techlaw.stanford.edu/home.html">http://www.techlaw.stanford.edu/home.html</a></td>
</tr>
<tr>
<td>UCLA Cyberspace Law and Policy</td>
<td><a href="http://www.gse.ucla.edu/iclp/hp.html">http://www.gse.ucla.edu/iclp/hp.html</a></td>
</tr>
</tbody>
</table>

Table 9.7. Other resources

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>French Legal Collections</strong></td>
<td></td>
</tr>
<tr>
<td>Admireoutes</td>
<td><a href="http://www.admiroutes.asso.fr/initiati/chrono.htm">http://www.admiroutes.asso.fr/initiati/chrono.htm</a></td>
</tr>
<tr>
<td>Internet pour les juristes</td>
<td><a href="http://www.grolier.fr/cyberlexnet/INFO/info.htm">http://www.grolier.fr/cyberlexnet/INFO/info.htm</a></td>
</tr>
<tr>
<td>Legalnet</td>
<td><a href="http://www.legalis.net/legalnet/">http://www.legalis.net/legalnet/</a></td>
</tr>
<tr>
<td>L'Internet juridique</td>
<td><a href="http://www.argia.fr/ijj/">http://www.argia.fr/ijj/</a></td>
</tr>
<tr>
<td>Lois, décrets et conventions de CNEUITA</td>
<td><a href="http://www.axinet.com/cnejita/INDEXDRT.HTM">http://www.axinet.com/cnejita/INDEXDRT.HTM</a></td>
</tr>
<tr>
<td>Pages juridiques de Jérôme Rabenou</td>
<td><a href="http://web.fdn.fr/~rabenou/">http://web.fdn.fr/~rabenou/</a></td>
</tr>
<tr>
<td>Site des Codes et textes de loi de Planete Internet</td>
<td><a href="http://www.planete.net/~mirage/">http://www.planete.net/~mirage/</a></td>
</tr>
<tr>
<td>Tous les droits sur l'Internet</td>
<td><a href="http://www.grolier.fr/cyberlexnet/coop.htm">http://www.grolier.fr/cyberlexnet/coop.htm</a></td>
</tr>
<tr>
<td><strong>German Legal Collections</strong></td>
<td></td>
</tr>
<tr>
<td>German Academic Article: Multimedia and Law: General Legal Problems</td>
<td><a href="http://www.jura.uni-tuebingen.de/~moeschel/seminar97riesenkampff.htm">http://www.jura.uni-tuebingen.de/~moeschel/seminar97riesenkampff.htm</a></td>
</tr>
<tr>
<td>German general multimedia materials</td>
<td><a href="http://stud-www.uni-marburg.de/~koeh2/gcp/leitseiten/MultiMedia/master.htm">http://stud-www.uni-marburg.de/~koeh2/gcp/leitseiten/MultiMedia/master.htm</a></td>
</tr>
<tr>
<td>German Law Articles on Different Legal Issues</td>
<td><a href="http://www.beck.de/njw-cor/frames/rightlaw/law-archive.htm">http://www.beck.de/njw-cor/frames/rightlaw/law-archive.htm</a></td>
</tr>
<tr>
<td>German recent regulatory developments on Information Society</td>
<td><a href="http://www.ispo.cec.be/esis/DERegresu.html">http://www.ispo.cec.be/esis/DERegresu.html</a></td>
</tr>
<tr>
<td>German references to On-line Law</td>
<td><a href="http://www.kanzlei.de/netlaw.htm">http://www.kanzlei.de/netlaw.htm</a></td>
</tr>
<tr>
<td>Herbert.Burkert's collection</td>
<td><a href="http://www.gmd.de/People/Herbert.Burkert/">http://www.gmd.de/People/Herbert.Burkert/</a></td>
</tr>
<tr>
<td>Introduction speech to the IuKDG</td>
<td><a href="http://www.iid.de/rahmen/rede180497.html">http://www.iid.de/rahmen/rede180497.html</a></td>
</tr>
<tr>
<td>Legal framework of the IuKDG</td>
<td><a href="http://www.iid.de/rahmen/eckwerte_bmbf.html">http://www.iid.de/rahmen/eckwerte_bmbf.html</a></td>
</tr>
<tr>
<td>Legal history of German IuKDG</td>
<td><a href="http://www.kanzlei.de/mmg.htm">http://www.kanzlei.de/mmg.htm</a></td>
</tr>
<tr>
<td>Motivation to German IuKDG</td>
<td><a href="http://www.kanzlei.de/iukdgbg.htm">http://www.kanzlei.de/iukdgbg.htm</a></td>
</tr>
<tr>
<td>Regulation Developments on Information Society Issues in EU member states</td>
<td><a href="http://www.ispo.cec.be/esis/HomeregQ2.html">http://www.ispo.cec.be/esis/HomeregQ2.html</a></td>
</tr>
</tbody>
</table>
### 9.2.2. By Topic

#### Table 9.8. Access

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
</table>

#### Table 9.9. Computer Crime

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFF &quot;Computer Crime Law&quot; Archive</td>
<td><a href="http://www.eff.org/pub/Publications/CuD/Law">http://www.eff.org/pub/Publications/CuD/Law</a></td>
</tr>
<tr>
<td>United Nations on the prevention and control of computer-related crime</td>
<td><a href="http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html">http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html</a></td>
</tr>
</tbody>
</table>

