Unit IV

Ethics and public policy :

Introduction

Such a topic immediately raises at least three questions. First, what is ethics? Second, what is public policy? And third, how, and in what ways, are ethics and public policy connected? All three questions have, unsurprisingly, generated large literatures.

Put simply, ethics is about what we ought to do or ought not to do. That is, it is concerned with what is good and bad, right and wrong, just and unjust, or noble and ignoble, and how we can tell the difference. There are many different and often competing ethical frameworks, theories, and principles, and there is certainly no complete agreement about the ethical standards and behaviour that should apply in specific contexts. However, it is generally accepted that the domain of ethics embraces not merely the discrete actions of individuals but also the actions of groups of individuals – whether these groups are small, such as families, or large, such as nations and the international community. Hence, ethical inquiry – or what is often called moral philosophy – is not confined to the private sphere of life; it is equally relevant to the public realm, including the decisions of those who act on behalf of the public, whether at the national or sub-national level.

Public policy has been defined in many ways, but a relatively uncontroversial approach is to suggest that it is about what governments choose to do and or not to do. Hence, public policy is concerned primarily with governmental action and inaction. This of course includes both empirical and normative questions. At the empirical level, there are the issues of what governments do in practice and how this varies over time and between jurisdictions. At the normative level, key issues include what governments ought to do and ought not to do, and what principles should guide decision making. From this perspective, then, ethics lies at the heart of public policy and is relevant, as Michael Mintrom argues persuasively in this volume, to all aspects of the policy-making cycle – including the tasks of defining the problem, identifying and assessing the available options, decision making, implementation, evaluation and – where justified – termination.

This of course does not mean that public policy is solely about ethics. Many aspects of policy analysis lack an ethical dimension. For instance, whether a particular country has a policy on nuclear weapons, climate change, refugees, or agricultural subsidies is an empirical matter, for which there is usually a straightforward factual answer. But whether it should have a policy on such matters and, if so, what this policy ought to be, are fundamentally ethical questions. They thus require careful ethical analysis if they are to be answered in a rigorous and justifiable manner.

Just as not all aspects of public policy have an ethical dimension, not all values are ethical values. Mathematical values, for instance, are different in nature and purpose to ethical values. At the same time, we need to be alert: particular statistics or metrics, such as gross

domestic product or the consumer price index, often embody or reflect certain ethical assumptions and values, or may be used to justify a certain policy stance, which in turn reflects a particular ethical purpose. Equally, as is widely recognised, the market price of a good or service may not equate to its 'true' worth to society – perhaps because the price fails to take into account the positive and negative externalities associated with the production of the good or service in question. But of course the question of how we should determine the 'true' worth of something raises many profound ethical issues.

We discuss the relevance of ethics to public policy and explore the various ways in which ethical inquiry is relevant to policy analysis and governmental decision making. We also briefly examine some of the ethical challenges that face public policy practitioners – whether policy analysts, senior advisers, or decision makers – including the problem of conflicting moral imperatives.

We then focus on one of the great moral challenges of the 21st century, namely how the global community should address the problem of human-induced climate change. The policy issues here are many and varied, and the ethical dilemmas facing humanity are complex and profoundly difficult. For instance, what responsibilities do those living today have to future generations and other species? What constitutes a 'dangerous', or alternatively 'safe', amount of climate change? What kind and magnitude of risks are ethically acceptable? How should the burdens of mitigation and adaptation be shared across the international community? And what discount rate should be applied to analyses of the costs and benefits of actions to address climate change?

Ethical foundations of public policy

Let us return, then, to the relationship between ethics and public policy: in what ways is ethics relevant to policy makers and those who advise them? There are at least two issues that are central to policy analysis and that are fundamentally ethical in nature. First, what is policy for? Or, to put it differently, what ends should governments strive to achieve? Second, what are the appropriate means or policy instruments for achieving these ends? Bear in mind that ends and means are closely interrelated: some ends, for instance, are simultaneously the means for achieving other purposes.

With respect to the purpose of public policy, any answer necessarily entails ethical values. The problem, however, is to determine which particular values should be pursued and what the end should be. On this matter moral and political philosophers have offered many different answers over the centuries. One common approach has been to say that public policy should be directed towards the goal of building the good society, or at least a better one than we currently experience.

