7

Government and the Environment of Certainty and Trust

Mancur Olsen, the Nobel prize-winning economist, addressed the legal foundations for market development in his last book, published after his death (Olsen 2000). He noted that when legal foundations are lacking, economic transactions tend to be anchored in spot markets in time or geography. To encourage economic transactions to take place beyond spot markets, to where time or space separates the transaction, requires a promise that after one half of the transaction is complete, the other half will occur in the future or at some other place. As discussed in the context of the economics of the Internet marketplace, an essential force for value creation comes from exploiting such markets in time and space. Olsen's remarkable insights support the critical importance of legal foundations for electronic commerce—without ever mentioning the Internet!

Fostering this environment of certainty and trust requires governments to both intervene and forbear. On the one hand, government must put into place the framework: the codification of rules, enforcement, and consistent application. On the other hand, government need not intervene to determine what technological solutions might best fill the legal frame. It is not the job of the law, but of technology, for example, to derive the means to ensure the validity of electronic signatures, although case law may tell which technological solution best achieves the legal objective.

But is the legal framework sufficient to create the certainty and trust needed to encourage the growth of electronic commerce? Or is government intervention necessary to ensure that users will indeed use the Internet and gain its benefits? And under what jurisdiction do laws and regulations operate? Electronic commerce is global; legal jurisdictions, unless agreed to multilaterally, are local or national.

Legal Framework

In order for electronic commerce to flourish, a commercial legal framework needs to be in place to recognize, facilitate, and enforce electronic transactions worldwide. Most laws and policies governing the physical world apply generally to the Internet, even if they were written before the advent of electronic commerce, though some modification may be necessary. Countries anxious to promote electronic commerce may be tempted to write laws and regulations specific to electronic commerce. Instead, general commercial law, including contract rights and intellectual property protection is needed to promote development; it can then be adapted if necessary to accommodate electronic commerce.

National and international efforts to date have been directed at building the legal and technical infrastructure—the validity of contracts, protection of intellectual property, and standards and protocols—to ensure the interoperability of the Internet. Recognizing the global reach of the Internet and of electronic commerce implies an international approach, since contracts will not be enforceable if only one country recognizes the legal validity of an electronically signed contract. Similarly, intellectual property will not be adequately protected if only a handful of countries provide copyright, patent, and trademark protections; computers will be unable to communicate unless there are standardized interfaces connecting networks that permit interoperable applications.

One approach that promotes international coordination is drafting model laws and uniform rules, conventions and treaties, and technical standards and protocols. To the extent that countries adopt similar legal and technical bases—either through government agreement or private sector acclamation—potential conflicts are minimized. Governments can use these tools to inform national laws and policies. For example, the United Nations Commission on International Trade Law (UNCITRAL) has adopted model legislation for international contracts and is working on uniform rules on electronic signatures; the World Intellectual Property Organization (WIPO) has drafted new treaties; and international groups, both government and private, are promoting standards and protocols.

National efforts need not be identical—either in law or through technology applications—but they must be internally consistent and internationally interoperable. Divergent national approaches resulting either from the failure to adopt legal protections or from raising barriers, will adversely affect electronic commerce to everyone's detriment.

Some countries, including the United States and the European Union, have legislative bodies that must pass and implement legislation at both federal and subfederal levels. Tensions can result from differences in the pace of legislative change at the two levels, as well as cause tussles over jurisdiction. These problems within countries and legislative regions are the precursor to similar issues to be played out globally. Observing how

the United States and the European Union face these issues can be insightful. Much of this section therefore will examine the United States and European Union as representatives of alternative approaches to both jurisdictional overlap and the need for policy interoperability.

Commercial Code and Contracts

National and international efforts now underway to address legal rules for electronic commerce are primarily adapting contract law. UNCITRAL has been the focal point for efforts to develop model legislation to guide the use of international contracts in electronic commerce. While specific contracts between parties could resolve legal issues raised in conducting business electronically, UNCITRAL concluded that relying on local law was unsatisfactory. As a result, it adopted the Model Law on Electronic Commerce in 1996. This is a set of internationally acceptable rules and principles to guide states in removing legal uncertainties arising in the electronic environment.[1] The UNCITRAL model law, endorsed by business groups like the International Chamber of Commerce, has been enacted by a number of countries.

