LEGAL PROGRAMMING:
Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond
Other published titles in the series:

E-BUSINESS MANAGEMENT: *Integration of Web Technologies with Business Models* / Michael J. Shaw
VIRTUAL CORPORATE UNIVERSITIES: *A Matrix of Knowledge and Learning for the New Digital Dawn* / Walter R.J. Baets & Gert Van der Linden
SCALABLE ENTERPRISE SYSTEMS: *An Introduction to Recent Advances* / edited by Vittal Prabhu, Soundar Kumara, Manjunath Kamath
LEGAL PROGRAMMING:
Designing Legally Compliant RFID and Software Agent Architectures for Retail Processes and Beyond

Brian Subirana
Malcolm Bain

Springer
Dedication

This book is dedicated to:

B. Subirana to Mercedes Vilanova Ribas

M. Bain to Natacha Rodríguez Jorro
## Contents

Dedication \hspace{1cm} v  
List of Figures \hspace{1cm} ix  
List of Tables \hspace{1cm} xi  
Preface \hspace{1cm} xv  
Foreword \hspace{1cm} xix  
Chapter 1: Introduction \hspace{1cm} 1  
Chapter 2: Contracts \hspace{1cm} 57  
Chapter 3: Intellectual Property Rights \hspace{1cm} 101  
Chapter 4: Consumer Protection \hspace{1cm} 145  
Chapter 5: Privacy \hspace{1cm} 193  
Chapter 6: Conclusions \hspace{1cm} 245  
References \hspace{1cm} 295  
Index \hspace{1cm} 311
List of Figures

*Figure 1-1.* Research Scenario Interactions ................................................................. 46
*Figure 1-2.* Research Process .......................................................................................... 54
*Figure 2-1.* Contract Law Analysis .................................................................................. 58
*Figure 3-1.* Intellectual Property Rights Analysis ........................................................... 103
*Figure 4-1.* Consumer Protection Law Analysis ............................................................... 147
*Figure 5-1.* Personal Data Protection Analysis ................................................................. 194
*Figure 6-1.* MIT Process view of the Firm ....................................................................... 266
List of Tables

Table 1-1. Some legal issues relating to the Internet architecture ........................................... 3
Table 1-2. Online commerce risks .............................................................................................. 6
Table 1-3. IPv6 .............................................................................................................................. 9
Table 1-4. Agents and traditional computing systems ................................................................... 20
Table 1-5. Applications of intelligent agent technology in ecommerce ........................................ 25
Table 1-6. Ecommerce oriented agent projects ............................................................................. 26
Table 1-7. Agent characteristics and legal issues .......................................................................... 32
Table 1-8. Legal issues of the Consumer Buying Behaviour model .............................................. 33
Table 1-9. Legal definitions of agents .......................................................................................... 34
Table 1-10. Potential Legal areas concerned by the research Agents' processes ......................... 47

Table 2-1. Laws on electronic contracting .................................................................................... 62
Table 2-2. Summary Description of Agent A ................................................................................ 64
Table 2-3. Summary Description of Agent B ................................................................................ 64
Table 2-4. Summary Description of Agent C ................................................................................ 65
Table 2-5. Electronic and Digital Signatures in the EU Framework Directive ............................... 83
Table 2-6. Legal risks of Agent C’s contracting processes ............................................................. 99

Table 3-1. Overview of Agent D .................................................................................................... 113
Table 3-2. IPR concerns raised by Agent D processes ................................................................. 116
Table 3-3. Some suggested processes for legalising shopping Agent D’s processes .................. 137

Table 4-1. Issues between agent provider and consumer ............................................................. 163
Table 4-2. Issues between consumers and retail stores ............................................................... 164
Table 4-3. Consumer Protection processes for advertising and selling agents ......................... 191

Table 5-1. Justifications for personal data processing ................................................................. 204
Table 5-2. Anonymiser technologies ............................................................................................ 227
Table 5-3. Elements of P3P ......................................................................................................... 230
Table 5-4. Advertising and Selling Agent - Privacy processes .................................................... 240
Table 5-5. Shopping Agent C - Privacy processes ....................................................................... 241

Table 6-1. Example Use-Case with Consumer PMA ................................................................. 258
Table 6-2. Business Process Modelling Technologies ................................................................. 287
Contributing Authors

Brian Subirana, Associate Professor at IESE Business School

Visiting Associate Professor of RFID, Auto-ID Laboratory and MIT Department of Mechanical Engineering.

Visiting Associate Professor of Information Technologies at the Center for Coordination Science of the MIT Sloan School of Management.

Corresponding author:

subirana@iese.edu, subirana@mit.edu.

IESE Business School, Avda Pearson 21, 08034 Barcelona

MIT Auto-ID Laboratory, Building NE46-6th Floor, 400 Technology Square, Cambridge, MA 02139

Center for Coordination Science, Sloan School of Management, 3 Cambridge Center, MIT NE20-336, Cambridge, MA 02142, USA

Prof. B. Subirana holds a PhD in Computer Science from the AI Lab at MIT and an MBA from MIT Sloan where he has been Visiting Associate Professor in 2002, 2003 and 2004. Since 2004 he is also Visiting Associate Professor at the MIT Department of Mechanical Engineering. Prior to joining IESE, he was with The Boston Consulting Group. With over 200 publications, his research focuses on the computational modeling of firms including the MIT Process Handbook, Auto-ID/RFID, E-contracting; advanced learning technologies; and on the role of the CEO in Information Technology.
Malcolm Bain

M. Bain is an English solicitor, with a Masters Degree in International Studies (European Law specialty). His work experience includes 4 years in a City law firm in London and 3 years in an IT firm and recently as researcher for IESF Business School, working on ICT law and Information Society research projects, including ecommerce platforms, distributed systems and software agents. He has also taught English Legal System and Legal Translation at graduate level.
Preface

What would we show somebody who awoke from 500 years’ sleep to illustrate life at the beginning of the 21st century?

