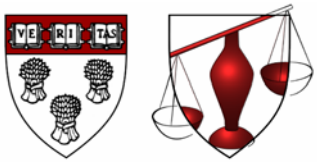

THE BERKMAN CENTER FOR INTERNET & SOCIETY

AT HARVARD LAW SCHOOL

Research Publication No. 2007-3

March 2007

E-Compliance: Towards A Roadmap for Effective Risk Management

Urs Gasser
Daniel M. Haeusermann

23 Everett Street • Second Floor • Cambridge, Massachusetts 02138
+1 617.495.7547 • +1 617.495.7641 (fax) • http://cyber.law.harvard.edu • cyber@law.harvard.edu

JEL Classification: K200, L860, M140, O320

E-COMPLIANCE: TOWARDS A ROADMAP FOR EFFECTIVE RISK MANAGEMENT

Urs Gasser*
Daniel M. Haeusermann**

*Translated by James M. Thurman****

ABSTRACT

In the past decade, the legal system has done a remarkable job in absorbing the shockwaves of digital technology. As a result, the use of information and communication technologies in corporate settings in general and E-Business solutions in particular have become business as usual not only for dot-com managers, but increasingly also for inhouse lawyers and outside counsel.

The authors of this article, however, argue that the widespread use of digital communication technology on the part of business organizations leads at least in part (and most likely also latently) to new types of challenges when it comes to the management of risks at the intersection of law, technology, and the marketplace. In order to effectively manage these challenges and associated risks in diverse areas such as security, privacy, consumer protection, IP, and content governance, the authors call for an integrated and comprehensive compliance concept in response to the structural and substantive peculiarities of the digital environment in which corporations - both in and outside the dot-com industry - operate today.

The article starts with a brief overview of what we might describe as a shift from traditional compliance to e-Compliance. It then maps the central themes of E-Compliance and the characteristics of a comprehensive E-Compliance strategy. After discussing the key challenges of E-Compliance, the article outlines practical guidelines for the management of E-Compliance activities and ends with recommendations.

Keywords: Compliance, Risk Management, E-Commerce, Soft Law, Records Management, IT and Law, Web2.0

---

* SJD (St. Gallen), LL.M. (Harv.), Attorney-at-Law, Associate Professor of Law, Director, Research Center for Information Law, University of St. Gallen, Faculty Fellow, Berkman Center for Internet & Society, Harvard Law School. E-mail: ugasser@cyber.law.harvard.edu.

** lic.iur., Research Assistant, Research Center for Information Law, University of St. Gallen, E-mail: Daniel.Haeusermann@unisg.ch.

*** J.D., Esq. Research Assistant, Research Center for Information Law, University of St. Gallen, E-mail: James.Thurman@unisg.ch. An extended version of this article will be published in German in: ARTER, OLIVER/JÖRG, FLORIAN S. (Eds.): Internet-Recht und Electronic Commerce Law, 9. Tagungsband, Bern 2007.

E-COMPLIANCE:
TOWARDS A ROADMAP FOR EFFECTIVE RISK MANAGEMENT

Urs Gasser
Daniel M. Haeusermann

Translated by James M. Thurman

Table of Contents

1. Introduction
2. From Compliance to E-Compliance
3. Central Themes of E-Compliance
   3.1. Overview
   3.2. Compliance Risk Areas
   3.3. Three Not-so-fictitious Case Scenarios
4. Characteristics of E-Compliance
   4.1. Overview
   4.2. Interconnection of Law and Technology
   4.3. Innovation and Dynamization of Law
   4.4. Internationalization of Legal Problems
   4.5. Growing Significance of Soft Law
5. The Challenge in E-Compliance: Risk Management
6. Practical Guidelines for the Management of E-Compliance Activities
   6.1. Master the Interplay of IT and Law
   6.2. Recognize Changes in Due Time
   6.3. Adopt a Global Perspective
   6.4. Strengthen Intraorganizational Cooperation
7. Conclusion
References

1. Introduction

As E-Commerce has continued to grow, dealing with the corresponding legal issues has become business as usual, though there have been prominent exceptions.[1] Indeed law appears to have absorbed the initial shockwaves of digital technologies, whether

[1] *E.g.*, *Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd. et al.* 125 S.Ct. 2764 (2005); *Copiepresse c. Google Inc.*, Tribunal de première instance de Bruxelles, 13 February 2007, N°. 06/10.928/C, available at http://www.copiepresse.be/copiepresse_google.pdf; *Rolex v. Ricardo*, OLG Köln (Germany), 18 March 2005, N°. 6 U 12/01, available at http://www.justiz.nrw.de/ses/nrwesearch.php.

through subsumption of new or not-so-new problems under old rules or through innovative efforts on the part of the legal system itself.[2] Observed systemically, rapid innovation in information and communication technologies and the emergence of e-Business models caught the legal system up in a remarkable process of adaptation. Certainly, the corresponding adjustment and feedback processes of the last ten years have not gone completely smoothly. Particularly, difficulties have emerged in those areas of corporate practice involving multiple aspects of compliance with the part newly created, part long-standing but newly interpreted ground rules of information law.

Under the heading "E-Compliance,"[3] this article examines the structural effects that the digitization of communication, or more precisely the use of digital communications media on the part of organizations,[4] has had for internal compliance. *E-Compliance* can thus be described as *the management of risks at the intersection of law, technology and the market that have emerged through and in reaction to the computerization and digital networking*.

2. From Compliance to E-Compliance

Compliance—a concept that initially stemmed from the U.S. banking world—generally indicates the observance of norms on the part of an organization. In the opinion of many scholars, including the authors of this article, compliance entails not only the observance of legislation, industry standards, statutes, directives, etc., but also ethical behavior on the part of the organization, that is, *corporate citizenship*.[5] Compliance also has a *managerial* dimension and in this sense represents the totality of all measures aimed at preventing the violation of rules on the part of the organization, its functional elements and its employees.[6]

---

2 For a discussion of the possible forms of reaction on the part of the law, *see* section 4.3 below.

3 In English-speaking countries, the term "e-compliance" is often used in connection with or as a designation for software which is utilized in compliance (in the conventional sense): *see*, *e.g.*, ROSSI, SANDRA: Insurers sign mega-dollar e-compliance deal, IDG Data, 11 December 2003 (available via factiva.com). Additionally, e-compliance may designate legal conformity of websites: *see*, *e.g*, PR NEWSWIRE: e-Compliance Concerns to be Addressed at the Market Conduct Exchange, 9 October 2001 (available via factiva.com).

4 Including digital communication within an organization, between organizations (Business-to-Business) and between organizations and private individuals (Business-to-Consumer).

5 *See* PAINE, 109 *et seq.*; LAUFER, 160 *et seq*.