#### Table 9.10. Content

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Affaire UEIF</td>
<td><a href="http://www.legalis.net/legalnet/judiciaire/responsabilite.htm">http://www.legalis.net/legalnet/judiciaire/responsabilite.htm</a></td>
</tr>
<tr>
<td>Commission Beaussant et la Charte de l'Internet</td>
<td><a href="http://www.telecom.gouv.fr/francais/activ/techno/techndoc.htm">http://www.telecom.gouv.fr/francais/activ/techno/techndoc.htm</a></td>
</tr>
<tr>
<td>Contrôle de contenu, usage de la profession de fournisseur d'accès et d'information?</td>
<td><a href="http://www.grolier.fr/cyberlexnet/SECU/A961012.htm">http://www.grolier.fr/cyberlexnet/SECU/A961012.htm</a></td>
</tr>
<tr>
<td>Contrôler le contenu des Newsgroups</td>
<td><a href="http://www.grolier.fr/cyberlexnet/SECU/A960827.htm">http://www.grolier.fr/cyberlexnet/SECU/A960827.htm</a></td>
</tr>
<tr>
<td>Controlling illegal content over the Internet</td>
<td><a href="http://www.argia.fr/ljj/control.html">http://www.argia.fr/ljj/control.html</a></td>
</tr>
<tr>
<td>Defamation on Computer Networks (Australia)</td>
<td><a href="http://www.kbs.citri.edu.au/law/defame.html">http://www.kbs.citri.edu.au/law/defame.html</a></td>
</tr>
<tr>
<td>Deontologie pour l'Internet</td>
<td><a href="http://www.calvacom.fr/jurisnet/actualite/articles/art_elgo_140696.shtml">http://www.calvacom.fr/jurisnet/actualite/articles/art_elgo_140696.shtml</a></td>
</tr>
<tr>
<td>Dossier Union Européenne sur le contenu illicite</td>
<td><a href="http://www.aui.fr/Dossiers/UE/presentation.html">http://www.aui.fr/Dossiers/UE/presentation.html</a></td>
</tr>
<tr>
<td>EU Regulation of Internet content</td>
<td><a href="http://www2.echo.lu/legal/en/internet/content.html">http://www2.echo.lu/legal/en/internet/content.html</a></td>
</tr>
<tr>
<td>German Internet Content Task Force</td>
<td><a href="http://www.anwalt.de/icti/">http://www.anwalt.de/icti/</a></td>
</tr>
<tr>
<td>Groupe de travail de l'UE sur le contenu illicite</td>
<td><a href="http://www.axinet.com/cnejita/TEXTES/GTIINTEU.HTM">http://www.axinet.com/cnejita/TEXTES/GTIINTEU.HTM</a></td>
</tr>
<tr>
<td>ILPF: Content Blocking Working Group</td>
<td><a href="http://www.ilp.org/work/content.htm">http://www.ilp.org/work/content.htm</a></td>
</tr>
<tr>
<td>Internet et diffamation</td>
<td><a href="http://www.legalis.net/legalnet/judiciaire/internet_diffamation.htm">http://www.legalis.net/legalnet/judiciaire/internet_diffamation.htm</a></td>
</tr>
<tr>
<td>Internet Watch Coalition - hotline</td>
<td><a href="http://www.internetwatch.org/uk/hotline/">http://www.internetwatch.org/uk/hotline/</a></td>
</tr>
<tr>
<td>JILT: The Regulation of Pornography and Child Pornography on the Internet</td>
<td><a href="http://elj.warwick.ac.uk/jilt/internet/97_1akdz/defaut.htm">http://elj.warwick.ac.uk/jilt/internet/97_1akdz/defaut.htm</a></td>
</tr>
<tr>
<td>La Charte de l'Internet</td>
<td><a href="http://www.planete.net/code-internet/ccode2.html">http://www.planete.net/code-internet/ccode2.html</a></td>
</tr>
<tr>
<td>Le droit applicable à l'Internet</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A970428.htm">http://www.grolier.fr/cyberlexnet/COM/A970428.htm</a></td>
</tr>
<tr>
<td>Legal Action Against Individuals Involved in On-line Scams (Minnesota A.G. Files)</td>
<td><a href="http://www.state.mn.us/ebranch/ag/">http://www.state.mn.us/ebranch/ag/</a></td>
</tr>
<tr>
<td>Rating the Net</td>
<td><a href="http://www.msen.com/~weinberg/rating.htm">http://www.msen.com/~weinberg/rating.htm</a></td>
</tr>
</tbody>
</table>
### Table 9.11. Contract

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Civil titre III Des Contrats...</td>
<td><a href="http://www.fdn.fr/-rabenou/civil/L3T03.html">http://www.fdn.fr/-rabenou/civil/L3T03.html</a></td>
</tr>
<tr>
<td>Consumer Project on Technology's UCC Protest</td>
<td><a href="http://www.cpittech.org/ucc/ucc.html">http://www.cpittech.org/ucc/ucc.html</a></td>
</tr>
<tr>
<td>Contrats types</td>
<td><a href="http://www.legalis.net/legalnet/contrats.htm">http://www.legalis.net/legalnet/contrats.htm</a></td>
</tr>
<tr>
<td>German case law - Contract law</td>
<td><a href="http://www.netlaw.de/urteile/index.html#Vertragsrecht">http://www.netlaw.de/urteile/index.html#Vertragsrecht</a></td>
</tr>
<tr>
<td>German contract issues</td>
<td><a href="http://www.beck.de/njw-cor/frames/right/law/law_mausklick.htm">http://www.beck.de/njw-cor/frames/right/law/law_mausklick.htm</a></td>
</tr>
</tbody>
</table>