A key issue for many of these approaches is that they beg the question of what is 'good', 'valuable', or 'just'. What, for instance, constitutes a 'good' or 'just' society? What kinds of 'values' – pleasure, happiness, well-being – should be maximised? But setting aside the issue of providing a theory of the good, justice, or value, a related issue is what constitutes a good policy. From the perspective of moral philosophy, there are two broad approaches to answering this question. The first, which is a consequentialist approach, is to assess the goodness or otherwise of a policy solely on the basis of its consequences. But the consequences of a policy are often difficult to discern or may not be fully evident for many

years or even decades. Moreover, the consequences may include both positive and negative impacts, and the weighing up of these is often highly controversial. Hence, judging the worth of a policy solely on the basis of its consequences is fraught with problems.

The Treasury's wellbeing framework has five dimensions:

- centrally, the level of freedom and opportunity that people enjoy;
- second, the aggregate level of consumption possibilities;
- third, the distribution of consumption possibilities;
- fourth, the level of risk that people are required to bear; and
- fifth, the level of complexity that people are required to deal with.

Treasury's perspective on freedom and opportunity has been heavily influenced by the work of Amartya Sen on the contribution that 'substantive freedoms' make to development.

According to Amartya Sen, the true measure of human development is the capabilities that an individual has to choose a life they have reason to value. … Capabilities allow an individual to fully function in society. They are not income and, while they include basic civil rights and political freedoms, they are not limited to 'rights'.

For public policy makers, many of the significant challenges are not simply theoretical or ethical. Any real solution to the problem of climate change, in addition to being just, needs to be effective, practical, and politically achievable. For example, the problem of justifying why we should prioritise climate change over other pressing aims, such as the recent global financial crisis, presents a significant political challenge for public policy makers and officials. Large parts of the population continue to raise the issue of empirical uncertainty, so continue to be sceptical about the science of climate change and whether we can be certain about its causes and effects. Although these doubts are not surprising – especially given the impact that policies such as emissions trading schemes and emissions taxes are likely to have on large parts of the population – they are irrational. On any reasonable cost–benefit analysis of the problem, the magnitude of the harmful consequences of climate change and the risks of the impacts far outweigh any concerns about empirical uncertainty.

The far more daunting challenge facing public policy makers arises from the interdisciplinary nature of the problem. Beyond the purely ethical complexities described earlier, any effective solution obviously needs to rely on a scientific analysis to identify the causes and effects of climate change as well as effective strategies for mitigation and adaptation. At the same time, public policy makers need an economic analysis of the costs and benefits of potential strategies and policies. The issues that arise from analysing the problem from each of these perspectives are, of course, enormously complex.

The interdisciplinary nature of the problem of climate change does not arise merely from the fact it requires analyses from many different perspectives – scientific, economic, ethical, and political. As Reisinger and Larsen discuss, many of the key concepts at the heart of the debate on climate change are inherently interdisciplinary. 'Key vulnerabilities', 'dangerous climate change', and 'acceptable risks', for example, can be defined only on the basis of both scientific and ethical analyses. Likewise, determining the appropriate discount rate – a key concept in any cost–benefit analysis that reflects the value of goods and service in the future compared with today – can be informed only by both economic and ethical analyses. Of course, drawing on different disciplinary perspectives is not without its challenges, but, as highlighted in this volume, it can enrich our understanding and deepen our appreciation

of the complexity and gravity of the issues at stake. Arguably, the problem of climate change illustrates this better than any other contemporary ethical or policy dilemma.

Perspectives on ethics and the economy

The final part looks at issues related to 'economics', in particular the relationship between ethical behaviour and the functioning of markets, the question of how far markets should be regulated, the moral dilemma of 'freeloading' in systems that allocate welfare benefits unconditionally, and the challenges posed by rising economic inequality. Forming a backdrop to this section is the global financial crisis that first shook the world in 2008, and three of the chapters engage directly with that crisis. Many commentators viewed this crisis as a consequence of highly unethical behaviour on the part of people in the financial and banking industry, prompting calls for a radical re-examination of the way markets operate and a fresh look at issues such as accountability, regulation, and control. These calls directly and indirectly inform the contributions to this part.