6 In this context, the OECD Principles of Corporate Governance speak of "internal programmes and procedures to promote compliance with applicable laws, regulations and standards." OECD Principles of Corporate Governance (2004), available at http://www.oecd.org/dataoecd/32/18/31557724.pdf, 63. Note that this notion is broader than the notion of "compliance and ethics program" used in Chapter 8 (§8B2.1.) of the 2005 Federal Sentencing Guidelines (available at http://www.ussc.gov/2005guid/8b2_1.htm), which is defined as "a program designed to prevent and detect criminal conduct." (Application notes, section 1, *ibid*.)

Thematically the general understanding of compliance has changed in the last few years. Due to its origins in the banking sector, compliance has traditionally been focused on sector-specific areas of risk such as service and financial market surveillance, insider trading, money laundering and the like. With its extension to other industries—after all, customers and shareholders of every organization are interested in uncovering malfeasance—compliance has evolved from a segmented approach focused on specific legal areas or fields of activity to a comprehensive concept which today also includes the observance of anti-trust, anti-bribery, labor and environmental rules, to name just a few examples.[7] In the course of the dot-com boom of the late 90s, a new compliance risk area was added under the heading "electronic communication" which carries with it the structure of what we here call "e-Compliance."

3. Central Themes of E-Compliance

3.1. Overview

As stressed above, e-Compliance concerns an organization's handling of the changes in the legal system that have resulted from digitization. These changes can (and must) be analyzed from the perspective of positive law applicable to digital subject matter, which is traditionally accomplished through the identification of risk areas or the creation of a new compliance risk area that might be termed "electronic communication." At the same time, the changes in the legal system referenced above point toward certain structures that overlay these risk areas and partially obscure them from view. These structures have significant implications for the design of an internal (e-)compliance program.

Against this background, Section 3.2 sketches the most important compliance risk areas e-Compliance must deal with. Section 3.3 then formulates three case scenarios as links between the identified risk areas and the second part of this article, which systematically discusses the characteristics of e-Compliance (Section 4 and 5) and, from these characteristics, ultimately attempts to arrive at a few practical guidelines for the management of e-Compliance activities within a corporation (Section 6).

3.2. Compliance Risk Areas

Practical experience clearly indicates that e-Compliance is marked by *thematic diversity* and represents a pervasive task. In essence, five central areas of risk may be identified which usually lie within the purview of e-Compliance, albeit with different relevance for

---

[7] *See* OECD Principles of Corporate Governance (note 6), 63.

each individual organization—depending on sector, size of the organization, business model, etc. The majority of the identified areas below are not only relevant for dot-com businesses such as eBay, Google, or Microsoft but also for traditional companies since they also communicate via electronic channels both internally and externally.

- *Security*: The assurance of IT security is unquestionably at the core of e-Compliance. Security questions range from threats from viruses, worms, spyware and the like to hacking, or the theft of data or hardware such as laptops.[8] In order to protect information and secure information systems, multi-faceted technical, administrative and personnel-related measures are required and must be attuned to legal requirements as well as self-regulatory initiatives, such as industry "codes of practice", etc.

- *Data Privacy*: Closely related to the field of security is the observance of data privacy statutes in the processing of customer and employee data. Currently, many European mid to large-sized organizations must face crucial data privacy and employment law-related issues which stem from the use of the internet in the workplace generally and of e-mail in particular. Thus, the question arises, for instance, as to what extent and under what circumstances management can enforce and monitor internal company policies—particularly the prohibition of private e-mail usage.[9]

  Issues surrounding the protection of customer data recently made headlines in the United States—for instance in the context of personalized online advertising,[10] the release of search terms to criminal enforcement authorities[11] or to private parties,[12] and also in the context of social networking sites.[13]

---

[8] *See*, *e.g.*, BARR, STEPHEN, Sleepless Over Security Breaches, Washington Post, November 14, 2006, D04.

[9] More recently, instant messaging and blogging has gained media attention, *see*, *e.g.*, SHARMA, AMOL and VASCELLARO, JESSICA E., Those IMs Aren't As Private as You Think, The Wall Street Journal, 4 October 2006, D1, and KLEIN, JEFFREY S. and PAPPAS, NICHOLAS J., Employment Law; News; When Private Sectors Employer Fires Worker for Blogging, New York Law Journal, Vol. 237 (2007), 3.

[10] Google's e-mail service, Gmail, for instance, displays advertisements to the user based on the content of their opened messages. News of this practice was met with severe objections from data privacy advocates (BBC News, 5 April 2004, http://news.bbc.co.uk/2/hi/business/3602745.stm and 13 April 2004, http://news.bbc.co.uk/1/hi/business/3621169.stm). These concerns quickly quieted, however, once Google explained the functionality of the service and made assurances that it respected the privacy of its users (*See* Communiqué from Google, 15 June 2004, http://mail.google.com/mail/help/more.html).

[11] The most prominent case to date is *Gonzales v. Google*, in which the U.S. Department of Justice demanded from Google the production of a million URLs from their search index as well as numerous search terms which had been entered by users within a week. Ultimately, Google was forced to release 50,000 URLs, but not the search terms. *Gonzales v. Google Inc.*, 234 F.R.D. 674 (N.D.Cal., Mar 17, 2006) (No. CV06-8006MISCJW), available at http://www.google.com/press/images/ruling_20060317.pdf.

[12] In August 2006, AOL published 19 million search queries for research purposes. In some instances, this information allowed the identification of individual users (BBC News, 8 August 2006,

- *Consumer Protection:* Similar to privacy concerns, consumer protection represents yet another important subject for e-Compliance. Consumer protection law obviously plays a significant role in e-Commerce, for instance with regard to the viability of choice of law and forum selection clauses, or the formation, performance and termination of consumer contracts. Achieving compliance in cross-border dealings becomes particularly difficult in light of the prevailing heterogeneous body of consumer protection law.

- *Intellectual Property, especially Copyright Law*: For online businesses, the compliance field has traditionally been associated with intellectual property law and copyright law, in particular.[14] In accordance with the general trend toward a "participatory culture,"[15] models for online business are increasingly designed on the participation of users (Web 2.0). As a consequence, the risks of copyright infringement for online-intermediaries increase considerably,[16] and specifically for violations perpetrated by their own customers. This trend may be observed on both sides of the Atlantic.[17] Legal issues become particularly complex and even go beyond e-Compliance issues where large-scale digitization projects[18] and aggregation services[19] are concerned.

---

http://news.bbc.co.uk/1/hi/technology/5255732.stm). As a consequence, AOL's Chief Technology Officer had to resign (BBC News, 21 August 2006, http://news.bbc.co.uk/1/hi/business/5272974.stm).