One possibility would be to have her stand in the junction of Massachusetts Ave and Memorial Drive in Cambridge, MA. She would see vehicles of all types, including lorries carrying boxes, pallets, bottles or tin cans; tarmac streets and slim metal bridges; sailing, rowing or motor boats on the river; cables over and under the streets for electricity and telephones; and people in today’s latest fashion, including fancy running shoes with lights on their heels and cell phone watches. Focusing in on nearby stores, she might see shoppers wandering around the shelves, listening to music on mp3 players through headphones, and the cashier running up the bill on the automatic till, complete with keyboard and computer screen.

The different details of this view would provide insights into society today, and recent and not so recent history in science and engineering, new businesses and lifestyles. From the motor engine to cars, planes and personal transport. From electricity to telephones to the Internet. From calculators to computers and PDAs. From local shops to large supermarkets – specialist or general purpose–, including cash and carry and home delivery. A similar view from Piazza San Marco in 15th century Venice or Leicester Square in the 19th century London would also have this special power to provide an understanding of society at that particular time.

What could we do if we wanted to understand how the world may be in the future? The store or shopping mall today is a meeting place and emblematic of our current lifestyle. Like the person at the crossroads looking at her close surroundings, we could sit in a future grocery store trolley and consider life within the shop. We could simply sit there and look at a few specific processes: advertising and making special offers, consulting product details, looking for complementary items, comparing brands. Just as the view on Harvard Bridge can reveal wider aspects of today’s society, the store’s processes are like a lens showing what the future will be like in a more general way.
Through this lens, we can see and try to understand a section of future lifestyles and of the world: new technologies, new processes, new attitudes.

This is what we have done in this work, focusing on a few select shopping processes, supported by emerging agent-based computing technologies linked to RFID-enhanced objects and environment, to act as our lens for the future.

As part of this quest for understanding, we have considered the alignment and compliance of these shopping processes with the current and emerging legal framework. The law, as the collection of normative precepts underlying the structure and interactions of society, not only establishes the regulatory framework of this future, but also creates a series of hurdles and challenges, risks and opportunities to get there. The law will directly affect the design and structure of this near future, both for the development and programming of hardware and software (in our case, for grocery shopping), and also for the business and social processes supported by these technologies.

We have considered four particular areas of law that define the behaviour of actors within this view “from-the-store-trolley”: contract law covering buying and selling processes, intellectual property rights for the protection of digital materials and content, and consumer and privacy protections that regulate the interactions between businesses and individuals, and are fundamental for achieving trust in what has been called the Information Society.

These laws may determine certain constraints – and opportunities – for business and technical processes in the future. An easy example: many potential applications for agent technology will involve the identification of users and the use of their personal data by merchants or other organisations. We could cite payment authentication agents, or customisation agents for merchants to maintain details of customer purchases for targeted marketing and personalised assistance during the shopping experience. From a legal perspective the collection, storage and processing of this data, not to mention the transferring of the data to third parties for synergies with profiling and other marketing activities, raise serious issues as regards the privacy of individuals and the invasion of their private lives. They may also constitute breach of personal data protection rules under European and national legislation. The design of these processes and the development of supporting technologies (e.g. software agents) will have to take these rules into account.

In this research, we have learned a number of things. Among them, we have learned that while almost all on-line commercial activities and related processes may on the whole be illegal, agent-based transactions in RFID-augmented environments will expose businesses and individuals to higher levels of risk – while providing a glimpse of how certain obstacles created by the digitisation of society may be overcome. Our research has also shown that the hurdles towards regulatory compliance and trust in future and emerging technologies can be usefully analysed with a process view. This view provides a level of abstraction where the mismatch between law and technology may potentially be reconciled.
This work has not only led us to outline the legal risks for certain shopping processes in this not-too-distant future scenario, it has also enabled us to determine certain next steps for research in this area. On the one hand, the creation of a formal taxonomy of high level concepts that are legally and technically meaningful, together with the development of legal programming methodology and technologies. On the other, widening the sphere of interest, we believe that research should aim to develop unified view of the firm so that it can act as a lens not just for the legal aspects of society but also for understanding business and technological evolution.
Foreword

The ability to express and apply law to specific facts requires intelligence. This is true both of humans and computers. Though a challenging problem, there are computer systems today that show it can be done.

But it is genius to show with simplicity how people can structure their activities in light of the law to achieve their goals at work, home and in life generally. Such is the task Brian Subirana and Malcolm Bain have undertaken in this book, and they have succeeded in pointing the way for those that follow.

The approach to legal programming proposed in this book provides a workable, generic and reusable process. Subirana and Bain show how legal principles can be modeled and digitally codified in a standardized method. This process paints a picture of a future where the law can be directly supported and reflected in transactional systems, reducing the costs and delays of regulatory compliance, avoiding the harms these laws were created to combat, and enhancing the property protection, privacy and other freedoms and rights people expect. A vision of cross-border, efficient, real-time, interoperable systems of commerce, trade and business is made possible, with a sense of compelling nearness.

As nations teeter on the edge of the information age, it is becoming clear that as yet unimagined technologies, professions and entire economic sectors will soon emerge. Examples from the dawning of the industrial age illustrate this: electricity lead to mass production; the automobile lead to suburbia; the telephone lead to teleworking, etc. In all these examples they entirely transformed industries and formed new economic, political, social and legal regimes that followed.