It is tempting to conclude that the global economic downturn offered a stark illustration of what can happen when ethics gets uncoupled from economics, when markets are allowed to operate in a totally 'unfettered' way. In the ever more brutal 'dog eat dog' world of contemporary capitalism what matters most is securing global brand recognition, improving shareholder returns, and discovering ever more imaginative ways of 'making money from money'. The voices seeking to highlight the human consequences of economic activity, or calling for moral restraint in the interests of 'the common good', seem like ever fainter cries in a more and more inhospitable wilderness.

Privacy Protection in Electronic Commer

Introduction

The potential of electronic commerce has attracted the attention of many business and consumers. However, online shopping has not been adopted as quickly as expected. Internet users are concerned about the privacy of information they supply to Web sites , and this is one factor that has been holding them back from open acceptance of the electronic marketplace. Many people believe privacy protection in the United States is inadequate. A recent Harris Poll shows that 84% of Americans are concerned about threats to personal privacy, and 78% believe consumers have lost control over how their personal information is used . Researchers at the Wharton School of Business claim that privacy and security concerns are actually driving people away from the Internet . The cost of privacy violation to potential economic growth is rising in America. What was once seen as a threat to civil society is now a clear and present danger to the economic health of the country. Unless privacy is adequately protected, the revolutionary potential of the Internet may not be realized .

Information privacy is the "claim of individuals, groups, or institutions to determine for themselves when, and to what extent, information about them is communicated to others".

Privacy protection should prevent non-permitted, illegal, and/or unethical use of private information. It is important to note that the right of privacy is not absolute. Privacy must be balanced against the needs of society. Criminals may use privacy protection to cover their crimes. The public's right to know surmounts the individual's right of privacy.

Security and privacy are often related to each other but they are not the same. In the computer security community there is still much confusion between privacy and security concepts. Privacy requires security, because without the ability to control access and distribution of information privacy cannot be protected. But security is not privacy. Information is secure if the *owner* of information can control that information. Information is private if the *subject* of information can control that information. Anonymous information has no subject, and thus ensures that information is private. Anonymity requires security and guarantees privacy, but is neither .

The complexity of manually collecting, sorting, filing, and accessing information from several different agencies was, in many cases, a built-in protection against the misuse of private information. However, in the Internet and Web environment, information about users can be easily collected, integrated and analyzed from different sources through the use of network, database, data warehouse and data mining technologies. The potential of privacy violation therefore becomes much higher. Technologies such as firewalls, public key encryption, secure sockets layer have been used to improve security, but they may not necessarily protect consumers' privacy.

Privacy protection is a very complex issue. It is not simply a technical, but mostly an

economical, social, and legal issue, that involves multiple parties often with conflicting interests. From one side, businesses want to use information technology to identify, collect, and even trade customers' personal and preference information in order to make

Protecting Intellectual Property

You may not realize it, but you deal with intellectual property (IP) every day. If you own a website, that website is your intellectual property. The way you deal with IP — yours and others — can directly impact the success of your business.

What's Intellectual Property?

"Intellectual property can be broken down into four types: patents, trademarks, copyrights and trade secrets."

- A patent deals with a completely new invention – a useful item, a novel look on an already-existing item or a new plant species. Depending on the type, patents are good for between 14 and 20 years. The scope of a patent is defined by its claims. Each claim is only one sentence but the claims of a patent may go on for pages, which is why it's best to hire an experienced patent attorney.
- A trademark designates an object's source; it's a mark or name associated with quality. In trademark law, arbitrary names are encouraged (i. e. Kodak, Kleenex, Apple). The less your trademark describes your product, the stronger it is. Conversely, if you sell film, using "Film" as a trademark won't hold up in court.

Again, there are common-law trademarks but they're hard to prove and offer less protection than a state or federal trademark.

- Copyrights protect creative expression – websites, songs. There is such a thing as common-law copyright, which means that when you create something, you automatically have certain rights. The difficulty lies in proving you were first to create it.