In the United States and the European Union, the operational unit for commercial law is at the subfederal level. Within the United States, the Electronic Signatures in Global and National Act of 2000 embodies the general principles of the UNCITRAL Model Law, but state law has jurisdiction and must be revised. The National Conference of Commissioners of Uniform State Law, the American Law Institute, and private sector groups like the American Bar Association, are promoting the Uniform Electronic Transactions Act (UETA). UETA relies on existing principles of contract law; its objective is to establish legal equivalence between electronic records and signatures and paper and signed documents; it is the first comprehensive effort to adapt state law to electronic commerce. However, not all states have signed on, nor must they, making elusive the common contract framework necessary for the growth of electronic commerce.[2]

In contrast, the European Union, in response to concerns that existing national rules on the formation and performance of contracts were inconsistent, proposes to establish a coherent legal framework for the develop-

1. The model law has rules to validate and recognize contracts formed through electronic means; set requirements for contract formation and governance of electronic contract performance; defines the characteristics of a valid electronic writing and an original document; provides for the acceptability of electronic signatures for legal and commercial purposes; and supports the admission of computer evidence in court. See http://www.uncitral.org.

2. As of April 2000, 7 states had adopted UETA and 27 more had legislation pending. In facilitating a uniform domestic legal framework for electronic transactions, UETA may provide an international model.

ment of electronic commerce within the Single Market. The European Parliament formally adopted the Directive on Electronic Commerce on 4 May 2000, and member states must implement it within 18 months from publication in the Official Journal of the European Union.[3]

Will mandates at the federal level yield standardization where common approaches and certainty are needed? Not necessarily. On the one hand, the Directive provides that electronic commerce service providers are subject to national laws of the *country of origin*, which implies that such business activities need not be consistent with the laws of 15 different member states. On the other hand, the Commission's proposed regulation on jurisdiction and enforcement of judgments in civil and commercial matters[4] provides that in international on-line contract disputes, a consumer can seek redress *in his/her own country* if the seller approached the consumer through ads. This draft directive could require companies to comply with 15 different sets of consumer protections. Thus, even mandating a ''federal'' or EU-level directive does not necessarily standardize approaches. Efforts to address the inconsistencies between the EU directives are underway (Mitchener, *Wall Street Journal*, 22 November 1999; Greenberg, *E-Commerce Times*, 1 November 1999).

The US and EU examples show that there are two types of inconsistency that governments need to consider in trying to promote certainty: One is between legislative bodies at *different levels of government*; the second is across functional bodies or agencies *within a governmental level*.

Security: Encryption and Authentication and Certification

More than 80 percent of companies indicate that security is the leading barrier to expanding electronic commerce with their customers and partners. After the February 2000 hacker attacks paralyzed several popular Web sites, surveys showed that nearly 60 percent viewed the attacks as a ''watershed event'' for US electronic commerce, 65 percent would be more cautious when doing business online as a result of the attacks (Information Technology Association 2000), and 70 percent were not comfortable providing credit-card information over the Internet (Center for Democracy and Technology 1999). It is not just the consumer who is concerned: The May 2000 Love Bug virus cost companies billions of dollars

3. The directive addresses treatment of electronic contracts, the definition of where operators are established, transparency and information requirements for operators and commercial communications, liability of intermediary service providers, dispute settlement, and the role of and cooperation between national authorities. See Directive on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the internal market (Directive on Electronic Commerce) at http://www.ispo.cec.be/commerce/legal/legal.html.

4. A revision of the Brussels convention.

as their internal computer systems crashed and communications were disrupted.

Security implies that consumers and businesses can be confident that

- communications and data are safe from unauthorized access or modification,
- sellers and buyers are who they say they are, and
- both the individual transaction mechanisms and the overall network are secure.

Promoting secure systems and certifying the authenticity of parties to a transaction are essential to a climate of trust for the purchase and sale of products over the Internet.