### Table 9.12. Digital Signatures

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABA CyberNotary Committee</td>
<td><a href="http://www.abanet.org/scitech/ec/cn/home.html">http://www.abanet.org/scitech/ec/cn/home.html</a></td>
</tr>
<tr>
<td>Chiffrement et notaires electroniques</td>
<td><a href="http://www.planete-internet.com/cryptocrypto/decret/">http://www.planete-internet.com/cryptocrypto/decret/</a></td>
</tr>
<tr>
<td>Digital Signature Guidelines</td>
<td><a href="http://www.abanet.org/scitech/ec/isc/dsg.html">http://www.abanet.org/scitech/ec/isc/dsg.html</a></td>
</tr>
<tr>
<td>Digital Signature Legislation (KUB, NL)</td>
<td><a href="http://cwis.kub.nl/~frw/people/hoi/DS-lawsu.htm">http://cwis.kub.nl/~frw/people/hoi/DS-lawsu.htm</a></td>
</tr>
<tr>
<td>Digital Signatures (KUB, NL)</td>
<td><a href="http://cwis.kub.nl/~frw/people/hoi/digsig2.htm">http://cwis.kub.nl/~frw/people/hoi/digsig2.htm</a></td>
</tr>
<tr>
<td>Dsig Table of Contents</td>
<td><a href="http://www.w3.org/Security/Dsig/Overview.html">http://www.w3.org/Security/Dsig/Overview.html</a></td>
</tr>
<tr>
<td>German academic criticism on German digital signature act</td>
<td><a href="http://www.uni-kassel.de/db6/oeff_recht/publikationen/krantisemerkung.html">http://www.uni-kassel.de/db6/oeff_recht/publikationen/krantisemerkung.html</a></td>
</tr>
<tr>
<td>German academic position on digital signature act</td>
<td><a href="http://www.uni-kassel.de/db6/oeff_recht/publikationen/stellungnahme_digitalesignatur.html">http://www.uni-kassel.de/db6/oeff_recht/publikationen/stellungnahme_digitalesignatur.html</a></td>
</tr>
<tr>
<td>German Digital Signature Act</td>
<td><a href="http://www.netlaw.de/gesetze/sigg.htm">http://www.netlaw.de/gesetze/sigg.htm</a></td>
</tr>
<tr>
<td>German digital signature materials</td>
<td><a href="http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Digitale_Signatur/master.htm">http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Digitale_Signatur/master.htm</a></td>
</tr>
<tr>
<td>German Digital Signature Ordinance Draft</td>
<td><a href="http://ourworld.compuserve.com/homepages/cmun/howlaw/law_deville.htm">http://ourworld.compuserve.com/homepages/cmun/howlaw/law_deville.htm</a></td>
</tr>
<tr>
<td>ILPF: Digital Signature Resources</td>
<td><a href="http://www.ilpf.org/digsig/digsig2.htm">http://www.ilpf.org/digsig/digsig2.htm</a></td>
</tr>
<tr>
<td>ILPF: Digital Signature Working Group</td>
<td><a href="http://www.ilpf.org/digsig/digsig.htm">http://www.ilpf.org/digsig/digsig.htm</a></td>
</tr>
<tr>
<td>ILPF: Federal Digital Signature Laws</td>
<td><a href="http://www.ilpf.org/digsig/federal.htm">http://www.ilpf.org/digsig/federal.htm</a></td>
</tr>
<tr>
<td>ILPF: International Digital Signature Laws</td>
<td><a href="http://www.ilpf.org/digsig/intl.htm">http://www.ilpf.org/digsig/intl.htm</a></td>
</tr>
<tr>
<td>Massachusetts page on Digital Signature Law and Policy</td>
<td><a href="http://www.magnet.state.ma.us/itd/legal/pollaw.htm">http://www.magnet.state.ma.us/itd/legal/pollaw.htm</a></td>
</tr>
</tbody>
</table>
### Table 9.13. Enforcement

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atteintes informatiques (Fr)</td>
<td><a href="http://www.fdn.fr/~rabenou/intrus.html">http://www.fdn.fr/~rabenou/intrus.html</a></td>
</tr>
<tr>
<td>Répression fraude informatique (Fr)</td>
<td><a href="http://www.axinet.com/cnejita(TEXTES/LO050186.HTM)">http://www.axinet.com/cnejita(TEXTES/LO050186.HTM)</a></td>
</tr>
</tbody>
</table>

### Table 9.14. Encryption

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;It Came From Planet Clipper &quot;</td>
<td><a href="http://www.stack.nl/~galactus/remailers/index-anon.html">http://www.stack.nl/~galactus/remailers/index-anon.html</a></td>
</tr>
<tr>
<td>Anonymity: Index (NI)</td>
<td><a href="http://www.epfl.ch/SIC/SA/publications/FL95/">http://www.epfl.ch/SIC/SA/publications/FL95/</a> fi-7-95/7-95-page3.html</td>
</tr>
<tr>
<td>Chiffrement des données</td>
<td><a href="http://www.cpsr.org/cpsr/ni/encyber-">http://www.cpsr.org/cpsr/ni/encyber-</a> rights/web/crypto_german_deutsch.html</td>
</tr>
<tr>
<td>Commerce electronique et cryptologie</td>
<td><a href="http://www.argia.fr/ilij/ArticleAvril11.html">http://www.argia.fr/ilij/ArticleAvril11.html</a></td>
</tr>
<tr>
<td>Constitutional Impact of McCain-Kerrey (US)</td>
<td><a href="http://www.grolier.fr/cyberlexnet/SECU/confid.htm">http://www.grolier.fr/cyberlexnet/SECU/confid.htm</a></td>
</tr>
<tr>
<td>Crypto Law Survey</td>
<td><a href="http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/">http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/</a></td>
</tr>
<tr>
<td>Crypto Regulation in Europe (NI conference paper)</td>
<td><a href="http://www.cdt.org/crypto/legis_105/mccain_kerrey/const_impact.html">http://www.cdt.org/crypto/legis_105/mccain_kerrey/const_impact.html</a></td>
</tr>
<tr>
<td>Crypto.Com Homepage</td>
<td><a href="http://cwis.kub.n1/~frw/people/koops/lawsurv.htm">http://cwis.kub.n1/~frw/people/koops/lawsurv.htm</a></td>
</tr>
<tr>
<td>Crypto.com Key Recovery Study</td>
<td><a href="http://cwis.kub.n1/~frw/people/koops/jenc8bjk.htm">http://cwis.kub.n1/~frw/people/koops/jenc8bjk.htm</a></td>
</tr>
<tr>
<td>Cryptographie: les enjeux et l’état de la législation française</td>
<td><a href="http://www.crypto.com/key_study/">http://www.crypto.com/key_study/</a></td>
</tr>
<tr>
<td>Cryptographie? L’information, cible facile sur un réseau public</td>
<td><a href="http://www.argia.fr/ilij/ArticleAvril11.html">http://www.argia.fr/ilij/ArticleAvril11.html</a></td>
</tr>
<tr>
<td>Cryptography and Liberty (JILT)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/">http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/</a></td>
</tr>
<tr>
<td>Data Encryption and the Law(s)</td>
<td><a href="http://web.cnam.fr/Netwerk/Crypto/survey.html">http://web.cnam.fr/Netwerk/Crypto/survey.html</a></td>
</tr>
<tr>
<td>EPIC Archive - Cryptography Policy</td>
<td><a href="http://www.epic.org/crypto">http://www.epic.org/crypto</a></td>
</tr>
<tr>
<td>European Cryptography Resources</td>
<td><a href="http://www.modeemi.cs.tut.fi/~avs/eu-crypto.html">http://www.modeemi.cs.tut.fi/~avs/eu-crypto.html</a></td>
</tr>
<tr>
<td>Extracts from Nicholas Bohm’s Response to DTI (JILT)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/consult/ukcrypt/bohm.htm">http://elj.warwick.ac.uk/jilt/consult/ukcrypt/bohm.htm</a></td>
</tr>
<tr>
<td>German academics’ position on encryption</td>
<td><a href="http://www.provet.org/kk/kindex.htm">http://www.provet.org/kk/kindex.htm</a></td>
</tr>
<tr>
<td>German encryption materials (Provet)</td>
<td><a href="http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Kryptographie/master.htm">http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Kryptographie/master.htm</a></td>
</tr>
<tr>
<td>German encryption materials (U. Marburg)</td>
<td><a href="http://www.iks-jena.de/mitarb/lutz/security/cryptoban/">http://www.iks-jena.de/mitarb/lutz/security/cryptoban/</a></td>
</tr>
<tr>
<td>German encryption sources</td>
<td><a href="http://www.telesec.de/recht.htm">http://www.telesec.de/recht.htm</a></td>
</tr>
<tr>
<td>German legal developments on encryption</td>
<td><a href="http://www.telesec.de/kryptiges.htm">http://www.telesec.de/kryptiges.htm</a></td>
</tr>
<tr>
<td>German positions on encryption policy</td>
<td><a href="http://www.fitug.de/ulf/crypto/verbot.html">http://www.fitug.de/ulf/crypto/verbot.html</a></td>
</tr>
<tr>
<td>Germany: Kryptographie: Rechtliche Situation, politische Diskussion</td>
<td><a href="http://elj.warwick.ac.uk/jilt/Consult/ukcrypt/ukdtipap.htm">http://elj.warwick.ac.uk/jilt/Consult/ukcrypt/ukdtipap.htm</a></td>
</tr>
<tr>
<td>JILT: DTI proposals for the licensing of Trusted Third Parties for the provision of Encryption services</td>
<td><a href="http://elj.warwick.ac.uk/jilt/Consult/ukcrypt/ukdtipap.htm">http://elj.warwick.ac.uk/jilt/Consult/ukcrypt/ukdtipap.htm</a></td>
</tr>
</tbody>
</table>
La Cryptographie