In previous global economic transformations, the law has kept pace by supporting and reflecting the underlying changes. The underlying principles of contract law have been applied by judges, attorneys and the parties to their newly emerging circumstances.
For example, several contract principles have been unchanged but applied in novel ways to novel facts from agrarian, to industrial scenarios, to pen and seal, to typed name, and now to any "symbol, sound or process".

Now, however, at the advent of the digital society, the law will not merely be applied to novel situations, it will itself be revolutionized by digital technology. MIT coined the view that computer code can itself be a form of law, by structuring the rights and responsibilities of users of systems.

In many ways directions markup languages in the legal arena, point out several ways in which computer code is in fact becoming de facto or de jure law. Now, it can also be said we are seeing the start of law addressing itself directly to computer systems and code. With RFID, Auto-ID, EPC and ubiquitous intelligence, there is an increasing opportunity for law makers to enact statutes and regulations that read like computer code. For example, one can point out the specific system requirements in various e-Banking regulations, eCommerce and digital signature statutes and extrapolate a point of intersection where the law will be enacted as code or as models of code, perhaps according to the types of programming models and languages Subirana and Bain propose.

Daniel Greenwood, Esq
Lecturer, MIT
Director, MIT E-Commerce Architecture Program
Chapter 1

INTRODUCTION
Almost all on-line activities are illegal...

And so when men have both done and suffered injustice and have had experience of both, not being able to avoid the one and obtain the other, they think that they had better agree among themselves to have neither; hence there arise laws and mutual covenants.
Plato's Republic, Book 2. (Glaucon)

1. INTERNET TECHNOLOGIES AND THE LAW

1.1 Almost all online business activities are illegal

From many viewpoints, most commercial online transactions do not comply with the law and, even if they do, they generally fail to meet users’ expectations in various ways. Recent examples of infringements include the invalidity of browser-wrap contracts in certain circumstances, multiple cases of breaches of European data protection requirements in relation to the collection and security of storage of personal data during the course of transactions, or the non-collection or payment of tax (VAT or Sales Tax) on cross border or interstate transactions.

These transactions are also carried out in a way which does not reflect the desires of the negotiating parties. For example, weaker or more technically lacking parties (usually buyers) generally have to accept the terms of the other party (seller). In Business to Consumer (B2C) ecommerce, this is in fact close to a real world store transaction, where shoppers are basically required to purchase goods subject to the store's terms and conditions. However in the real-world business to business (B2B) context most contracts are individually negotiated to achieve a balance of risk and allocation of liability. This is often not the case in B2B ecommerce.
In addition, online transactions rarely satisfy lower level non-binding but still valid standards of conduct, good faith and, in the consumer context, fair trading\textsuperscript{1}. While some of these norms are indeed legislated in certain jurisdictions (for example, good faith obligations in negotiations in some European continental jurisdictions), they are often only contained in sector codes of conduct, like the direct marketing association’s codes. Non-binding “norms” in the area of the marketing and sale of goods and services online (including spam emails - unsolicited commercial communications, in European legal language, which have now been regulated -, and banners, pop-ups, etc.), secondary actions involving the collection and use of personal data (the planting of cookies, web-bugs, etc.), and regarding the exclusion of liability and the provision of warranties or guarantees, are also widely flouted by online commerce platforms.

From a theoretical economic point of view, it can also be argued that these transactions lack efficiency due to the failure to fulfil participant expectations and demands. That is to say, parties have to accept what is technically feasible or technically required by online commerce platforms, but which is not necessarily the most economically efficient for them. This creates higher transaction costs than necessary.

Despite all its promises of efficiency and cost reduction, much of ecommerce seems therefore to break the laws of the market and society as well as the laws under the constitution.

In this, we are not just referring to the legal issues surrounding the technologies that underlie the Internet and World Wide Web (WWW) and create the network architecture and framework for ecommerce: these have their own separate legal issues. The Domain Name System is bedevilled with problems of cyber-squatting, typo-squatting, competing and non-competing uses of domain names, reverse hijacking and free speech, and overall governance issues. The patenting of technology and business methods, i.e. of protocols and standards, software applications and ecommerce models (e.g. "One click" shopping, information downloading, etc.), is still debated and is currently seen as an obstacle to technical and commercial development. The simple use of hyperlinks is considered a violation by some parties (especially deep-linking or in-lining links), an infringement of intellectual property rights, trademarks, database rights, trespass or unfair competition (see Table 1 below).

\textsuperscript{1} What L. Lessig might call market or social "norms" in \textit{Code}, 1999. Some good faith and fair trading principles are indeed binding in certain European jurisdictions, but we refer here to the slightly greyer area of trading standards.
### Linking

While no case seems to be definitive on the question, examples of hyperlink cases include the following. In *Ticketmaster v. Tickets.com*, a California court decided that hyperlink from one website to another does not constitute copyright infringement: "deep linking by itself... does not necessarily involve unfair competition". It was argued that hypertext linking is not per se illegal if "consumers understand whose site they are on and that one company has not simply duplicated another's page", however when it is coupled with other business practices, it may be improper (e.g. anti-competitive practices). This was what happened in *E-bay v. Bidder's Edge*, where Bidder's Edge robots continuously searched and linked to E-bay's site to provide auction information to users and overloaded of E-bay site's servers.

#### Deeplinking

In *Danske Dagblades Forening v. Newsbooster.com*, a Danish court declared that Newsbooster violated copyright laws by "deep linking" to newspaper articles of the Danish Newspaper Publishers' Association and ordered Newsbooster to stop linking, bypassing the front page (with advertising revenue). Its service was competing directly with the newspapers and "eroded the value of banner advertising on their website", in breach of the Danish Copyright Act and the Danish Marketing Act. In December 2000, StepStone, an on-line recruitment company, obtained a court order in Germany under implementation of the EU copyright and database regulations preventing OFiR, a Danish rival from deep-linking to StepStone's job advertisements. StepStone argued this linking to be prejudicial to its brand position in the long term, and visitors were not taken to the home page and therefore did not see its banner advertising.