While a range of technologies, techniques and protocols promote secure Internet transactions, the primary ways to establish security and trust on open networks has been through two major technology applications—encryption and authentication.[5] Authentication techniques, including digital or electronic signatures and certification mechanisms, help to ensure the origin of the data (authentication) and verify whether data has been altered (integrity). Encryption helps to keep data and communications confidential.

How has electronic commerce changed the environment and put a higher premium on security? The Internet uses an open, nonproprietary protocol that allows for more global marketplace participation, from large to small firms and consumers, as well as multiple jurisdictions. It operates much more quickly, requiring that money and products be transmitted or mailed simultaneously rather than sequentially. It is also more anonymous, with fly-by-night companies potentially operating outside the reach of authorities.

Encryption

Encryption is widely regarded as the most promising answer to the problem of securing electronic transactions. Lawrence Lessig, an expert on the legal aspects of the Internet, asserts that ''encryption technologies are the most important technological breakthrough in the last one thousand years'' (Lessig 1999). Encryption is the transformation of data based on the operation of mathematical algorithms, which reduce messages to a set of numbers that can be decoded only by those who have the algorithm

5. Early examples of security protocols for online transactions like using credit-card information over the Internet were Netscape's secure socket layer (SSL) and the secure electronic transaction (SET) protocol adopted by credit card companies, but both were only partial solutions to the security problem.

key that created the coded text.[6] Encryption represents the locks and keys of electronic commerce, enabling individuals to keep data and communications confidential as they are transmitted over the Internet.

Electronic mail, on-line banking, Internet credit-card purchases, electronic taxes, and medical records all use some form of encryption technology. As more businesses and individuals come online, the need for strong, reliable encryption technologies will increase. Its use is likely to become ubiquitous.

The widespread use of encryption, however, raises fundamental law enforcement and national security problems. The same technology that guarantees secure and private transactions for consumers can also be used by criminals and terrorists to hide their illegal activities. Intelligence gathering by governments for national and foreign policy purposes depends on access to information. The more data encrypted, the more difficulty intelligence agencies have in collecting information. Because of these legitimate and competing objectives encryption policy has been one of the most contentious electronic commerce-related issues within the United States, and between the United States and other countries. Encryption policy exemplifies the problem of both overlapping jurisdictions as well as issue convergence—that is, policies broached by one government will impact another—and second, even within a country, policymaking objectives overlap so that policies to achieve several objectives cannot be made independently.

In an attempt to balance national security and domestic law enforcement concerns with the need for security and trust in electronic transactions, the United States had restricted exports of ''strong'' encryption.[7] Export controls have been the primary means to limit the proliferation abroad of encryption technology that intelligence and law enforcement groups find difficult to break. Within the United States there are no restrictions on the use or strength of domestic encryption, in part because of the US domestic political culture.[8]

Other governments face the same commercial, security, and law enforcement concerns, but their approaches differ. Many countries (including France, China, Israel, Russia, and South Africa) restrict domestic use of encryption products. Laws in Singapore and Malaysia require

---

6. For a detailed explanation of encryption, its applications, and types of encryption, see http://www.rsasecurity.com/rsalabs/faq/1-7.html.

7. The strength of encryption—how easy it is to break the code—depends on the algorithm: The greater the number of possible keys, the longer it will take to crack. DES, the data encryption standard, is 56-bit encryption, which means that 100,000,000,000,000,000 keys are used. Adopted in 1976, it remains the official US standard for encryption today. See Singh (1999).

8. Some members of the law enforcement community do want to restrict the domestic use of encryption (arguably a more effective means of control than export controls).

users to disclose their encryption keys or face criminal penalties (Clausing 2000b). Earlier this year, China announced plans to ban companies from buying products containing foreign encryptions, and to require foreign firms to register their software with the government. The change in US policy (see box 7.1) means that other countries that had depended on the United States to prohibit the export of strong encryption are now considering domestic controls.