For only $30 you can register with the U.S. Copyright Office. The forms aren't complicated, and once they've been filed you have a lot more protection in an infringement suit. The copyright is good for your lifetime and 70 years after you die, and you can make it assignable to anyone upon your death.

Copyrights don't protect the information found in a book or on a website, but they protect the layout and presentation. For websites, registering your first and last 25 pages of code protects the code for your entire website and the creative expression of your display screens.

- Trade secrets are governed by state laws and vary from state to state. They encompass a variety of things from formulas (think Coca-Cola) to customer lists to product sources. Many companies have contracts that expressly prohibit their employees and vendors from giving away any information they're exposed to while doing business with them. Commonly known facts aren't considered trade secrets so it's good to be discreet with your valuable information.

Internet Censorship

Introduction

.

The lack of similar laws in comparable countries is not due to a failure of Parliaments or Governments to consider the problems of illegal content or content unsuitable for minors on the Internet.

The remainder of this document contains an overview of governmental approaches to dealing with Internet content that is illegal, or is unsuitable for minors, followed by sections containing more detailed information about various countries.

Overview

Since approximately 1995, numerous governments around the world have been addressing the problems of material on the Internet that is illegal under their offline laws, and also that considered harmful or otherwise unsuitable for minors. The nature of material of principal concern has varied substantially. For example: political speech; promotion of or incitement to racial hatred; pornographic material. Few governments have attempted to ban or otherwise legislatively restrict access to "matter unsuitable for minors" as distinct from material illegal to distribute to adults.

As at March 2002, government policies concerning censorship of the Internet may be broadly grouped into four categories:

a) Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies.

> This approach is taken in the United Kingdom, Canada, and a considerable number of Western European countries. It also appears to be the current approach in New Zealand where applicability of offline classification/censorship laws to content on the Internet seems less than clear.
>
> In these countries laws of general application apply to illegal Internet content such as child pornography and incitement to racial hatred.
>
> Content "unsuitable for minors" is not illegal to make available on the Internet, nor must access to same be controlled by a restricted access system. Some (perhaps all) such governments encourage the voluntary use of, and ongoing development of, technologies

that enable Internet users to control their own, and their children's, access to content on the Internet.

b) Criminal law penalties (fines or jail terms) applicable to content providers who make content "unsuitable for minors" available online.

This approach is taken in some Australian State jurisdictions and has been attempted in the USA (although no such US Federal law is presently enforceable, and to the best of EFA's knowledge nor is any such US State law).

In these countries, in addition, laws of general application apply to content that is illegal for reasons other than its unsuitability for children, such as child pornography.

c) Government mandated blocking of access to content deemed unsuitable for adults.

This approach is taken in Australian Commonwealth law (although it has not been enforced in this manner to date) and also in, for example, China, Saudi Arabia, Singapore, the United Arab Emirates and Vietnam. Some countries require Internet access providers to block material while others only allow restricted access to the Internet through a government controlled access point.

d) Government prohibition of public access to the Internet.

A number of countries either prohibit general public access to the Internet, or require Internet users to be registered/licensed by a government authority before permitting them restricted access as in (c) above. Information on countries in this category is available in the Reporters Without Borders/Reporters Sans Frontiers report Enemies of the Internet of February 2001.

In the many countries that have Internet censorship laws far more restrictive than those existing or proposed in Australia, governmental focus appears to be on prohibiting and/or restricting politically sensitive speech, criticism of the government, etc. These governments do not appear to have any focus on prohibiting or restricting content deemed unsuitable for minors as distinct from content deemed unsuitable for adults.

Internet Indecency

While indecent materials constitute a small percent on the World Wide Web, they have received much attention because they are easy to search out or stumble upon. Although the First Amendment, in general, protects pornography, the Supreme Court has held that it does not protect two types of pornography: obscenity and child pornography. Consequently, the government may, and has, banned them.

Even before the advent of the internet, the Supreme Court ruled on obscenity. In 1973, the Supreme Court defined obscene pornography as that which depicts or describes patently offensive ‘hard core’ sexual conduct. The case which this came from was Miller v. California,

which also created the Miller Test, a three part test to decide whether something was obscene or had artistic value.