13 Services such as MySpace find themselves confronted with the problem that minor-aged users may put themselves at risk through the publication of personal information—in particular since such information may and has attracted pedophiles (BBC News, 11 April 2006, http://news.bbc.co.uk/1/hi/technology/4898526.stm).

14 Generally, IP holdings (incl. patents) are an increasingly important domain of compliance, especially for multinational corporations. *see*, *e.g.*, MERKEL, KELLY, How To Stump A Corporate Lawyer: Means Of Effective Legal Risk Management For IP Counsel, Journal of Legal Technology Risk Management 1 (2006), 1-7.

15 *See generally* GASSER/ERNST.

16 The prime example is YouTube, where users may upload and publish short video clips. Anyone who sees his or her copyright infringed through a video on the service may (based on Section 512(c)(3) Digital Millennium Copyright Act, 17 U.S.C. § 512 (1998)) demand that YouTube delete the material (*see* http://www.youtube.com/t/dmca_policy).

17 See the examples in n. 18 & 19, below.

18 An example is Google Book Search (http://books.google.com): Google is currently digitizing 18 million books with the cooperation of five renowned U.S. university libraries. Works that are no longer copyright protected are available in full text while copyrighted books are searchable in full text but only short snippets surrounding the search term are displayed. Despite the fact that Google provides rightsholders with the opportunity to have their works removed from the database, the Authors' Guild and several large publishing houses have brought a lawsuit against Google. *See* LESSIG, Public Domain, 68 *et seq.*; *see also generally* PROSKINE; LUNDEEN.

19 For example, in the Belgian decisions relating to the *Copiepresse* case mentioned in n. 1 above: According to the court's latest decision from Feb. 13, 2006, the caching of articles and pictures from the online editions of Belgian newspapers as well as their publication as textual excerpts through the Google News service infringed the copyrights of the relevant media companies.

- *"Content Governance"*: The compliance departments of internet providers in particular face the challenge of complying with a plethora of national regulations that govern the online content which they themselves produce or host on behalf of their users and which is delivered worldwide. For instance, civil and criminal liability for third party content is largely unclear in Switzerland. Whereas certain categories of internet providers were initially shielded from liability in the U.S. and in Europe, the pendulum now appears to be swinging back in the other direction.[20] Ethical norms have also come to play an increasingly important role in this field, as demonstrated by the recent case of U.S. internet businesses which have begun offering services on the Chinese market.[21]

3.3. Three Not-so-fictitious Case Scenarios

The risk areas for E-Compliance identified in the previous section are merely formal categories. The following three examples which the authors take from their consulting experiences—with minor changes—may illustrate the managerial challenges associated with e-compliance. They demonstrate that real-life cases always combine several aspects of e-Compliance. Moreover, the examples will preface the exposition of common features of e-Compliance in the next Section.

(a) Doyouwatch.indie.channels.cc

A group of business administration and computer science students plans to form a company which will administer a website at "www.doyouwatch.indie.channels.cc." On this site, users will be able to upload and view video clips for free. They would like to cover the costs of maintaining the website and server space through advertising. In the event that the English language version should prove successful, the group plans to expand the service to include foreign language films.

A venture capitalist is ready to finance the project but first wants to have a detailed compliance plan which addresses the following questions among others: To what extent will the company be liable for copyright infringements on the part of users, for example, when they upload commercial music videos? What legal duties does the company have to eliminate the publication of illegal content—such as child pornography—and do these duties differ according to where the service is offered? Can the company be sued when a user uploads videos that impinge upon the privacy of another person? How does the company intend to react in the event that the videos of terrorist organizations appear on the website? How can the costs of ascertaining the authors of such content be

---

[20] *See* Section 4.3 below.

[21] See latter part of Section 4.4. *See also* GASSER, Search Engines, 146.

held in check? How can the Terms of Service and Privacy Policy of the service be made compliant with relevant consumer protection law?

(b) Brilliant Chemicals

Swiss multinational, Brilliant Chemicals Group, would like to harmonize and simplify its "Corporate Records & Information Management" program in order to structure its business operations more efficiently and to cut costs. Business records are not to be preserved for a longer period than is required by law and should be kept exclusively in electronic form. Management is also considering outsourcing the document management infrastructure to an IT provider operating in a low-income country.

In the ensuing internal consultations, the Legal & Compliance Department draws attention to the following: (1) The preservation of data in a single location is out of the question since many countries require that certain documents, particularly tax-related ones, be maintained domestically. (2) Each country in which Brilliant Chemicals operates has different statutory provisions concerning the scope of commercial preservation duties and the required level of information security. Additionally, regulations relating to the development and manufacturing of chemicals come into play, which often include decade-long preservation duties for related documents. (3) The legal status for the admission and probative value of electronically scanned documents as evidence is unsettled in many countries, and the risk of litigation is considerable if the company is no longer able to produce originals. (4) The desired enterprise content management system has to be able to bring a halt to the regular deletion of data whenever a litigation hold becomes necessary. Numerous information has to be quickly located and in complete form within the context of discovery proceedings. (5) Significant concerns regarding the adequate level of data protection in the low-income country call the viability of an outsourcing approach to records management into question. Further, it is unclear to what extent trade secrets would find protection under the laws of the respective country—both in terms of law on the books and law in action.

(c) Heidi Bank

Heidi Bank is an internationally-operating Swiss private bank for sophisticated private and institutional clients. Its core competences are Private and Investment Banking. Heidi Bank has subsidiaries in several EU member states as well as in the U.S. Currently, each legal entity has its own e-mail retention policy. The U.S. subsidiary, for instance, allows its employees to respond to client's requests via e-mail, monitors the e-mail traffic of its employees systematically, and retains all e-mails for ten years on magnetic tapes. In contrast, the Swiss parent company bans e-mail exchanges with clients entirely, leaves it to the discretion of its employees to archive important e-mail messages, and deletes all

other messages after 60 days. Heidi Bank's owner, Dr. Nötzli, is not pleased with the different ways in which e-mail is treated in different offices and asks the legal and compliance department to draft a global e-mail retention policy for Heidi Bank.

In an interim report e-mailed to Dr. Nötzli, the bank's General Counsel flags the following problems: The bank's U.S. back-up system does not allow for complete and consistent e-mail retention due to technical and organizational flaws. The anticipated costs to produce e-mails in the context of an e-discovery could easily reach into the six figures.[22] Not all of the Swiss company's employees have sufficient background in Swiss corporate law to enable them to make accurate decisions with regard to which e-mails are legally required to be preserved and which are not. In addition, the General Counsel points out the multi-faceted data protection issues that arise in the context of e-mail exchanges among the different companies located across Europe, especially regarding practices such as e-mail forwarding and the sending of blind copies (BCC:).

A whistleblower within Heidi Bank forwards the General Counsel's interim report to the Securities and Exchange Commission (SEC), which considers sanctions against Heidi Bank for not having an adequate e-mail retention policy in place.