 Lambda 2.12 - Crypto : French TTPs
 L'ancienne loi sur la cryptologie, Loi numero 90-1170
 du 30 Decembre 1990
 Le Chiffrement en France

 Le SCSSI, grand serrurier de la Republique
 Les dispositions de la reglementation touchant à l'usage
 de la cryptologie doivent être assouplies.
 Liberte de crypter
 Links to encryption-related material (UK)
 L'utilisation de chiffrement en France
 Nouvelle loi sur la cryptologie, Loi no. 96-659 du 26
 juillet 1996
 Perkins Coie: Encryption/Cryptography

 PGP-related links

 Phil's Pretty Good Software
 Public Key Infrastructure (PKI) links

 Security and Encryption Links

 Self incrimination and cryptographic keys (US)
 Summary of CBI Response to DTI (JILT)
 Summary of Cyber Liberties Response to DTI (JILT)
 Summary of The Law Society's Response to DTI
 (JILT)
 UK Notarial Forum response to DTI (JILT)

 UKERNA Secure Email Project
 Yahoo! UK & Ireland - Computers and
 Internet:Security and Encryption

 Table 9.15. Intellectual property rights

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actualité : Des agents APP assermentés pour pister les contrefacteurs sur Internet (Fr)</td>
<td><a href="http://www.celog.fr/expertises/agentapp.htm">http://www.celog.fr/expertises/agentapp.htm</a></td>
</tr>
<tr>
<td>Affaire Queneau (Fr)</td>
<td><a href="http://www.legalis.net/legalnet/judiciaire/comm_ord_0697.htm">http://www.legalis.net/legalnet/judiciaire/comm_ord_0697.htm</a></td>
</tr>
<tr>
<td>Affaires Brel et Sardou (Fr)</td>
<td><a href="http://www.celog.fr/expertises/refere.htm">http://www.celog.fr/expertises/refere.htm</a></td>
</tr>
<tr>
<td>Agence pour la Protection des Programmes (Fr)</td>
<td><a href="http://app.legalis.net/paris/">http://app.legalis.net/paris/</a></td>
</tr>
<tr>
<td>AIPL Copyright Law: Pending Legislation, Testimony and Reports to Congress</td>
<td><a href="http://access-iplaw.com/web/complaw.html">http://access-iplaw.com/web/complaw.html</a></td>
</tr>
<tr>
<td>AIPL International IP Sites</td>
<td><a href="http://access-iplaw.com/web/internip.html">http://access-iplaw.com/web/internip.html</a></td>
</tr>
<tr>
<td>Article: &quot;Multimedia und das Urheberrecht&quot; - (De - Multimedia and Copyright)</td>
<td><a href="http://www.jura.uni-tuebingen.de/~s-s/besl/sem97/sem.html">http://www.jura.uni-tuebingen.de/~s-s/besl/sem97/sem.html</a></td>
</tr>
<tr>
<td>Case law -- Trademarks (De)</td>
<td><a href="http://www.netlaw.de/urteile/index.htm#Kennzeichenrecht">http://www.netlaw.de/urteile/index.htm#Kennzeichenrecht</a></td>
</tr>
<tr>
<td>Code de la propriété intellectuelle (Fr)</td>
<td><a href="http://www.celog.fr/cpi/">http://www.celog.fr/cpi/</a></td>
</tr>
</tbody>
</table>
**Site Title** | **Site Address (URL)**
---|---
Database Protection | http://www.lawcircle.com/current.html
Deutscher Bundestag - Enquete-Kommission: Neue Medien und Urheberrecht (New media and copyright) | http://www.bundestag.de/gremien/14344y.htm
Domain name materials (De) | http://stud-www.uni-marburg.de/-Koch2/gcp/leitseiten/DomaIn_Names/master.htm
Domain name rights - article (De) | http://www.anwalt.de/dnslaw/Index.htm
Domain name situation (De) | http://seamless.seamless.com:80/bzt/domain3.html
Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft | http://www.bundestag.de/gremien/14344x.htm
German case law -- Copyright | http://www.netlaw.de/urteile/index.html#Urheberrecht
German domain name law - article (De) | http://www.kanzlei.de/namenssc.htm
German legal issues on Internet links | http://www.beck.de/njw-cor/frames/right/law/law_ernst497.htm
German legal issues regarding copyright | http://www.beck.de/njw-cor/frames/right/2_frameset_law_ernst497.htm
Germany: Legal issues on hyperlinks | http://www.beck.de/njw-cor/frames/right/law/law_koch-copyright.htm
Intellectual Property Rights Overview Jurisprudence droit d'auteur (Fr) | http://www.w3.org/IPR
Jurisprudence et droit d'auteur (Fr) | http://www.aui.fr/Groupes/GT-RRS/jurisprudence.html
La location des oeuvres sur suport numerique (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970510.htm
La propriete intellectuelle d'un serveur Web (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970512.htm
La protection des droits de la personnalité dans les réseaux multimédias (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970409.htm
Le multimedia a l'epreuve du droit francais (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970510.htm
Legal Discussion on Domain Names (De) | http://www.akuern.de/netlaw/dthema.htm
Legal issues regarding Internet links | http://www.beck.de/njw-cor/frames/right/law/law_comment_ernst.htm
Legal problems and domain names (De) | http://lip-service.com/Anwalt/bettinger.html
Multimédia : risques et parades juridiques (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970119.htm
NII Copyright Protection Act of 1995 | http://thomas.loc.gov/cgi-bin/query/z?c104:S.1284:
References to IPR law (De) | http://www.kanzlei.de/wettb.htm
Société de l'information et propriété intellectuelle (Fr) | http://www.grolier.fr/cyberlexnet/COM/A970421.htm
US HR 2441 | http://www.nclis.gov/info/2441.html
Web et droits d'auteur (Fr) | http://www.argia.fr/lij/articleMai96-1.html