However, as the Internet grew more complex and vast, more regulations were needed to regulate the available obscene material. In the late 1990s, several pieces of legislation were passed in order to control obscenity on the web including the Communications Decency Act, Child Online Protection Act, and the Children's Internet Protection Act.

This topic has stirred much discussion as many doubt the feasibility of policing the internet in its entirety. Others scrutinize the government's intrusion into the public sphere as many times regulations may skirt the line between protecting national interest and invading into the private sector of our citizenship.

Taxation of e-commerce

Introduction to taxation of e-commerce

E-commerce presents a major challenge for tax administrations, given the often multi-jurisdictional nature of the transactions and the potential anonymity of the parties.

Can withholding tax be imposed on e-commerce payments?

Introduction

Where transactions involve the supply of digitised goods over the internet there are issues concerning the characterisation of the income generated– i.e. are these business profits or royalties? The provision of digitised goods such as software or music which can be downloaded would, under traditional rules, generally be the provision of a right to use a product, and in most jurisdictions would give rise to royalties. However, if the same goods were provided in non-digitised form (i.e. sold in a physical form such as a CD-ROM), there would be a supply of goods giving rise to profits.

VAT and e-commerce

Introduction

Where goods or services are supplied by a UK business to a customer whether the business is obliged to account for VAT in the UK, elsewhere, or at all, will depend upon whether the supply is of goods or services, where the supply is treated as made and whether the customer is in an EU member state. The implications of e-commerce for VAT purposes can be examined in the context of three types of transaction:

- Supplies of physical goods to business or private consumers;
- Supplies of intangible goods or services to business;

- Supplies of intangible goods or services to private consumers.

It should be noted that significant changes to the VAT treatment of cross border supplies of services came into effect from 1 January 2010. However these changes did not change the place of supply of electronically supplied services.

Supply of physical goods to business or private consumers

The basic position is that in general supplies of physical goods are deemed to be made in the place where the goods are located when they are dispatched. Where the goods are merely ordered using electronic communications, this will not affect the way in which they are treated for VAT purposes. The location of goods and therefore their place of supply for VAT purposes will not be altered by internet ordering.

As VAT legislation was originally drafted in the context of goods physically being supplied, there is generally little difficulty in applying the existing regime to this type of transaction. Note however that digitised products are treated as a supply of services and not goods.

The VAT treatment of a supply of goods to a customer within the EU will depend upon whether the customer is a VAT registered business or not. If goods are sent from the UK to a VAT registered business in another member state they can be zero-rated by the UK supplier provided certain conditions are complied with, which include obtaining the customer's VAT registration number.

Supply of electronic services to business customers

Supplies of digitised products are treated as supplies of services rather than goods. Since 1 January 2010, the basic rule for supplies of services where the customer is registered for VAT is that services are deemed to be supplied where the **customer** belongs. Individuals receiving supplies in a personal capacity are treated as belonging where they have their usual place of residence and businesses are treated as belonging where they have a business or fixed establishment which has the benefit of the service.

Further guidance on these rules can be found on the HMRC website. Electronically supplied services include the following:

- website supply, web hosting and distance maintenance of programmes and equipment; the supply of software and the updating of software;
- the supply of images, text and information, and the making available of databases;
- the supply of music, films and games (including games of chance and gambling games);
- the supply of political, cultural, artistic, sporting, scientific, educational or entertainment broadcasts (including broadcasts of events);
- the supply of distance teaching;
- online auction services; and
- internet service packages.

For further guidance on what is covered, see the HMRC website.

Security and the Basics of Encryption in E-Commerce

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption.

Encryption is a generic term that refers to the act of encoding data, in this context so that those data can be securely transmitted via the Internet. As Professor Lawrence Lessig of Stanford Law School put it, "Here is something that will sound very extreme but is at most, I think, a slight exaggeration: encryption technologies are the most important technological breakthrough in the last one thousand years." Encryption can protect the data at the simplest level by preventing other people from reading the data. In the event that someone intercepts a data transmission and manages to deceive any user identification scheme, the data that they see appears to be gibberish without a way to decode it. Encryption technologies can help in other ways as well, by establishing the identity of users (or abusers); control the unauthorized transmission or forwarding of data; verify the integrity of the data (i.e., that it has not been altered in any way); and ensure that users take responsibility for data that they have transmitted. Encryption can therefore be used either to keep communications secret (defensively) or to identify people involved in communications (offensively).