4. Characteristics of E-Compliance

4.1. Overview

Against the background of the risk areas and examples outlined in Section 3, what are the most important *characteristics* of e-Compliance that distinguish it at least in part from traditional compliance?

In our view, the four characteristics are:

1. Law and digital technology are inseparably interconnected.
2. E-Compliance has to cope with and manage legal risks arising from the legal uncertainty created by the quicksilver environment of present and future IT law.
3. Digitization and the expansion of the internet have led to a more pronounced "internationalization" of both old and new legal issues.

---

[22] *Zubulake v. UBS Warburg LLC, et al.*, No. 02 Civ. 1243 (S.D.N.Y.). In this case, the presiding judge determined that even "inaccessible data", that is, data, which is no longer actively online but rather resides on back-up tapes, falls within the scope of discovery. Here, the defendant was obliged to cover the lion's share of the costs (ca. USD 450,000).

4. The dynamics of digitization and the associated legal uncertainty has increased the relevance of soft law.

We will now examine each of these characteristics in greater detail.

4.2. Interconnection of Law and Technology

Information and communication technology and law are closely interconnected in business practice.

First of all, the use of information and communication technology may be regarded as an *important compliance risk area* that touches on many different fields.[23] Thus, the problems and issues of e-Compliance stem specifically from the increasingly pervasive use of IT on part of business organizations. The concerns of the legal department of Heidi Bank surrounding the use and retention of e-mail reflect this development as do those of the venture capitalist considering the project doyouwatch.indie.channels.cc. Notably, this project has only become possible due to the technological developments of recent years—namely the deployment of broadband connections.

Information technology, however, also offers new approaches for the fulfillment of legal duties that are (initially) technology-independent. In this sense, IT also represents an *instrument* of e-Compliance, and software that supports and in part automates compliance tasks plays an important role in large and internationally operative organizations.[24] Particularly companies with extensive U.S. relations—as with Brilliant Chemicals in our example—are interested in software products which permit centralized and workflow-based information and records management and can, for example, suspend the automatic deletion of data in the event that a litigation hold becomes necessary.

Going beyond these highly complex, but structurally conventional software products, legal norms in certain areas are increasingly fashioned and expressed in accordance with formal logic to allow their ready implementation in software applications.[25] Such applications are available, for example, in the area of anti-money-laundering efforts or are currently being developed for the enforcement of copyrights.[26] LAWRENCE LESSIG'S famous phrase with reference to the architecture of cyberspace, "code is law",[27] must

---

[23] *See* Section 3.1 above.

[24] *See*, *e.g.*, AGUILAR KLEIN, MELISSA, Building Compliance Efforts With IT Roadmaps, Compliance Week, June 20, 2006.

[25] *See generally* GIBLIN ET AL.

[26] *See* DELANEY, KEVIN J., Copyright Tool Will Scan Web For Violations, The Wall Street Journal Online, December 18, 2006, available at http://tinyurl.com/sjmp61.

[27] LESSIG, Code, 6.

therefore be extended to include components of the *automated enforcement* of law through code.[28] These developments, however, are still in their beginnings and the reliability of such systems in individual cases remains to be seen.

E-Compliance is thus nearly as much a *technical* challenge as a legal one and will be even more so in the future.

4.3. Innovation and Dynamization of Law

The interconnection of IT and law outlined in the last section is also reflected on a systemic level. This fact becomes particularly apparent whenever a product or service that has been enabled by technological innovation is introduced on the market. Typically, technical innovations of interest to our subject go through a series of phases,[29] during which conflicts emerge due to the new technology's disruptive effects.[30] These conflicts play themselves out in the legal arena (courts, legislation) in addition to other fora. In this regard, three forms of reaction to disruptive innovation on the part of the law may be identified[31]: First the subsumtion of new phenomena under existing legal rules; second, the creation of new law (be it case-law or statutes); third, a latent disturbance of the existing structure of the law which often results in a need for legal reform in the long-run. All of these reactions contribute to the *dynamization of the law*.[32] The precise outcome of these forms of reaction can even be difficult for experts to predict—similar to the impact of disruptive innovation. In this manner, considerable legal uncertainty can emerge for business organizations. One famous example is the U.S. Supreme Court's *Grokster* decision of 2005,[33] which has unforeseeable consequences for a novel company such as doyouwatch.indie.channels.cc. Brilliant Chemicals' concerns regarding the probative value of electronic scans also testify to such legal uncertainty.

---

[28] For additional discussion on these issues, *see generally* GRIMMELMANN.

[29] A foundational piece with regard to the subject of ICT is SPAR, who distinguishes four phases: Innovation, Commercialization, Creative Anarchy and Regulation ("rules").

[30] On the theory of "disruptive technology", *see generally* CHRISTENSEN. Some "disruptive technologies"—and above all digital information technology in contrast to analogue—often lead to shifts in business models but in a few cases also to shifts in the legal order, where, for instance, they render existing legal institutions obsolete. That these shifts bring about legal innovation is probable but by no means automatic since it requires action on the part of actors within the justice system (courts, legislature, academia).

[31] GASSER, E-Commerce, 387-391.

[32] Illustrative is the emerging regulation of search engines. *See* GASSER, Search Engines, esp. 131-143.

[33] *Metro-Goldwyn-Mayer Studios Inc., et al. v. Grokster, Ltd. et al.*, 125 S.Ct. 2764 (2005). On the basis of the entire prior history, it was generally expected that the Supreme Court would further refine the *Sony-Betamax* doctrine regarding so-called "dual-use technologies" for digital networks. However, the court left precisely this question open and instead introduced a new doctrine into the realm of copyright which was derived from patent law. The result has created uncertainty for technology entrepreneurs. *See generally* GASSER/PALFREY.

Even in areas where the legislature has reacted relatively quickly to digitization and the expansion of the internet, a sense of legal uncertainty can nonetheless prevail—not only with regard to the application of new rules but also with regard to *future legal developments*. These may even run contrary to developments of the past. As mentioned above, laws were enacted only a couple of years ago that excluded online intermediaries from liability for the content of third parties in an effort to promote e-Commerce.[34] Since that time, however, a worldwide counter-trend has taken shape in which online intermediaries *are* held responsible for ensuring that their users comply with the law.[35] Thus, in order for online intermediaries to ensure their own compliance with the law, they increasingly need to ensure that their users are compliant with the law. The questions formulated in the example of doyouwatch.indie.channels.cc are thus very topical, and the start-up would be well advised to incorporate measures for the early recognition of future legal developments into its compliance plans.

To sum up, e-Compliance has to cope with and manage legal risks arising from the legal uncertainty created by the quicksilver environment of present and future IT law.