#### Framing

In *Kelly v. Arriba*, in San Francisco in February 2002, the Court of Appeals held that a search engine that linked to copyrighted material by "framing" it in a new browser window (directly linked to the referring site) infringed the copyright owner's rights.

#### Exemptions

In August 2000, in *PCM v. Kranten.com*, an Amsterdam court ruled in support of deep linking in a case where one news site was linking to stories on other web sites of various newspapers. While the plaintiff argued that the links would bypass the branding and advertising on the home page of its web site, the court decided that deep linking to other sites is a widespread and commonly accepted practice on the Internet and that, under copyright law, there is an exception to copying for the reporting of current events, provided there is sufficient acknowledgement. In March 2003 a Spanish court denied penalties against *ajoderse.com* for linking to illegal content, as it could not be proved that the website had knowledge of the illegality of the linked page. While in Napster it was held that the system directly infringed copyright, providing and encouraging links to infringing materials (and indirectly facilitating individual file sharers' copyright infringement), recently (April 2003) *Grokster* and *Morpheus* — with a more decentralised system - were held exempt of liability for not contributing to or authorizing it.

---

Database protection
In *Mainpost v Newsclub*, Munich's Upper Court held that using a search engine to locate stories on newspapers' sites violates European Union database protection law. NewsClub was accused of searching through and linking directly to Mainpost content which the court held was entitled to database protections. The actions of Newsclub led a systematic and repeated reproduction of immaterial parts of the database, an act which unreasonably violates the rights of the database producer.

Trademark protection
In *Shetland Times v. Wills*, it was held that trademarks use of third party trademarks to link to other sites could constitute a breach of the trademark protections. In *Playboy Enterprises Inc. v. Welles* Playboy objected to the use of its trademark in the webpage of one of its models, and there have been several cases of using competitors trademarks as website tags (metatags) or in invisible print, so they are picked up by search engines (*Road Tech Computer Systems v. Mandata (Management & Data Services) Limited*).

What we are discussing are simple commercial (and also non-commercial) activities carried out within this imperfect technological framework. Despite recent attempts to comply with relevant laws — enhanced privacy policies and statements, improved contracting processes, encryption and digital signatures for confidentiality and security, etc. — there are many specific instances of potential and real violations that occur during the course of any commercial transaction. These include accessing and extracting contents from online databases, the reproduction and distribution of protected or confidential materials, the conclusion of certain contracts where parties have not been informed of their rights, or attempts to remove or restrict rights that cannot be limited. This latter, for instance, is most evident in consumer transactions and is highlighted by the use of standard form "click-wrap" contracts.

Let us make a fairly extended example in the consumer context. Take a simple transaction such as an online purchase by a consumer of a book, CD, holiday or travel ticket. The following list sets out several different actions that could constitute a breach of regulation, market or social norms:

- The seller’s platform\(^3\) collects transmission related data ("traffic data": headers, clickstream data) that, if linked with personal data provided by the user, will start to create a user profile. Processing of such data may be restricted by data protection regulations.
- The seller’s website plants a cookie on the user’s equipment, allegedly for technical reasons. This cookie can send web-surfing (traffic) and other information back to the original website or to third party sites. The user is not informed of the reasons and processes of the cookie. The webpage

\(^3\) We use the word "platform" for online commerce applications: this is principally a seller's web-site, but it is more than that, as it can include non-website based computing elements, such as the back-office components, where many transaction related processes are carried out.
may also contain web-bugs that can also be used for monitoring user data and activities.

- The procedure for online contracting is not always clear though superficially obvious: "click here" to agree to a contract. In fact, consumers will probably find in the terms and conditions that the "I agree" or "I accept" button is only really an "I make an offer - and maybe the site will accept" button... in one jurisdiction (e.g. in the UK) while in another (e.g. Spain) sufficient description and clarity of terms may indicate that indeed the I Agree button is the final step for the conclusion of a contract.

- The seller's website collects personal data from the user (name, address, credit card numbers), over which the user has no further control. Most website privacy statements relating to the use of this data are insufficient for the purposes of informing the data subject and obtaining properly informed consent. In addition, the consumer has little guarantee that the collecting enterprise will respect its own policy - or that parties to whom it transfers such data will also do so.

- The ISP may use the personal data in many ways that breach both the data protection regulation and the ISP's own privacy declaration: this includes automatic processing and transfers and sales of data to third parties or through jurisdictions which provide little or no personal data protection.

- The website does not contain a clear statement of the Information Society Service Provider (ISSP), its contact details, VAT registration number, etc. in accordance with the EC Ecommerce Directive.

- The website does not contain sufficient description of products and services offered, either to comply with consumer protection requirements or generally to give the consumers the information they want or need (misleading, insufficient, etc.). In addition, prices may not be what they seem to be, especially for mistaken special offers and additional transaction costs (charges, transport, etc.)

- The user has to agree to unilateral (non-negotiated) contractual terms, that often include exemptions and restrictions that may be (a) invalid due to unfairness or (b) not acceptable to the user. Often such contractual terms are difficult to find and the user rarely reads them before entering into the online agreement.

- The transaction may not be recorded in such a way as to comply with legal requirements (e.g. set out in the EU Ecommerce Directive) or recommended information management procedures guaranteeing

---

4 Despite efforts of trustmarks and other web quality seals for online trading.

5 See for example, the problems of Argos when they advertised TVs at GBP 2.99, or Kodak commented in "Kodak snaps under customer pressure", ZDNet UK, 31.01.2002.
Chapter 1

integrity and authenticity sufficient to satisfy legal requirements for evidence presented in court.