The basic means of encrypting data involves a symmetric cryptosystem. The same key is used to encrypt and to decrypt data. Think about a regular, garden-variety code, which has only one key: two kids in a tree-house, pretending to be spies, might tell one another that their messages will be encoded according to a scheme where each number, from one to 26, refers to a letter of the alphabet (so that 1 = A, 2 = B, 3 = C, etc.). The key refers to the scheme that helps match up the encoded information with the real message. Or perhaps the kids got a little more sophisticated, and used a computer to generate a random match-up of the 26 letters with 26 numbers (so that 6 = A, 13 = B, 2 = C, etc.). These codes might work for a while, managing to confuse a nosy younger brother who wants to know what the notes they are passing mean, but the codes are fairly easy to crack. Much more complex codes, generated by algorithms, can be broken by powerful computers when only one key exists.

Public Key Encryption, or asymmetric encryption, is much more important than symmetric encryption for the purposes of e-commerce. The big improvement wrought by Public Key Encryption was the introduction of the second key - which makes a world of difference in terms of protecting the integrity of data. Public Key Encryption relies on two keys, one of which is public and one of which is private. If you have one key, you cannot infer the other key.

Here's how it works: I have a public key, and I give that key (really, information about how to encode the message) out to anyone with whom I wish to communicate. You take my

public key and use it to encode a message. You send that message, in coded form, over the network. Anyone else who sees the message cannot read it, because they have only the public key. The message only makes sense when it gets to me, as I have the only copy of the private key, which does the decoding magic, to turn the zeros and ones (bits of information) into readable text.

The most common use of PKE for e-commerce involves the use of so-called Digital Certificates issued by "trusted" third parties. Here's how this one works. Say you are a customer of Big Safe Bank and you would like to communicate with your bank. If you sent the bank some information (for instance, "please wire the contents of my savings account to a new account in Switzerland"), you might worry that the information could get intercepted en route but you might also worry that the bank would not know it was you who sent the information. You and Big Safe Bank agree to use a trusted third party to help you communicate in an encrypted manner to one another over the Internet. The bank contracts with VeriSign or another provider of a Digital Certificates. When you send a message to the bank, you send your message about wiring funds encrypted twice: once with your own private key, and once with the bank's public key, along with a certificate, encrypted using the institution's private key. Once the bank gets your message, they use the institution's private key to decrypt the certificate, which in turn gives the bank your public key. The key in the certificate can decrypt the message you sent to such an extent that all the bank then needs is its own key to read the message. After all those keys have worked their magic instantaneously, the bank can be certain of two things: that you were the one who sent the message and that the message was not read along the way. And you know that the only one who could have read the message was the bank. The funds get transferred, as requested - probably using another encrypted data transmission.

Public Key Encryption ostensibly creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs - information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.

Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could "carry" certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of e-commerce.

There are non-technical limitations to PKI. It is said that it simply shifts the security risk to the certificate authorities. They wonder who will certify the certifier and how safe their key data will be in these hands. Some governments have demanded access to such key repositories in the interest of national security.

Other interesting issues worth pursuing for further information related to encryption include:

- secure sockets layer (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols;
- the effectiveness - and occasion flaws - in easily-accessible (freeware) security technologies such as PGP;

- other uses of encryption, such as the closely-related notions of digital signatures (very broadly defined), access controls, and watermarks;
- the technical means by which keys use hash tables to achieve the encryption and decryption process;
- regulation of Ceritificate Authorities (CAs), Registration Authorities that validate users as having been issued certificates and the directories that store certificates, public keys and certificate management information;
- policies that identify how an institution manages certificates for its own personnel, including legal liabilities and limitations, standards on contents of certificates, and actual user practices;
- the history of codes, from ancient times through the second World War to present day, including the recent controversy over whether encryption methods of a certain force should be treated as "armaments" illegal for export by the United States government and the debate over the so-called "Clipper Chip."