4.4. Internationalization of Legal Problems

Digitization and particularly the expansion of the internet superimposed a significant international dimension onto both old and new legal problems. The global reach of network computing almost completely detaches business contacts (such as B2B or B2C transactions) from the location of the physical (sales or service) infrastructure of a company. In sharp contrast to this, companies who engage in online business are linked to those foreign jurisdictions in which their business partners reside. As a consequence, the likelihood of being subject to a foreign jurisdiction with unfamiliar laws has drastically increased for these companies. Conflict of law issues in e-Business are only the tip of the iceberg. A much more challenging task is to achieve compliance with differing legal rules in a corporate environment whose IT infrastructure is gradually being centralized, and whose management aims to create uniform rules for information management (e.g. document retention policy) and electronic communication (e.g. e-mail policy).

From an IT perspective, the challenge of achieving compliance is further complicated wherever the regulatory models, approaches, and statutory frameworks not only diverge but are contradictory. A current example, which is of particular significance for the financial services industry today, concerns the procurement of electronic evidence in

---

[34] *See* PALFREY/ROGOYSKI, 20. Examples are Section 230 of the U.S. Communications Decency Act (47 U.S.C. § 230 (2003)) and Section 512 of the Digital Millennium Copyright Act (17 U.S.C. § 512 (1998)) as well as the limitation on liability for intermediaries in Art. 12-15 of the E-Commerce-Directive (2000/31/EG, 8 June 2000).

[35] PALFREY/ROGOYSKI, 20 *et seq.*

civil suits both in Europe as well as in the U.S.: The common view in the U.S. is that e-Discovery extends to all relevant electronic records over which a party (e.g., the U.S. subsidiary of a Swiss bank) has "control"—independent of the physical location of the server where data is stored.[36] According to the prevailing European view, this principle stands in direct opposition to the principles of mutual assistance in judicial matters.[37] Under certain circumstances the persons conducting discovery of documents stored in Switzerland may even be punishable for carrying out "prohibited acts for a foreign state" or for performing "economic intelligence service" (Articles 271 and 273 of the Swiss Penal Code).[38]

Additionally, the interconnection of the world through digital networks has given another push to *extraterritorial jurisdiction*: The relevant sections of the oft-cited Sarbanes-Oxley Act,[39] for instance, also apply to companies whose securities are secondarily listed on a U.S. stock exchange.[40] Inversely, U.S. jurisdiction in these cases extends to companies that are domiciled overseas and (primarily) listed on a foreign stock exchange, regardless of whether they have business operations in the United States. The E.U. Directive on the Protection of Personal Data[41] also has indirect extraterritorial application since the transfer of personal data to countries outside the E.U. that do not have an adequate level of protection is only permissible under very restricted conditions. (Art. 25 para. 1 and 26 para. 1). As a direct consequence of these rules, the U.S. Department of Commerce issued "Safe Harbor Privacy Principles", which were subsequently approved

---

[36] FRCP Rule 34(a) (2006) states that a party to litigation may be ordered to produce any materials subject to discovery (including "electronically stored information") which are in the "possession, custody or control" of that party. That custody over materials is key, irrespective of their physical location (even outside the United States) has long been accepted. *See Elder-Beerman Stores Corp. v. Federated Dept. Stores, Inc.*, 45 F.R.D. 515 (S.D.N.Y. 1968); *Gerling Int'l. Insur. Co. v. Comm'r of Internal Revenue*, 839 F.2d 131, 140 (3d Cir. 1988). The discovery of digital documents or records residing on a computer or other electronic media has been possible under the Federal Rules since at least the 1970 Amendments. *See, e.g., Emerick v. Fenick Industries, Inc.*, 539 F.2d 1379 (C.A. Fla. 1976). The recent 2006 Amendments have explicitly expanded the application of discovery obligations to "electronically stored information." *See* Report to the Judicial Conference Committee on Rules of Practice and Procedure, Appendix C (Sept. 2005), available at http://www. uscourts.gov/rules/Reports/ST09-2005.pdf. Thus, electronically stored information stored on foreign servers or other media located abroad may be subject to production.

[37] E.g. the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, available at http://www.hcch.net/index_en.php?act=conventions.text&cid=82.

[38] *See generally* GASSER/THURMAN (forthcoming). With regard to banking law, the authors also discuss the issues concerning e-discovery and Swiss Bank Secrecy (Art. 47 BankG). *See also* the information provided by the SWISS-AMERICAN CHAMBER OF COMMERCE, available at http://www.amcham.ch/switzerland/m_prohibited_procedural_details.htm.

[39] Pub. L. No. 107-204, 116 Stat. 745.

[40] See in particular Titles III, IV, VIII (Sec. 806), IX & XI of the Sarbanes-Oxley Act and relevant provisions of the Securities and Exchange Act 1934, 15 U.S.C. 78a *et seq*.

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

by the European Commission.[42] Thus, U.S. companies who wish to receive personal data from E.U.-based companies must comply with those Principles—effectively subjecting parts of their U.S. operations to E.U. data privacy law.

Yet, e-Compliance is not only required to align the use of a global medium to local laws but also in some instances must account for divergent *social norms*[43] as well as *ethical principles*—in the broad sense of "compliance" introduced at the beginning of this article.[44] This often neglected dimension of e-Compliance surfaced for instance when several U.S. internet businesses landed in the crossfire of criticism due to their operations in China and "compliance" with Chinese law.[45] Under a great deal of public pressure, hearings were held in Congress and a bill for a "Global Online Freedom Act" was introduced which aims to ensure that U.S. internet businesses operating in countries with repressive regimes do not violate U.S. legal and moral principles with regard to freedom of speech and the right to privacy.[46] The affected businesses are now working to keep their promise to develop a Code of Ethics and are supported in these efforts by a group of academic research centers.[47] In doing so, they hope, according to the opinions of observers, to preempt unfavorable legislation.

4.5. Growing Significance of Soft Law

Soft law, that is, non-legally binding norms such as international standards, codes of conduct, and best practice models, make up a substantial portion of the totality of norms which are to be observed in e-Compliance. Factors that arguably contributed to this development are the legal uncertainty associated with the dynamization of the law, the accentuated internationalization of legal problems concerning digital communication as well as the highly technical character of legal materials. Soft law concerns the most var-

---

[42] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, C(2000) 2441.

[43] Even between Europe and the United States different mentalities prevail, as for example with regard to attitudes towards "political correctness".

[44] *See* Section 2 *above*.

[45] *See, e.g.*, THOMPSON, CLIVE: Google's China Problem (and China's Google Problem), The New York Times, April 23, 2006, available at http://www.nytimes.com/2006/04/23/magazine/23google.html?ei=5090&en=97200276105636 3f&ex=1303444800.