**Table 9.16. Jurisdiction**

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AG's Jurisdiction position (US - State of Mn)</td>
<td><a href="http://www.state.mn.us/ebranch/ag/memo.txt">http://www.state.mn.us/ebranch/ag/memo.txt</a></td>
</tr>
<tr>
<td>Brief in “Granite Homes” case (US - State of Mn)</td>
<td><a href="http://www.state.mn.us/ebranch/ag/brief.txt">http://www.state.mn.us/ebranch/ag/brief.txt</a></td>
</tr>
<tr>
<td>Jurisdiction issues on the Internet (De)</td>
<td><a href="http://www.netlaw.de/publikat/ct/ohio.html">http://www.netlaw.de/publikat/ct/ohio.html</a></td>
</tr>
<tr>
<td>Jurisdiction Over Commerce On The Internet</td>
<td><a href="http://www.kslaw.com/menu/jurisdict.htm">http://www.kslaw.com/menu/jurisdict.htm</a></td>
</tr>
<tr>
<td>Law And Borders--The Rise of Law in Cyberspace</td>
<td><a href="http://www.cli.org/X0025_LBFIN.html">http://www.cli.org/X0025_LBFIN.html</a></td>
</tr>
</tbody>
</table>
### Table 9.17. Liability

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyse critique des contrats des services en ligne</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A970505.htm">http://www.grolier.fr/cyberlexnet/COM/A970505.htm</a></td>
</tr>
<tr>
<td>Droit de l'Internet</td>
<td><a href="http://www.legalis.net/legalnet/judiciaire/weber.htm">http://www.legalis.net/legalnet/judiciaire/weber.htm</a></td>
</tr>
<tr>
<td>German Telekommunikationsgesetz - TDG</td>
<td><a href="http://www.netlaw.de/gesetze/tdg.htm">http://www.netlaw.de/gesetze/tdg.htm</a></td>
</tr>
<tr>
<td>Internet, zone de non-droit?</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A960828.htm">http://www.grolier.fr/cyberlexnet/COM/A960828.htm</a></td>
</tr>
<tr>
<td>ISP Liability materials (De)</td>
<td><a href="http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Providerhaftung/master.htm">http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Providerhaftung/master.htm</a></td>
</tr>
<tr>
<td>Jurisprudences - responsabilité des fournisseurs d'accès</td>
<td><a href="http://www.legalis.net/legalnet/judiciaire/responsabilite.html">http://www.legalis.net/legalnet/judiciaire/responsabilite.html</a></td>
</tr>
</tbody>
</table>