Legal Issues of Electronic Commerce

In its recent Communication on Electronic Commerce, the European Commission stressed that "in order to allow for electronic commerce operators to reap the full benefits of the Single Market, it is essential to avoid regulatory inconsistencies and to ensure a coherent legal and regulatory framework for electronic commerce". The types of pitfalls that are facing any company or person wanting to set up a distance selling activity on the Internet, offering goods or services to consumers and businesses located world wide are numerous, they vary according to the type of relation you are considering entering (consumer, business), and according to the legal framework you are accustomed to operating in. To make things even more difficult, the answers are often unclear, non existent, contradictory and constitute real obstacles to conducting a commercial activity on the network.

The legal framework we are operating in is increasingly becoming complex and burdensome in one single jurisdiction alone, let alone when you are faced simultaneously with hundreds of potentially applicable legislations because you are entering agreements with customers located anywhere in the world. Besides, a number of companies and consumers are still unaware of the legal constraints they may encounter by entering electronic transactions. The objective of this present draft is to fill this gap by providing an overview of relevant legal issues raised by the development of electronic commerce.

Taxation Law

- What criteria may be used to associate on line transactions with the territory of a country?
- How can double taxation be prevented?
- How do the direct taxes rules apply in an electronic environment, both for businesses and for individuals?
- Do general taxation, VAT and custom duties regimes apply to electronic transactions?
- What is the nature of supplies on the Internet? Are the products delivered electronically goods or services?

- How can digital documents comply with existing administrative requirements to keep written evidence of commercial operation and registration in accountancy?
- How can the place and the time of the supply be determined?
- Are electronic transactions exports or imports pursuant the European VAT directives?

Electronic Payments

- What are the existing advantages and obstacles to introducing technical systems that enable electronic payments in an electronic transaction?
- Are banking regulations applicable to issuers of cybercash and cyber credit cards? Does such electronic cash constitute legal tender?
- How can credit cards and other electronic payments satisfy the legal requirements in electronic environments?
- How can privacy, consumer protection and bank secrecy be fulfilled in an electronic banking relationship?
- What is the situation concerning the use of electronic negotiable documents?

Contract Law and Evidence

- Which are the nature , parties and subject matter of the contracts?
- How to enter contracts electronically?
- What is the value of an electronic document and a digital signature?
- Where and when does the offer take place?
- What are the terms and conditions governing the contract?

Liability

- What type of liability could the various actors (service provider, access provider, TTP, seller, banking institution,) involved in the offering of goods or services face?
- What type of damages are covered?
- What are the causes of liability?

Intellectual Property Rights

- How to protect a web site, a domain name, a trade mark or any other type of intellectual property right against illegal misappropriation?
- How to control the use of protected material on the global infrastructure?
- Which rights are concerned when downloading, viewing or printing a protected work? Is there a exhaustion of rights?
- How can the rightholder expect to obtain remuneration?
- How can his moral rights be ensured?
- How should licence agreements be drafted?
- What is the legal protection of the integrity of ECMS?
- Is it possible to detect illegal use?
- Who can be considered as liable in case of copyright or trade mark infringement?

Consumer Protection

- What general or specific rules must be respected when entering a contract with a consumer or when advertising a product?
- What is the regulation of offers and marketing practices?
- What are the abusive terms of a contract?
- What type of information has to be included in a web site?
- How are the distance selling contracts regulated?
- What is the regulation of product and services liability and of products labelling and packaging?
- How can consumers have easy access to jurisdiction and which are the possibilities for consumer associations to defend consumers interests?

Privacy Issues

- What are the applicable general and specific legislations?
- Can personal data be transferred?
- What are the technical developments currently undertaken to improve the protection of privacy on the Internet? How do they comply with privacy provisions?

International Private Law

- What are the competent jurisdictions and the applicable law in the following matters: Contracts, Liability, Intellectual property Rights, Marketing and competition law, electronic payments and banking issues
- What are the specific mandatory criteria in the context of consumer protection?
- How can a jurisdictional decision be enforced in another country?
- Is on-line litigation and arbitration in commercial cases relevant?