[46] *See* Global Online Freedom Act of 2006, H.R. 4780, available at http://www.govtrack.us/congress/billtext.xpd?bill=h109-4780. The bill has been reintroduced in 2007 as H.R. 275, available at http://www.govtrack.us/congress/billtext.xpd?bill=h110-275.

[47] Among them is the Research Center for Information Law at the University of St. Gallen (FIR-HSG, http://www.fir.unisg.ch), with which the authors of this article are affiliated. *See* PALFREY, JOHN G., Testimony to the U.S. House of Representatives Committee on International Relations, February 15, 2006, available at http://blogs.law.harvard.edu/palfrey/testimony-to-the-us-house-of-representatives-committee-on-international-relations/.

ied subjects and all levels of electronic communication, including the physical and logical infrastructure as well as the content layer. The following examples may illustrate the diverse range of soft law instruments relevant to our subject:

- *IT Security:* standards such as BS 7799/ISO 17799 and CobiT, as well as the OECD Guidelines for the Security of Information Systems and Networks[48] and the OECD Guidelines for Cryptography Policy;[49]
- *Data Privacy:* the "Web Privacy Seal" certification offered by TRUSTe[50] as well as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data;[51]
- *Voluntary Content Regulation:* the Codes of Conduct provided by industry organizations representing access providers, hosting service providers, and search engines in Germany, France, and the United Kingdom;[52]
- *Records Management:* ISO standard 15489-1 and its implementations, such as the Swiss standards and guidelines eCH-0026 and eCH-0038.[53]

The relevancy of these heterogeneous normative sources varies according to business models, the geographic area of operations, products and services, etc. of each organization. However, even from these few examples, it is clear that soft law not only plays a role for companies of the dot-com sector: whereas the codes of conduct for internet intermediaries and data privacy norms are of central importance for doyouwatch.indie.channels.cc,[54] the "old economy" company Brilliant Chemicals will be interested in records management and IT security standards in addition to data privacy norms.

5. The Challenge in E-Compliance: Risk Management

E-Compliance particularly concerns the observance of legal and non-legal norms. As with traditional compliance, the following *additional functions* also come into consideration: the active monitoring of legal, regulatory, technical and market-related develop-

---

48 Available at http://www.oecd.org/dataoecd/16/22/15582260.pdf.

49 Available at http://www.oecd.org/document/11/0,2340,en_2649_34255_1814731_1_1_1_1,00.html.

50 *See* WEBER, Regulatory Models, 167-169.

51 Available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

52 UK: Internet Watch Foundation (http://www.iwf.org.uk); Germany: Verein Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V. (http://www.fsm.de); France: Association des Fournisseurs d'Accès et de Services Internet (http://www.afa-france.com). On the benefits and drawbacks of such approaches, see WEBER, Regulatory Models, 195-202.

53 All available at http://www.ech.ch.

54 *See* n. 52 above.

ments; support of management in issuing internal guidelines and instructions (e.g. e-mail policy); participation in the development of industry standards and best practice rules; education of employees; preparation of suggestions for organizational measures; provision of legal advice in the event of concrete inquiries, etc.

With regard to e-Compliance, the common denominator in the fulfillment of these responsibilities consists of the *management of risks at the intersection of law, technology, and the market*. This focus on risk management is not new: due to many different factors, compliance today is generally understood to be an element of risk management.[55] Among the drivers of this development are the minimum capital requirements proposed by the Basel Committee on Banking Supervision (Basel II), which also contemplate operational risks—particularly legal risks.[56] By nature, Basel II is directed at banks, but the accord also influences the loan policies of banks insofar as they have to assign lower credit ratings to companies that have not developed sufficient measures for the management of operational risks.[57] Furthermore, it has generally become accepted that legal problems and even legal violations within a company can never be completely avoided, but are rather part of the general risk of doing business. Hence the opinion has emerged that the rational handling of such risks is part of good corporate governance.[58]

What does a rational handling of risks mean exactly? The first step in risk management involves the identification of relevant risks and (where possible) their quantitative evaluation.[59] For this reason, conditions under which risks may emerge must be analyzed and their probability as well as damage potential evaluated. As a result, measures aimed at minimizing risk may be outlined, prioritized, and subsequently implemented.[60]

If compliance issues are (at least partly) regarded as legal risks and one attempts to handle them applying the methods of risk management, two important practical issues emerge: First, in terms of personnel: To identify and evaluate legal risks, a great deal of theoretical and practical legal knowledge is required, which calls for the involvement of (in-house or outside) counsel. However, too often legal personnel lack the necessary tools, particularly quantitative methodology.[61] In addition, the acceptance of risks is for-

---

55 *See*, *e.g.*, MARTIN/MANLEY, 12.

56 *See generally* CHORAFAS, 49 *et seq.* What sort of legal risks the Basel II Accord actually covers is disputed. One key issue in this context is the possibility of quantifying legal risks.

57 *See* BARTELS, 48.

58 *See*, as to risk management in general, DREW/KENDRICK.

59 *See*, *e.g.*, the Inventory of Risk Management/Risk Assessment Methods and Tools by the European Network and Information Security Agency ENISA at http://www.enisa.europa.eu/rmra/rm_process_02.html.

60 *See*, for example, the risk management framework proposed by WEBER, Risk Management, 472.

61 This is particularly a problem in Europe, as legal education starts at the undergraduate level, which normally precludes students from gaining skills in quantitative methodology before going to law school.

eign to lawyerly thinking, which is aimed at eliminating risks and can lead to risk aversion. This mind-set can in turn manifest itself as a lack of acceptance of risk management approaches. The second issue concerns information, or more specifically quantitative data that are indispensable for a reliable risk assessment[62]: Court cases that represent a certain type of compliance risk are rare and generally poorly comparable with one another.

These general difficulties in handling risks are accentuated by a few *particularities* of the subject matter of e-Compliance. One is the rapid pace of technological change mentioned in Section 4.3 which leads to a dynamization of the law and in particular to less foreseeability of future legal developments. For this reason, it becomes more difficult, if not impossible, to quantify legal risks: Whereas companies have a wealth of experience upon which to base their risk assessments within "traditional" compliance risk areas,[63] such precedents are lacking with regard to the sort of risks that are the subject of e-Compliance.[64] These particularities are to be taken into account on the organizational level, as will be argued in the following Section.

6. Practical Guidelines for the Management of E-Compliance Activities

As a matter of course, management must adapt the responsibilities and tasks as well as the organizational structure of the company to the changing conditions of the contemporary business environment. This is no less true with regard to the paradigmatic shift from a paper-based to a digitally networked ecosystem of corporate information. The following considerations may offer some guidelines on this subject.

---

62 *See*, *e.g.*, CHORAFAS, 37: "all types of analytical treatment of quantification are 80% data problem and only 20% mathematical problem."