### Table 9.18. Personal Data

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>15ème rapport d'activité de la CNIL (Fr)</td>
<td><a href="http://info.in2p3.fr/secur/legal/cnil-presse-rapport15.html">http://info.in2p3.fr/secur/legal/cnil-presse-rapport15.html</a></td>
</tr>
<tr>
<td>Atteintes informatiques (Fr)</td>
<td><a href="http://www.fdn.fr/~rabenou/intrus.html">http://www.fdn.fr/~rabenou/intrus.html</a></td>
</tr>
<tr>
<td>Children's Online Privacy (US)</td>
<td><a href="http://www.ftc.gov/bcp/privacy2/comments3/index.html">http://www.ftc.gov/bcp/privacy2/comments3/index.html</a></td>
</tr>
<tr>
<td>Code SILEX (Fr)</td>
<td><a href="http://www.celog.fr/silex/tome1/sonmaire.htm">http://www.celog.fr/silex/tome1/sonmaire.htm</a></td>
</tr>
<tr>
<td>Computerized Data Bases Containing Sensitive Consumer (US)</td>
<td><a href="http://www.ftc.gov/bcp/privacy2/comments1/index.html">http://www.ftc.gov/bcp/privacy2/comments1/index.html</a></td>
</tr>
<tr>
<td>Consumer Online Privacy (US)</td>
<td><a href="http://www.uni-kassel.de/fb6/oeff_recht/publicationen/stellungnahme_tddg.html">http://www.uni-kassel.de/fb6/oeff_recht/publicationen/stellungnahme_tddg.html</a></td>
</tr>
<tr>
<td>German academic position on data protection act</td>
<td><a href="http://www.netlaw.de/urteile/index.html#Datenschutzrecht">http://www.netlaw.de/urteile/index.html#Datenschutzrecht</a></td>
</tr>
<tr>
<td>German case law -- Personal data</td>
<td><a href="http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Datenschutz/master.htm">http://stud-www.uni-marburg.de/~Koch2/gcp/leitseiten/Datenschutz/master.htm</a></td>
</tr>
<tr>
<td>German data protection materials</td>
<td><a href="http://www.vieweg.de/dud/dud/dudstart.htm">http://www.vieweg.de/dud/dud/dudstart.htm</a></td>
</tr>
<tr>
<td>German journal on data protection and security</td>
<td><a href="http://www.netlaw.de/gesetze/tddsg.htm">http://www.netlaw.de/gesetze/tddsg.htm</a></td>
</tr>
<tr>
<td>German Telekommunikationsdatenschutzgesetz - TDDSG</td>
<td><a href="http://www.fitug.de/news/agv.html">http://www.fitug.de/news/agv.html</a></td>
</tr>
<tr>
<td>User's Association position on personal data (De)</td>
<td><a href="http://www.celog.fr/info_lib/index.html">http://www.celog.fr/info_lib/index.html</a></td>
</tr>
<tr>
<td>Informatique &amp; Libertés (Fr)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/dp">http://elj.warwick.ac.uk/jilt/dp</a></td>
</tr>
<tr>
<td>Data Protection (JILT)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/consult/twdp/">http://elj.warwick.ac.uk/jilt/consult/twdp/</a></td>
</tr>
<tr>
<td>CFI Response to Data Protection Consultation Paper (UK)</td>
<td><a href="http://www.legalis.net/legalnet/jurisinfo.htm">http://www.legalis.net/legalnet/jurisinfo.htm</a></td>
</tr>
<tr>
<td>Jurisprudence : Informatique et libertés (Fr)</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A970117.htm">http://www.grolier.fr/cyberlexnet/COM/A970117.htm</a></td>
</tr>
<tr>
<td>La première réforme des bases de données juridiques publiques (Fr)</td>
<td><a href="http://www.fdn.fr/~rabenou/infolib.html">http://www.fdn.fr/~rabenou/infolib.html</a></td>
</tr>
<tr>
<td>Loi No 78-17 du 6 janvier 1978, Loi Informatique et Liberté (Fr)</td>
<td><a href="http://www.axinet.com/cnejita/TEXTES/LO050186.HTM">http://www.axinet.com/cnejita/TEXTES/LO050186.HTM</a></td>
</tr>
<tr>
<td>Répression fraude informatique (Fr)</td>
<td><a href="http://www.open.gov.uk/dpr/answer/content.htm">http://www.open.gov.uk/dpr/answer/content.htm</a></td>
</tr>
</tbody>
</table>
### Table 9.19. Privacy

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Surfing</td>
<td><a href="http://www.anonymizer.com">http://www.anonymizer.com</a></td>
</tr>
<tr>
<td>Commerce electronique (Fr)</td>
<td><a href="http://www.celog.fr/expertises/breves/semaine30_97.htm#commerceelectronique">http://www.celog.fr/expertises/breves/semaine30_97.htm#commerceelectronique</a></td>
</tr>
<tr>
<td>De la protection de la vie privée, des cookies indigestes (Fr)</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A970423.htm">http://www.grolier.fr/cyberlexnet/COM/A970423.htm</a></td>
</tr>
<tr>
<td>Electronic Privacy Information Center (EPIC)Home</td>
<td><a href="http://www.epic.org">http://www.epic.org</a></td>
</tr>
<tr>
<td>FTC Letter to Congress on Consumer Privacy (US)</td>
<td><a href="http://www.ftc.gov/os/9707/privac9b.htm">http://www.ftc.gov/os/9707/privac9b.htm</a></td>
</tr>
<tr>
<td>FTC Steps on Consumer Privacy Issues (US)</td>
<td><a href="http://www.ftc.gov/opa/9707/congpri2.htm">http://www.ftc.gov/opa/9707/congpri2.htm</a></td>
</tr>
<tr>
<td>German Privacy Information</td>
<td><a href="http://www.rewi.hu-berlin.de/Datenschutz/index.html">http://www.rewi.hu-berlin.de/Datenschutz/index.html</a></td>
</tr>
<tr>
<td>Internet Privacy Coalition</td>
<td><a href="http://www.privacy.org/IPC">http://www.privacy.org/IPC</a></td>
</tr>
<tr>
<td>Loi No 78-17 du 6 janvier 1978, Loi Informatique et Liberté (Fr)</td>
<td><a href="http://www.fdn.fr/~rabenou/infolib.html">http://www.fdn.fr/~rabenou/infolib.html</a></td>
</tr>
</tbody>
</table>

### Table 9.20. Reliability

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commerce électronique</td>
<td><a href="http://www.fdn.fr/~rabenou/massy.html">http://www.fdn.fr/~rabenou/massy.html</a></td>
</tr>
<tr>
<td>EPIC Archive - Computer Security</td>
<td><a href="http://www.epic.org/security">http://www.epic.org/security</a></td>
</tr>
<tr>
<td>French information security gopher</td>
<td>gopher://gopher.urec.fr:70/11/Securite/Docs/Lois</td>
</tr>
<tr>
<td>INFOSEC: ETS preparatory studies</td>
<td><a href="http://www.cordis.lu/infosec/src/prep.htm">http://www.cordis.lu/infosec/src/prep.htm</a></td>
</tr>
<tr>
<td>Security and Encryption Links</td>
<td><a href="http://www.cs.auckland.ac.nz/~pgut001/1inks.html">http://www.cs.auckland.ac.nz/~pgut001/1inks.html</a></td>
</tr>
<tr>
<td>Services en ligne et sécurités</td>
<td><a href="http://www.grolier.fr/cyberlexnet/COM/A970310.htm">http://www.grolier.fr/cyberlexnet/COM/A970310.htm</a></td>
</tr>
</tbody>
</table>