- The participants in the transaction may not be who they say they are, raising a problem of identification and authentication (that may partially be solved by digital signatures, which have not been taken up by the public in any degree). While the consumer may wish to maintain his or her anonymity (admittedly not possible in the purchase of a flight, where the passenger must be named, but in clear opposition to real world store sales where cash transactions guarantee anonymity), the website itself may be a "spoof", i.e. it is not who it says it is but some third party representing to be the airline / travel site in question, permitting various forms of Identity theft.

- The website may use images or text whose use may breach intellectual property rights of the original right holder, by copying, distributing, etc. The user may download such materials (content) and also copy, distribute and publish the data.

- The website's owner or Internet Service Provider may wish to apply the laws of its jurisdiction to the sale and have recourse to the courts of its country, whereas throughout Europe at least and in many other jurisdictions, the local courts will be competent and will apply local mandatory laws if they are more favourable.

This example is not aimed to scare the reader, as many of these problems are well known and have certain easy forms of redress; however it illustrates our argument that many online transactions, while seemingly acceptable, can and indeed do infringe a variety of applicable laws and other commercial and social norms – the Glaucon's laws and mutual covenants cited above.

Several recent and not so recent cases provide real examples of the above (see Table 1.2).

Table 1-2. Online commerce risks

<table>
<thead>
<tr>
<th>Online Commerce risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cookie risks</strong></td>
</tr>
<tr>
<td>While cookies are small files planted in your computer allegedly to assist browsing, they can collect, store and transmit considerable amounts of personal and confidential data to controllers. Another risk involves capturing a copy of the victim's browser cookies file, and reading cookies containing passwords to access web-mail files.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Procedure for online contracting, incorporation of terms and error correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is still not clear whether a website will be construed as an advertisement (or invitation to treat, in English law) or a full offer, depending on the certainty of the terms and the jurisdiction and applicable law of the case. Mistakes in websites may bind ISSPs, debated (but not resolved as the case was settled) in the Argos case, when they advertised TVs at</td>
</tr>
</tbody>
</table>

---

1. Introduction

Online Commerce risks

GBP 2.99. Kodak also offered cameras a low cost, and agreed to provide the cameras at ridiculously low prices⁷. In Germany, the Hamburg Regional Court (3 U 168/00 - 13/06/02) held that sending contractual and conditions via e-mail to a buyer cannot replace the seller adequately positioning those conditions terms on the website. The court held that terms and conditions must be present on a trader's website in such a way so that they are clearly visible to a website user, who could not be expected to search the website for such terms⁸.

Collection and use of personal data

Amazon was to revise its privacy policy in response to concerns raised by customers, consumer groups and US regulators, clarifying the circumstances under which it might sell or share customer information. Under that policy, Amazon warned customers that it might transfer its personal data "in the unlikely event" that the company or its assets were acquired. Previously, the company said it would not "sell, trade or rent your personal information to others" and did not make an exception for the case of a transfer of business control. It is argued that this revision did not resolve the primary "inadequacies" of the policy: Amazon still holds the option of selling its customer database, refuses to give customers access to all the data it holds on them and refuses to delete their past purchase records.

In Spain, various Internet based companies have been forced to close due to the heavy fines - up to 300.000 Euros - levied by the Data Protection Agency, including for example Guia Empresas Internet SL for having sent advertising and publicity emails to individuals, and selling email addresses to third parties.

Unilateral (non-negotiated) contractual terms, incorporation and enforcement

In Bruce G. Forrest v. Verizon Communications In, a US court dismissed the action based on the a forum stipulation in the "click wrap" contract that required dismissal of claims in Virginia unless authorized by statute, upholding the online contract, while in Canada, in Kanitz v. Rogers Cable Inc the court found that website notices may result in the binding amendment of a services contract, if sufficient notice is given (e.g. clearly on the main page). The Court held that customers were obliged to check relevant portions of the website from time to time to determine if service agreement amendments had been made. On the other hand, other courts have denied the effect of web terms, as the consumer did not have to view and "click through" them to download them. In Comb v. PayPal Inc., a U.S. court decided that an arbitration clause was procedurally unconscionable because it was a contract of adhesion, imposed and drafted by a party of superior bargaining strength; it therefore could not be enforced. In Specht v. Netscape Communications Corp the court ruled that an arbitration clause was unenforceable because Netscape failed to notify and properly obtain the users' assent to the terms (a "browse-wrap", where the user has to browse the site in order to know the agreement exists). More recently, in DeJohn v. TV Corporation International the U.S. District Court upheld a click-wrap agreement as the terms were not so unconscionable, and contained in a link directly above the Accept button.

Consumer protection rules

In the UK, in April 2003 Victoria Wines was obliged to change its online terms and conditions, when an Office of Fair Trading investigation claimed that it breached Distance Selling Regulations (implementation of the DSD and EU Ecommerce Directive) on delivery and cancellation rights and attempted to limit its liability to consumers in unfair and

---

⁷ Commented in "Kodak snaps under customer pressure", ZDNet UK, 31.012002
Online Commerce risks

unlawful ways.

Website design: pop-ups and banners
America Online announced in October 2002 that it would stop accepting third-party pop-up ads on its internet service, following complaints from customers who find them an “annoying interference” with their on-line experience. Weight Watchers sued USA Prescriptions Inc. because pop-up ads for its diet drugs appeared on WeightWatchers.com if users have “ad-ware” (such as Save Now or Gator) loaded in their computers delivering adverts with the user’s consent. In the lawsuit, filed in a federal court in New York, Weight Watchers alleged trade mark infringement and dilution, and “systematically and unlawfully trade” on its brand, while compromising Weight Watchers reputation and deceiving consumers. In Germany, a Düsseldorf court has recently held that exit pop-ups constitute unfair competition and are equivalent to spam – unsolicited commercial communications – which would require users’ consent.