Because of the tensions between the law enforcement, security, and commercial communities, multilateral coordination of encryption policies has been limited, although there has been discussion in the OECD. Its 1997 Guidelines on Cryptography Policy offer basic principles for formulating national policies to secure electronic commerce transactions; in 1999, OECD produced an Inventory of Controls on Cryptographic Technologies. The primary international instrument for export controls on encryption products is the Wassenaar Arrangement, an informal group that coordinates the export control policies of 33 nations. Because of the significant national security implications of encryption, the United States discouraged international institutions from addressing the issue other than through the Wassenaar Arrangement.

As one of the earliest users of the Internet, with an industry at the forefront of encryption methods, the US experience is worth reviewing to see how the problem of issue convergence played out. Several lessons emerge from how the United States tried to reconcile the competing interests of law enforcement, security, and commercial gain.

First, the attempt to restrict the proliferation of strong encryption abroad failed. In fact, it encouraged foreign firms to create their own encryption products—firms that the US government cannot directly regulate and which compete directly with US companies.

Second, the attempt to mandate a specific technological outcome—key escrow, key recovery, or recoverable encryption—was largely unsuccessful. The fact that some firms did respond to the pressure and produced recoverable products shows, however, that government actions can still influence the market, even when the policies are not successful. However, influence fell far short of an optimal solution.

Moreover, this experience offers evidence that governments should work to facilitate technologies that meet public policy *objectives*, rather than try to mandate a technological *outcome.* Given the competitive world economy, government restrictions without multilateral agreement are bound to be futile.

Third, there were (and continue to be) costs to government intervention. In this case, government actions actually impeded the growth of electronic commerce, since time and money were spent trying to push the market in a different direction from where innovation and the global industry were moving. US firms lost market share.

Box 7.1 US encryption policy

The evolution of US encryption policy over the past decade provides an example of government efforts to reconcile the competing objectives of national security and law enforcement with the desire to promote electronic commerce.

US policy has been characterized by one attempt after another to mandate the development and use of a specific type of encryption application. In 1993, the US government announced the ''Clipper Chip,'' which would be attached to a telephone and protect private communications. It used a key escrow system whereby two keys would be deposited with two separate government agencies, which law enforcement officials could access under certain circumstances. Predictably, industry and privacy groups rejected the proposal.

In 1995-96, the government revised its policy several times to relax export controls, provided that a key was escrowed with a USG-certified agent, not the USG. It also established the basis for a ''public key infrastructure'' system, which many experts believe could ultimately provide the basis for a secure environment. The administration finally settled on a policy that allowed the export of 56-bit or longer encryption, but only if US companies committed to develop ''key recovery'' products. Such products would permit the recovery of encryption keys, thereby allowing law enforcement officials access to the text of the communication under legal authorization. The administration's efforts amounted to a type of industrial policy in which the government leveraged firms' need to export to promote a technological solution that was optimal for government.

The policy of trying to mandate key recovery encryption engendered strong opposition from US high technology firms, who feared that export controls would result in competition abroad from companies not subject to comparable restrictions. At the time, US companies had most of the world market share in encryption technology. Privacy advocates also opposed the policy as an unwarranted intrusion on individuals' rights to ensure the privacy and security of their electronic communications. In addition, a blue-ribbon panel of the National Research Council issued a report in 1996 detailing the growing vulnerability of computer networks in the information age and the importance of encryption; it recommended the relaxation of export controls.[1]

(*continued next page*)

Finally, how encryption unfolded is a useful reminder that, in an age of revolutionary change, new thinking on issues like national security is essential. Important concerns about Internet technology can often best be addressed and potentially fixed by modifications to the same technology. This is clearly a task for the private sector. While it is appropriate for governments, on behalf of society, to identify needs and set public objectives, government regulation is likely to hinder optimal solutions.

Encryption is potentially the answer to the most difficult public policy issues related to electronic commerce, especially privacy. Encryption technologies can put decisions in the hands of users, letting them choose the degree of security or privacy their values require. The proper role of governments seeking to promote electronic commerce is to encourage the development and widespread use of this critical technology.