### Table 9.21. Tax

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA State Taxation White Paper</td>
<td><a href="http://www.isa.net/about/releases/taxwhpap.html">http://www.isa.net/about/releases/taxwhpap.html</a></td>
</tr>
</tbody>
</table>

### Table 9.22. Telecommunications, etc.

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Strategic Commitments and the Principle of Reciprocity in Interconnection Pricing” (US)</td>
<td><a href="http://econwpa.wustl.edu/eprints/io/papers/9701/9701001.abs">http://econwpa.wustl.edu/eprints/io/papers/9701/9701001.abs</a></td>
</tr>
<tr>
<td>Academic articles on telecommunication law (De)</td>
<td><a href="http://www.uni-muenster.de/Jura/wivwr/seminar.html">http://www.uni-muenster.de/Jura/wivwr/seminar.html</a></td>
</tr>
<tr>
<td>Article about “Digital Tornado” (VTW)</td>
<td><a href="http://www.vtw.org/">http://www.vtw.org/</a></td>
</tr>
<tr>
<td>British Telecom (UK)</td>
<td><a href="http://www.bt.com/">http://www.bt.com/</a></td>
</tr>
<tr>
<td>Centre for Communications Systems Research (Cambridge) (UK)</td>
<td><a href="http://www.ccsr.cam.ac.uk">http://www.ccsr.cam.ac.uk</a></td>
</tr>
<tr>
<td>Commentary to new Telecommunications Act (De)</td>
<td><a href="http://www.netlaw.de/publikat/ct/nadel.htm">http://www.netlaw.de/publikat/ct/nadel.htm</a></td>
</tr>
<tr>
<td>De nouvelles règles de jeu pour les telecommunications en France (Fr)</td>
<td><a href="http://www.telecom.gouv.fr/francais/regle-fr.htm">http://www.telecom.gouv.fr/francais/regle-fr.htm</a></td>
</tr>
<tr>
<td>Discussion on IuKDG (De)</td>
<td><a href="http://www.beck.de/njw-cor/frames/right/law/law_koch-kommentar_mmg_2706.htm">http://www.beck.de/njw-cor/frames/right/law/law_koch-kommentar_mmg_2706.htm</a></td>
</tr>
<tr>
<td>Discussion on telecommunications law (De)</td>
<td><a href="http://www.beck.de/njw-cor/frames/right/law/law_lammich.htm">http://www.beck.de/njw-cor/frames/right/law/law_lammich.htm</a></td>
</tr>
<tr>
<td>France Regulation (Fr)</td>
<td><a href="http://www.ispo.cec.be/esis/FRegresu.html">http://www.ispo.cec.be/esis/FRegresu.html</a></td>
</tr>
</tbody>
</table>
### Table 9.23. Other

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informations- und Kommunikationsdienste-Gesetz - IuKDG (De)</td>
<td><a href="http://www.iid.de/rahmen/iukdgbt.html">http://www.iid.de/rahmen/iukdgbt.html</a></td>
</tr>
<tr>
<td>Laboratories of DeRegulation? (JILT)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/telecoms/97_1hunt/">http://elj.warwick.ac.uk/jilt/telecoms/97_1hunt/</a></td>
</tr>
<tr>
<td>Länder law on media services draft (De)</td>
<td><a href="http://www.netlaw.de/gesetze/stvmd_3.htm">http://www.netlaw.de/gesetze/stvmd_3.htm</a></td>
</tr>
<tr>
<td>Le paysage réglementaire et économique (Fr)</td>
<td><a href="http://www.telecom.gov.fr/francais/activ/telecom/telecdoc.htm">http://www.telecom.gov.fr/francais/activ/telecom/telecdoc.htm</a></td>
</tr>
<tr>
<td>Legal Approval on the division of tasks between Federal and Länder authorities for info-services (De)</td>
<td><a href="http://www.mercury.co.uk/">http://www.mercury.co.uk/</a></td>
</tr>
<tr>
<td>Les documents de référence, les publications et les études (Fr)</td>
<td><a href="http://www.technologylaw.com/us_comm.html">http://www.technologylaw.com/us_comm.html</a></td>
</tr>
<tr>
<td>Mercury Communications (UK)</td>
<td><a href="http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc17020.html">http://www.fcc.gov/Bureaus/Miscellaneous/News_Releases/1997/nrmc17020.html</a></td>
</tr>
<tr>
<td>Netscape Universal Service Comments</td>
<td><a href="http://www.ofstel.gov.uk">http://www.ofstel.gov.uk</a></td>
</tr>
<tr>
<td>OFTEL (Office of Telecommunications) (UK)</td>
<td><a href="http://www.ofstel.gov.uk/consumer/univ_2.htm">http://www.ofstel.gov.uk/consumer/univ_2.htm</a></td>
</tr>
<tr>
<td>OFTEL Access to the Internet for Schools (UK)</td>
<td><a href="http://www.ofstel.gov.uk/superhwy/multi.htm">http://www.ofstel.gov.uk/superhwy/multi.htm</a></td>
</tr>
<tr>
<td>OFTEL Universal Telecommunications Service - 97 (UK)</td>
<td><a href="http://www.ofstel.gov.uk/telecur.htm">http://www.ofstel.gov.uk/telecur.htm</a></td>
</tr>
<tr>
<td>OFTEL: Education Superhighway (UK)</td>
<td><a href="http://www.telecom.gov.fr/francais/activ/telecom/lr96.htm">http://www.telecom.gov.fr/francais/activ/telecom/lr96.htm</a></td>
</tr>
<tr>
<td>Projet de loi sur la nouvelle réglementation des télécommunications en France (Fr)</td>
<td><a href="http://www.kanzlei.de/edvr.htm">http://www.kanzlei.de/edvr.htm</a></td>
</tr>
<tr>
<td>References to computer and telecommunications Law (De)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/telecoms/3naftel/">http://elj.warwick.ac.uk/jilt/telecoms/3naftel/</a></td>
</tr>
<tr>
<td>Regulating for Competition in the US and EU Telecoms Markets (Abstract) (JILT)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/bookrev/3lockett/3.htm">http://elj.warwick.ac.uk/jilt/bookrev/3lockett/3.htm</a></td>
</tr>
<tr>
<td>Review of Internet Law and Regulation (JILT)</td>
<td><a href="http://www.bundesregierung.de/.bin/lay/bmpt/rede.html">http://www.bundesregierung.de/.bin/lay/bmpt/rede.html</a></td>
</tr>
<tr>
<td>Speech by the German Minister of Telecommunication on Liberalization</td>
<td><a href="http://www.spp.umich.edu/telecom">http://www.spp.umich.edu/telecom</a></td>
</tr>
<tr>
<td>Telecom Information Resources (U. Michigan)</td>
<td><a href="http://elj.warwick.ac.uk/jilt/telecoms/default.htm">http://elj.warwick.ac.uk/jilt/telecoms/default.htm</a></td>
</tr>
<tr>
<td>Telecommunications Act of 1996 - Table of Contents (US)</td>
<td><a href="http://www.fcc.gov/telecom.html#fcc">http://www.fcc.gov/telecom.html#fcc</a></td>
</tr>
<tr>
<td>Telecommunications Act of 1996 (US)</td>
<td><a href="http://www.si.umich.edu/~prie/tprc/">http://www.si.umich.edu/~prie/tprc/</a></td>
</tr>
<tr>
<td>Telecommunications Regulation (US)</td>
<td></td>
</tr>
<tr>
<td>Telekommunikationsgesetz (De)</td>
<td></td>
</tr>
</tbody>
</table>