Identification
The FTC Report: “National and State Trends in ID theft, 2003” states that complaints of ID theft more than doubled to 85,820 in 2002 from 31,113 in 2000, accounting for 43% of total complaints made.

Jurisdiction and applicable law
While not specifically aimed at online commercial transactions, several cases illustrate the problem of determining the jurisdiction and applicable law to an Internet process or action. In LICRA v. Yahoo! Inc., the French court held that content online published by a US site, Yahoo!, infringed French anti-racism laws as it was displayable in France. In Gutnick v. Dow Jones, an Australian court asserted jurisdiction over a defamation dispute relating to content published on the US-based Dow Jones website.

Paradoxically, these cases may seem to contribute gradually - in a “Common Law” type of manner - to the creation of a body of law applied to activities carried out on the Internet. However tempting this may seem, this body is not mature, homogeneous or coherent. The scope of issues at stake - both technically, functionally and geographically – preclude the creation of a stable legal environment for the near future.

The rapidly evolving technology is one of the main factors of instability. IPv6 is a case in point⁹. This proposed protocol would identify (with an IP address) all devices connected to the network, including mainframes, PCs, WAP enabled mobile phones, intelligent objects (items with an RFID or other active electronic tag that could be connected, such as the vision of an intelligent refrigerator or home), and even persons wearing electronic chips. There would be no longer any need for dynamic IP addresses, as each item would be identified. This provides greater levels of certainty through potentially better identification. However, this technology is raising serious privacy issues, as personal objects would be identifiable by third parties, and individuals would lose a high degree of anonymity in relation to networked interactions. A consequence of this is that the speed of technological change

⁹ See the IPv6 website at http://www.ipv6tf.org/ and Table 1.3.
may prevent legal stability in this body of law relating to privacy, certainly in the short term.

Table 1-3. IPv6

<table>
<thead>
<tr>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>A new protocol for Internet addresses is being discussed – and gradually implemented –, to deal with the increased number of computers connected to the Internet: IPv6. This protocol will increase the number of bites from 4 to 16, with 6 of the 16 dedicated to a serial number of the Ethernet card on the computer or device, providing embedded digital identification of all devices connected to the net. Users will not be able to avoid this device identification (for all purposes: browsing, emails, SMS, chats, etc.), as with no number, there is no address and therefore no connection. Many new addresses are likely to be assigned to a new breed of internet-capable devices such as mobile phones, car navigation systems, home appliances, industrial equipment and other electronic instruments, some of them holding or revealing highly personal or sensitive information, such as location or device usage. This could enable the tracking of individual devices and thus potentially users, similar to a digital fingerprint. There have been initiatives to specify extensions to enhance privacy in IPv6 (RFC 3041, Privacy Extensions for Stateless Address Autoconfiguration in IPv6).</td>
</tr>
</tbody>
</table>

Another technology that may create a revolution in the way certain business are run – specifically logistics and supply chain management but potentially any business and the Internet itself – is Radio Frequency Identification (RFID). RFID tags are devices that may be added to certain goods or packaging (including transport pallets and cases) and provide a unique electronic identification (Electronic Product Code or EPC) of the item in question. These tags may transmit this identification (and other data, depending on the sophistication of the tag\(^{10}\)) to readers installed at certain points, for example at the entrance and exits of warehouses or motorways, on the retail floor or at supermarket check-out areas, or even on a shopping trolley. It has been said that these identification systems will create an “Internet of things”, as all tagged products may communicate with worldwide IT networks. This EPC network will allow computers to automatically recognise and identify any object, and then track, trace, monitor, and set off specific actions in relation to those objects. While potentially enabling a whole series of business innovations and efficiencies such as reducing shrinkage in supply chains, delivery tracking and customer personalisation, just like IPv6, RFID has set off a serious debate about the legality of emerging technologies, as it has the potential to be “privacy invasive” through tracking and tracing objects (and money\(^{11}\)) in individuals’

\(^{10}\) Tags come in different sizes of data and may be active or passive. Passive tags are smaller and may only be read, while active tags have an internal power supply (battery) and are usually “read/ write” – i.e. their data may be updated over time.

\(^{11}\) The European Central Bank is said to be still studying the possibility of integrating RFID tags in bank-notes. Yunko Yoshida: *Euro bank notes to embed RFID chips by 2005*, 2001 and Andreas Krisch: *RFIDs in Euro banknotes*, 2003.
possession. Again, we find a technology that has profound social and legal implications.

Other factors than technological change also contribute to legal uncertainty. The cross border nature of the Internet is a major element, as participants act and websites have effects in several jurisdictions. On the one hand different countries have varying approaches both to the level of legislation and regulation of the net (privacy being the prime example, though there may be some movements towards "equivalency", as the USA seems to be moving towards legislated rather than self-regulated privacy protection\(^{12}\)) and to the actual content of that regulation. Compliance with all jurisdictions is practically impossible (leading to the principle of regulation at origin embodied in the EU Ecommerce Directive – but hotly debated now in the ambit of VAT, as the EU tries to impose taxation at destination on non-EU sellers). Moreover, there are decisions from different jurisdictions leading to conflicting results, in a context where websites are accessible and transactions feasible in multiple jurisdictions. The Licra v. Yahoo! Inc. case commented above illustrates this: while the French court found that displaying and auctioning Nazi memorabilia violated France’s anti-racism laws, the US courts, having been asked to declare on the matter, held that this decision would not be enforceable in the USA as it would breach the principles of freedom of expression guaranteed by the US constitution.