63 Within the financial industry, for instance, available data may be sufficient for a reliable quantification of legal risks that arise, say, from bad advice on the part of an account manager vis-à-vis a client, or from the faulty design of financial products. The same applies to risks connected with high government regulation, for example in the financial, pharmaceutical or commercial aviation sectors.

64 Example 1: Before paper documents are scanned and destroyed, one has to evaluate, among other risks, those of evidentiary loss in a future lawsuit (for example because the authenticity of a particular signature cannot be proven). Not only is there no precedent here, but it is extremely difficult to predict how a court will react, not least because it depends on the attitude of the individual judge toward new technologies (*see* GASSER/HÄUSERMANN, 311).

Example 2: If and to what extent online intermediaries expose themselves to liability for copyright infringements on the part of their users is not even certain in the U.S., where there is a relatively rich body of case-law dealing with digital copyright. (*see* PALFREY, JOHN G., Making a Market Emerge out of Digital Copyright Uncertainty, available at http://blogs.law.harvard.edu/palfrey/2006/10/11/).

6.1. Master the Interplay of IT and Law

As has been established above, e-Compliance is just as much a technical endeavor as a legal one.[65] Successful e-Compliance therefore presupposes a great deal of interdisciplinary knowledge between IT and law. Accordingly, close and formalized cooperation between the compliance and IT departments is imperative for good corporate governance.[66] The communication between IT-personnel and lawyers is not always easy in light of the differing mind-sets and working styles; but it is nonetheless unavoidable for the identification and evaluation of risks at the intersection of law and technology.[67]

6.2. Recognize Changes in Due Time

As has been developed above, e-Compliance is characterized to a large extent by technological progress, which in turn creates the need for constant adjustment on the part of the legal system.[68] As a result, the legal environment for information technology evolves in a similar—and very dynamic—manner to technology itself. Corporations that fail to identify legal developments early enough may well risk the invalidation of their entire business model, as for example the *Grokster* case demonstrates.[69] Therefore, it can be imperative for an organization's survival to continually and systematically investigate signals within the political and legal system that herald potential, business-relevant change.[70] This can be done, for instance, through the formation of an interdisciplinary[71] think tank or through close cooperation with existing institutions. Such an early warn-

---

65 *See* the latter part of Section 4.2 above.

66 Additionally, the separation between legal services and the compliance department should be reconsidered, unless the legal department is exclusively responsible for handling litigation. Yet, even in this scenario, continuous contact between Legal and Compliance is unavoidable so that the latter may be supplied with relevant material for risk assessment.

67 *See* Section 5 above.

68 *See* Section 4.3 above.

69 *See* n. 33 above.

70 The doctrine of Technological Early Recognition (for a terminological discussion *see* HOLTMANNSPÖTTER/ZWECK, 68), which stems from the field of strategic management, offers useful insights for the legal field: Academic literature defines Technological Early Recognition as "the systematic observance and recognition of new technologies…which often announce themselves in the form of 'weak signals'" (trans.). Thus, it does not concern forecasts but rather "entrepreneurial looking-ahead", that is, the early identification of opportunities. In practice, Technological Early Recognition is primarily carried out on the corporate level as part of strategic Research and Development management. The organizational options are diverse; for instance, technological early recognition can be handled by an independent unit which is connected through an internal network of up to a hundred scouts or informants of all hierarchical levels. It is not unusual for these networks to also include research institutes, professional associations, standardization committees and the like. For more on this subject, *see* REGER, 304 *et seq*.

71 This proposition is derived directly from the St. Gallen approach to information law, that is, the evaluation of informational phenomena through a lens composed of the intersection of law, technology, business, and politics. *See* GASSER, Information Law, 12 *et seq.*; BURKERT, 76 *et seq*.

ing system is imperative for dot-com businesses. Still, the anticipation of legal developments can be of strategic importance for traditional sectors such as finance as well.

6.3. Adopt a Global Perspective

Due to the international character of the subject of e-Compliance,[72] it is essential that the personnel who deal with issues of e-Compliance adopt a global perspective. Thus, for instance, it is not enough for a global company to have a compliance department in each one of its local subsidiaries if the local compliance officers are not enabled and encouraged to exchange information and to discuss issues with their peers from other countries and the group headquarters. In this sense—as with traditional compliance—well-founded knowledge of the law of relevant jurisdictions must be developed since this action is a prerequisite for identifying and actively managing potential conflict zones which arise from the tension between global infrastructure and local law.[73] The required global perspective, however, also includes the construction of "soft" knowledge since culture-specific social norms must likewise be considered.[74] For these reasons, management must ensure that information flows continuously among the often geographically separated compliance departments of a large corporation. In practice, such knowledge will be supplied by the involvement of external consultants or the formation of advisory boards.

6.4. Strengthen Intraorganizational Cooperation

As we have seen above, increased company-wide collaboration is key in the field of e-Compliance.[75] On the one hand, collaboration is required in the sense of building "communities of knowledge" in order to handle appropriately the highly complex problems in the field of e-Compliance—which are in part industry-specific,[76] in part intersectoral,[77] but almost never company-specific. On the other hand, perhaps even more im-

---

[72] *See* Section 4.4 above.

[73] *See* first paragraph of Section 4.4 above.

[74] *See* accompanying text to n. 43 above.

[75] *See* Section 6.3 above.

[76] New sector-specific problems emerge where sector-specific legislation pertaining to digital subject-matter is applicable. For example, Swiss bank client confidentiality (Article 47 of the Federal Law on Banks and Savings Banks) also applies to e-mail communications, which are particularly susceptible to breaches of confidence: a U.S. court order compelling discovery can refer to e-mails or other electronic information that is stored in Switzerland and—according to Swiss law—subject to bank client confidentiality.
Generally, one might assume that most new legal issues will crop up within highly regulated industries (e.g. financial services, pharmaceuticals). After all, the existence of a regulatory agency in these sectors increases the likelihood that problems and legal uncertainties of that kind are tackled rather quickly and resolved competently.

[77] Some important examples are the preservation of electronic data, international data privacy, or consumer protection in e-commerce.

portantly, the increased significance of (mostly industry-driven) soft law[78] demands the increased readiness of industry players to participate in the composition of that soft law. In this respect, not only collaboration between companies is essential, but also the development of new forms of public-private partnership.[79]

In addition to these forms of institutional collaboration, also the *informal exchange of experiences* across corporate boundaries must not be neglected: For the very reason that e-Compliance issues are afflicted with new and considerable legal uncertainty, every single case represents a "reality check" with regard to existing measures whose viability can generally only be assessed on the basis of theoretical considerations at the time of adoption.