**Table:**

<table>
<thead>
<tr>
<th>Site Title</th>
<th>Site Address (URL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bibliography on Network Economics</td>
<td><a href="http://raven.stern.nyu.edu/networks/biblio.html">http://raven.stern.nyu.edu/networks/biblio.html</a></td>
</tr>
<tr>
<td>Economics of Networks Internet Site</td>
<td><a href="http://raven.stern.nyu.edu/networks/">http://raven.stern.nyu.edu/networks/</a></td>
</tr>
<tr>
<td>EPIC Archive International Free Speech</td>
<td><a href="http://www.epic.org/free_speech/intl">http://www.epic.org/free_speech/intl</a></td>
</tr>
<tr>
<td>Internet Economics Workshop notes (MIT)</td>
<td><a href="http://rccp.mit.edu/Workshops/ew-notes.txt">http://rccp.mit.edu/Workshops/ew-notes.txt</a></td>
</tr>
<tr>
<td>Rechtliche Probleme beim Electronic Commerce (De)</td>
<td><a href="http://www.netlaw.de/medien/dik96.htm">http://www.netlaw.de/medien/dik96.htm</a></td>
</tr>
<tr>
<td>Special Issue of the International Journal of Industrial Organization on the Economics of Networks</td>
<td><a href="http://raven.stern.nyu.edu/networks/special.html">http://raven.stern.nyu.edu/networks/special.html</a></td>
</tr>
<tr>
<td>Year-X Electronic Commerce Main Menu</td>
<td><a href="http://www.year-x.co.uk/ec/home.htm">http://www.year-x.co.uk/ec/home.htm</a></td>
</tr>
</tbody>
</table>
10. PERSONAL CONTACTS

The following individuals and organisations were among those who provided us with information. This information was not solicited or intended as legal advice, and these individuals bear no responsibility for the information or conclusions contained in this Report.

France

- Eric Barbry, Cabinet d’Avocats Bitoun, Verrechia et Associés, Paris/Association Cyberlex, France.
- Pascal Lagarde, SERICS (Service des Industries de Communication et de Service), Ministere de l’Economie, des Finances et de l’Industrie.
- Véronique Barry, SJTI (Service Juridique et Technique de l’Information et de la Communication), Ministere de l’Economie, des Finances et de l’Industrie.
- Sébastien Canivet, Association Citadel, Electronic Freedom Foundation France.
- Brigitte Bogucki,
- Richard Bellanger, DESS (Droit et Systèmes d’Information)
- Roger Wiesenbach, Law-France

Germany

- Associates at Projektgruppe Verfassungsvertragliche Technikgestaltung (Provet), Darmstadt
- Dr. jur. Johann Bizerwissenschaftlicher Assistent am Institut für öffentliches Recht der Johann Wolfgang Goethe-Universität in Frankfurt a. M.
- Christopher Kuner, Attorney-at-Law, Gleiss Lutz Hootz Hirsch, Frankfurt
- Professor Dr. Ulrich Sieber, Ordinarius für Strafrecht, Strafprozeßrecht, Informationsrecht und Rechtsinformatik an der Universität Würzburg
- Prof. Dr. jur. W. Kilian, Institut für Rechtsinformatik, Universität Hannover
- Prof. Mestmacher, Max-Planck Institut Copyrights - Stefan Engel-Flechsig, Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie

United Kingdom

- Members of the University of Warwick Law School and affiliates of the Centre for Globalisation, Regionalism and Emerging Markets, including Professor Hugh Beale, Professor Julio Faundez, Lesley Hitchens, Professor Morten Hviid, Roger Leng, Duncan Matthews, and Dallal Stevens.
- Staff of the Parliamentary Office of Science and Technology.
- Staff of the Law and Economic Working Group, The Lord Chancellor’s Department
- Professor Paul David, All Souls College, Oxford
- Professor Danial Quah, London School of Economics
- Professor Stephan Szymanski, London Business School
- Robert Tyler, BBC Multimedia Centre
- 178 -

- Professor Ian Lloyd, Strathclyde University

United States

- Professor Jan Brueckner, University of Illinois
- Professor Jonathan Baker, US Federal Trade Commission
- Professor A. Mitchell Polinsky, Stanford University
- Professor Hal Varian, University of California at Berkeley
- Dr. Walter Baer, RAND Corporation, Santa Monica, California
- Dr. Robert Andersen, RAND Corporation, Santa Monica, California
- Dr. Tora Bikson, RAND Corporation, Santa Monica, California
- Professor Ingo Vogelsang, Boston University
- Bruce Colfin, partner, Jacobson and Colfin, PC, New York, NY.