In addition, legislation is being enacted that has much wider cross-border effects than before, questioning the traditional and established principles of conflict of law which determine which courts can hear a case, and which law is applicable (private international law). Examples include the European Data Protection Directive, which indirectly forces other countries to establish equivalent levels of data protection, if they want to trade electronically with the EU. Personal data originating in the EU may only be transmitted to third countries that provide adequate protection. Non EU companies wishing to do business in EU now have to establish a data centre in the EU that complies with local laws or set up at home procedures for data protection that comply sufficiently with the EU regulations (e.g. under the Safe Harbour Agreement\(^{13}\)). This has the effect of exporting EU levels of personal data protection to third countries. Another law with extra-territorial effect is the US Anti-cybersquatting Consumer Protection Act (ACPA), dealing with cases of domain name cybersquatting. The ACPA, by treating

\(^{12}\) For example, see list of bills in congress at <http://www.cdt.org/legislation/107th/privacy/> (visited 05/04/2003).

\(^{13}\) An agreement between the European Commission and the US Department of Commerce whereby US companies that agree to abide by the Safe Harbour international privacy principles, offer sufficient levels of privacy protection so that personal data could be transferred from the EU to them without further regulatory authorisation (e.g. from Member States). See US Department of Commerce: Safe Harbor Privacy Principles 21.7.2000.
dot-com, dot-net, and dot-org domain names as property that can be sued *in rem,*\(^\text{14}\) allows all such cases to be taken in Virginia, USA, where the root-server is, no matter where the domain name holder resides (e.g. in the Barcelona.com case\(^\text{15}\)).

This monograph does not aim to debate the cross-border nature of ecommerce and how to solve these problems through harmonisation or private conflict of law provisions, nor the politics of regulation and self-regulation. Our point is that while this *corpus juris* is being created, parties concerned may not (yet) count on it for the levels of consistency, legal certainty and protection that are afforded by national and international laws applied to offline transactions. Thankfully, this won't and hasn't stopped entrepreneurs setting up Internet oriented businesses and ecommerce websites, however the manager responsible for creating a web-based commerce platform, the developer in charge of designing and programming it and the lawyer hired to audit the legality of the site, its processes and the transactions carried by the platform find themselves confronted by a variety of laws, regulations, soft laws, codes of conduct and other "requirements" with which to conform... or not.

This uncertainty has led to serious fears about ecommerce, certainly on behalf of consumers, and possibly to a slowdown in the general progress of ecommerce – hidden, maybe by the bursting of the dot-com bubble and the current general economic slowdown. Major consumer concerns are raised by breaches of privacy and online fraud, and consumers tend to transact with sites in their own jurisdiction, feeling safer, perhaps correctly, in the belief that either that their own country laws will protect them more, or that redress - if needed - will be simpler or cheaper to obtain. Attempts have been made to facilitate cross-border dispute resolution for Internet related transactions, with a host of online dispute resolution services including BBB.Online, the Virtual Magistrate and others. In the EU through these are supported by the e-confidence initiative\(^\text{16}\), a common package of measures which include the promotion of high standards of good business practices (e.g. codes of conduct, trust marks, complaint settlement procedures), and easy and affordable access to third-party alternative dispute resolution (ADR) systems, in particular for settling disputes arising from the expected increase in cross-border transactions over the Internet.

\(^\text{14}\) In US law, an action *in rem* means that the plaintiff is taking proceedings against a "thing" as opposed to a "person" (in personam), which is the normal means of making a legal claim.

\(^\text{15}\) Barcelona.com Inc. v. Excelentíssimo Ayuntamiento de Barcelona – citations are in the reference section at the end of this work.

\(^\text{16}\) Online at http://econfidence.jrc.it and http://www.eejnet.org/ (a network of contact points or "Clearing Houses" which provides consumers with information on available ADR schemes).
The EC reports that Europeans are far behind Americans in usage of the Internet for B2C shopping, with only 4.7% of European Internauts regularly shopping online compared to 30% of Americans\textsuperscript{17}. The EU report “Trust barriers for B2B e-marketplaces” highlights the protection of confidentiality of sensitive data (59.4% of interviewees) and the security of information systems (57.8%) as the main barriers for the use of e-marketplaces, while other worries include a lack of clear information on the terms and conditions of contracts (such as applicable law and jurisdiction - 56.3%), lack of information on the different steps for the conclusion of a contract (42%) or about the identity of the companies (37%) and uncertainties related to the settlement of disputes and on-line payments (48-50%)\textsuperscript{18}. Nearly all these issues are legal issues, and may be solved by technical-legal procedures.

1.2 Ecommerce technologies and models are also illegal

1.2.1 Ecommerce technologies

We consider that most of these problems come from both technical and business processes of online commerce: on the one hand, the technological infrastructure of the Internet environment, and on the other the participants in the transaction, their capacities, attitudes and policies.

Apart from the Internet infrastructure technologies mentioned above that cause legal uncertainty – links, domain names, caches, – other aspects of digital technologies contribute to legal uncertainty. First and foremost, Digitisation is the root of most Intellectual Property Rights problems, through the capacity to create infinite perfect copies of digital works and distribute, modify or publish them throughout the world. This also includes the availability of digitisation technologies (scanners, video capture) to create digital copies of non digital works. Technology models (client-server computing and distributed systems) cause other legal concerns: it is often unclear where data transfers are made (e.g. from, to, in or through a certain jurisdiction?) nor who is responsible. There are a series of intermediaries (application service providers, Internet website hosts, etc.) who are technically involved in online transactions and are being targeted in Internet related cases for primary or contributory infringements. Internet languages, mainly HTML – a language that only understands formats but not contents – is also problematic, as machines cannot yet automatically understand that a


document is a contract, or a paragraph is a contract term. Protocols are also problematic, as they let Internet actors obtain hidden data from users (e.g. click stream data), in violation of the notification and consent obligations protecting personal privacy.