7. Conclusion

Through significant efforts, the legal system has adjusted to the changes in the information and communications technology of daily corporate life—changes at the intersection of the market, technology, and law. Organizations must make adjustments on their part as well in order to deal with the consequences resulting from these changes in the legal system. The observation that led to this essay was that these adjustments represent a greater challenge than the already decreasing entropy surrounding concepts such as "e-commerce law" or "cyberlaw" would suggest. Our initial foray into the concept, characteristics, responsibilities and organizational guiding principles of e-Compliance confirms this observation.

E-Compliance, as discussed in this article, is confronted with the phenomenon of a close interconnection between law and technology, a prominent dynamization of the law, massive internationalization of issues and legal problems, as well as a strong increase in the significance of soft law. These characteristics, which in part may also apply to traditional areas of compliance such as financial market regulation, call in their interplay for the further development of compliance concepts as well as adaptation of the affected aspects of corporate organization. Due to the increasing amalgamation of corporate organizational nexus and ICT, the symbiotic relations between traditional compliance and e-Compliance will be increasingly amplified. The view that e-Compliance represents merely a single risk area among the many of compliance is therefore outdated in our opinion. E-Compliance is actually a multidimensional and multidisciplinary task, although there are certainly areas of law that are particularly affected by digitization (or

---

[78] *See* Section 4.5 above.

[79] *See*, *e.g.* WEBER, Risk Management, 476, on the subject of risk management concerning IT infrastructure.

also which particularly impact digitization)[80] and therefore are of particular importance for the field of e-Compliance.

Thus, in conclusion, the authors do not posit a special "e-Sphere" within or without existing compliance departments. Rather, we argue for an *integrated and comprehensive compliance concept* that appropriately makes allowance for the structural and substantive peculiarities of e-Compliance as outlined in this essay and stays abreast with the pace of digitization.

[80] *See* Section 3.2 above.

References

BARTELS, JOACHIM C.: Basel II and the Survival of the SME: Are Lenders and Borrowers Ready to Comply with Basel II?, Business Credit, Nov/Dec 2002, Vol. 104 Issue 10, 48.

BURKERT, HERBERT: The Information Law Approach: An Exemplification, in: Gasser, Urs (Ed.), Information Quality Regulation: Foundations, Perspectives, and Applications, Baden-Baden 2004, 75-90.

CHORAFAS, DIMITRIS N.: Operational Risk Control with Basel II, Oxford et al. 2004.

CHRISTENSEN, CLAYTON M.: The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Boston 2003.

DREW, STEPHEN A.W./KENDRICK, TERRY: Risk management: The five pillars of corporate governance, Journal of General Management, Vol. 31 No. 2 Winter 2005, 19.

GASSER, URS (E-Commerce): E-Commerce: Innovation im (Vertrags-)Recht?, Schweizerische Juristen-Zeitung (SJZ) 2001, 386-391.

GASSER, URS (Information Law): What is Information Law – and what could it be?, in: Gasser, Urs (Hrs./Ed.), Informationsrecht in „e"-Umgebungen – Information Law in eEnvironments, Baden-Baden 2004, 7-24.

GASSER, URS (Search Engines): Regulation of Search Engines: Taking Stock and Looking Ahead, 9 Yale Journal of Law & Technology 124 (2006).

GASSER, URS/ERNST, SILKE: From Shakespeare to DJ Danger Mouse: A Quick Look at Copyright and User Creativity in the Digital Age, Berkman Center Research Publication No. 2006-05, available at http://ssrn.com/abstract=909223.

GASSER, URS/HÄUSERMANN, DANIEL MARKUS: Beweisrechtliche Hindernisse bei der Digitalisierung von Unternehmensinformationen, Aktuelle Juristische Praxis (AJP) 2006, 305-316.

GASSER, URS/PALFREY, JOHN G.: Catch-as-Catch-Can: A Case Note On Grokster, available at http://ssrn.com/abstract=869030.

GASSER, URS/THURMAN, JAMES M.: E-Discovery: Wichtige Neuerungen im amerikanischen Prozessrecht (forthcoming).

GIBLIN, CHRISTOPHER/LIU, ALICE Y./MÜLLER, SAMUEL/PFITZMANN, BIRGIT/ZHOU, XIN: Regulations Expressed As Logical Models (REALM), in: Moens, M.-F./Spyns, P. (eds.), Proceedings of the 18th Annual Conference on Legal Knowledge and Information Systems (JURIX 2005), Amsterdam 2005, 37-48, available at http://www.zurich.ibm.com/security/publications/2005/GiLiMuPfZh05aREALM-JURIX.pdf.

GRIMMELMANN, JAMES: Regulation by Software, 114 Yale Law Journal 1719 (2005)

HOLTMANNSPÖTTER, DIRK/ZWECK, AXEL: Monitoring of Technology Forecasting Activities, ESTO Project Report, March 2001, available at http://esto.jrc.es/docs/forecasting.pdf.

LAUFER, WILLIAM S.: Integrity, Diligence, and the Limits of Good Corporate Citizenship, 34 American Business Law Journal 157 (1996).

LESSIG, LAWRENCE (Code): Code and Other Laws of Cyberspace, New York 1999.

LESSIG, LAWRENCE (Public Domain): Re-Crafting a Public Domain, 18 Yale Journal of Law and the Humanities 56 (2006).

LUNDEEN, KYLE: Searching for a Defense: The Google Library Litigation and the Fair Use Doctrine, 75 University of Missouri–Kansas City Law Review 265 (2006).

MARTIN, DAVID/MANLEY, MARK R.: Linking, compliance, risk management, Pensions & Investments, 9/4/2006, Vol. 34 Issue 18, 12.

PALFREY, JOHN G., JR./ROGOYSKI, ROBERT: The Move to the Middle: The Enduring Threat of "Harmful" Speech to Network Neutrality, Berkman Center Research Publication No. 2006-08, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916748.

PAINE, LYNN SHARP: Managing for Organizational Integrity, 1994 Harvard Business Review, Mar-Apr 1994, 106.

PROSKINE, EMILY ANNE: Google's Technicolor Dreamcoat: A Copyright Analysis of the Google Book Search Library Project, 21 Berkeley Technology Law Journal 213 (2006).

REGER, GUIDO: Technologie-Früherkennung: Organisation und Prozess, in: GASSMANN, OLIVER/KOBE, CARMEN, Management von Innovation und Risiko, Berlin et al. 2006.

SPAR, DEBORA L.: Ruling the Waves, From the Compass to the Internet, a History of Business and Politics along the Technological Frontier, New York et al. 2001.

WEBER, ROLF H. (Regulatory Models): Regulatory Models for the Online World, Zurich et al. 2002.

WEBER, ROLF H. (Risk Management): Legal Framework for Risk Management in Information Infrastructures, in: KIERKEGAARD, SYLVIA MERCADO (Ed.), Business, Law & Technology: Present and Emerging Trends, Volume 1, Copenhagen 2006, 470-481.