On a slightly less technical note, Internet related standardisation initiatives – W3C, IETF, etc – rarely take into account legal issues, while standard software development design methodologies don't take into account legal requirements unless users specify such a step.

Finally, and more generally, the law follows technology: hyperlinks, cookies and web-bugs, domain names, cache and mirroring, click-wrap contracts, click-stream data, pop-up ads, RFID tags, all predate regulation and rules. Regulators start applying “old law for new technologies”, then have catch up with technology and its multiple implementations through new legislation, and then cope with the delay between legislation and implementation – while technology moves on. The law also has to deal with technological and geographic variation and evolution of such non-compliant technologies or processes. One such attempt has been made in the EU, aiming to reach a level of abstraction to achieve technical neutrality, with the phrase "unsolicited commercial communications" for various forms of email, SMS or other “spam” (potentially, for example, banners and pop-ups).

There is also a reverse problem, that technology platforms need to meet moving legal standards: while version “1.0” may comply with the law on a certain date, further releases may be required to bring the application up to date within a changing legal framework. This may cause substantial interoperability issues over several platforms that may or may not be updated to the latest legal change. One of the key issues for future technology development will be how to manage and integrate “legal release control” into standard release management.

On top of the opportunities for abuse and the deficiencies of the technical infrastructure, the very models chosen for online commerce have not favoured compliance with the regulatory framework... when it existed.

1.2.2 Ecommerce Models

We argue that ecommerce has gone through two phases with two predominant commerce models: electronic data interchange (EDI), and electronic marketplaces (EM). EDI involves the electronic exchange of purchase orders and payments within a closed computer network, replacing the paper medium on which trade data were traditionally communicated by structured computer-to-computer transfer. Processes were structured by

19 This is being remedied by the semantic web efforts, whereby Internet content will be tagged for meaning and not just format. See www.semanticweb.org for more details on this, and our conclusions in Chapter 6.
trading partner agreements, which determined if not all, at least most aspects of data interchange and their legal validity between the parties. EMs establish an Internet based framework for connecting the many providers of a certain product with the many clients that want to purchase it. Products and prices may vary depending on each transaction, and often terms are dictated by either the seller website (seller-sponsored EM) or the EM’s general terms of business.

Online commerce is now proceeding through a third: transaction streams, which may be defined as electronic markets in which more than one player are involved in the transaction process. Transaction streams model how transactions on the Internet are actually being conducted – through a variety of intermediaries – and help explain the types of these new intermediaries that are appearing on the Internet.

Within these models, electronic commercial transactions are described as either hierarchical (within an established framework) or market-based (open participants, open parameters), and the appropriateness of one or other may depend on the products in question. In hierarchical transactions, most technical and legal matters are determined beforehand, e.g. within a project specification and a framework contract. This would be the example of EDI and most B2B platforms for EMs today. These are usually product- or sector-specific (Airlines, Chemicals, etc.) with close and even “closed” business relationships. Markets, and most B2C websites, on the other hand, are open to all comers. They will require extra mechanisms for “creating a context”, providing stability and trust through a variety of support services.

In the case of EDI, careful legal frameworks (including a UNCITRAL draft Model Law which became the Model Law on Ecommerce) have been set up to deal with legal issues, including provisions for contractual validity and electronic consent, evidence and dispute resolution. Open online trading and EMs, on the other hand, have signalled a breakdown in legal compliance, involving some of the infringements and problems mentioned above. The move from closed-circuit EDI (with overall process standardisation and management of documents and risks) to open EM has therefore led to the boom in legal issues raised by electronic transactions.

Several characteristics of the open web models such as EMs and transaction streams create legal problems:

---


1. Introduction

- Underlying attitudes to enterprise: under a “do first, then sort out the legal issues” attitude, electronic processes acquired standards and protocols (for presentation of data exchange, for contractual processes) that are not necessarily legal, even in more flexible regimes such as in the USA and less so in more protective continental jurisdictions.

- The speed of web platforms design: in most online commerce platforms, priority is given to business functionalities. Legally important considerations such as consumer protection, applicable laws, privacy controls are not generally considered, or are included post facto.

- A philosophy of personalisation or customisation: one of the main business advantages and indeed revenue streams of online commerce has been based on obtaining personal data from clients to provide improved personalised services and products. This has led to the unnecessary collection of too much personal data, low security standards (cutting costs, not incorporating security processes in the initial designs) and temptation to abuse the processing and transfer use of the data, for instance through reselling to other Internet participants (advertisers, other companies).

- The non interactive nature of web platforms: Despite claims for personalisation and interactivity, websites establish commercial transactions on standard legal terms: this doesn’t even involve the traditional “battle of the forms”. The description of interactivity is misleading in a legal context: there is no interaction regarding contracting process or data collection: accept our cookie or do not enter the site. Accept our standard terms or do not contract with us or participate in our B2B platform are typical policies.

- Low revenue streams: as online traders realise that ecommerce provides low revenue streams, the income from indirect sources such as sale of personal data becomes highly relevant. In addition, there is the financial instability and fragility of ecommerce companies, whereby when they fail their client databases are transferred to third parties, against the consent of the data subjects.

Transaction streams multiply these difficulties, as direct contractual relationships are clouded, and responsibilities and chains of liability are difficult to determine. Within these models, transaction processes are more complex, they involve more players and more data is being transferred. This raises the quantity and quality of legal issues at stake, as these are linked to the number of parties involved and the data transferred.