On the other hand, traditional societies or countries more concerned about domestic law and order and fundamental national security than is

Box 7.1 (*continued*)

In the face of mounting business and privacy opposition, and Congressional threats to eliminate encryption controls entirely, the United States significantly relaxed its policy in early 2000 to allow for the export of any encryption product regardless of strength to most customers with some minor exceptions. The policy shift, characterized by US government officials as helping business and promoting electronic commerce, was seen by many as a repudiation of US efforts to mandate a specific type of technology, but was nonetheless welcomed by high tech firms and US allies.[2]

Although the United States eventually was forced to abandon its policy, the attempt was not without costs. Whereas US companies making encryption products had few competitors in 1993, today there are many encryption firms—Brokat in Germany and Baltimore Technologies in Ireland among them—that have experienced phenomenal growth, due in large part to US restrictions. Despite industry opposition to the key recovery policy, many firms did actually develop products with recovery features built in, especially software firms.[3]

1. National Research Council Computer Science and Telecommunications Board (1 May 1996).

2. Secretary William Daley in US Department of Commerce, press release, ''Commerce Announces Streamlined Encryption Export Regulations, 12 January 2000.

3. Lessig, 1999, 52. Included in the list of companies that produce recoverable products are IBM, Network Associates, the owner of PGP, and Cisco as part of a router.

the United States are likely to resist the widespread use of encryption by their citizens. International discussions may help alter their view of the balance of benefits of the global network against the limitation of domestic jurisdictions. These discussions may also make clear the limited effectiveness of domestic approaches.

Authentication and Certification

Electronic or digital signatures[9] are used in electronic transactions to identify parties, authenticate messages and information, and verify that data have not been altered. Authentication techniques, which include digital or electronic signatures, can be implemented through different technologies depending on the needs of the parties and the transaction. Such methods are not new—passwords and other means have been used for years in EDI transactions—but today there are a wide variety of authentication methods.

9. Authentication includes digital signatures and other forms of electronic signatures—terms have been used interchangeably, creating confusion. The differences are the subject of international discussions, but for simplicity, *authentication* refers to the larger class of electronic applications whose function ranges from identification and authorization to legal recognition, thereby covering electronic signatures as well as other technologies.

Authentication techniques linking individuals and entities in the electronic environment are less meaningful if they are not accompanied by certification mechanisms. Certification authorities (CA) or other certification methods are independent means of verifying transactions and parties in the electronic world. A CA establishes trust by authenticating the identity of participants to an on-line transaction, providing legally-binding proof of messages sent over the Internet, and verifying the integrity of the information exchanged. Numerous private companies provide these certification services, as they have for years, without the benefit of legal protections or government approval.[10]

Internationally, the issue of authentication has been broached primarily in three different venues: UNCITRAL has been dealing with the legal issues, OECD the policy framework, and standards bodies like World Wide Web Consortium (W3C) and the International Organization for Standardization (ISO) on the technical standards. The private sector has contributed significantly to these bodies, including through the International Chamber of Commerce's GUIDEC—General Usage for Internationally Digitally Ensured Commerce—which provides definitions and best practices to facilitate a global framework to ensure commerce over electronic media.[11] As with encryption, a key issue in the context of authentication and certification is technology neutrality: Because the Internet is so dynamic, it is important that policymakers not codify a particular technological solution into standards or laws.

UNCITRAL has been drafting uniform rules to support the use of electronic signatures, as well as reviewing the legal aspects of digital signatures and certification authorities. Because authentication technologies evolve rapidly, the UNCITRAL Working Group adopted a technologically neutral approach to avoid excluding future technologies from the scope of the uniform rules. The draft rules, therefore, cover all forms of electronic signatures and authentication techniques, and address standards that certification authorities should meet.[12] Similarly, the OECD affirmed a nondiscriminatory approach to electronic authentication, and members have committed to amend laws and policies that may impede specific electronic authentication mechanisms.

However, the fact that such rules are not binding has led the United States, Japan, and France to call for an international convention on elec-

10. The US government has supported legislation to protect CAs from liability, believing that legal protections would encourage more widespread use of certification mechanisms.

11. http://www.iccubo.org/home/guidec/guide.asp.

12. Also addressed in the draft are the principle of party autonomy, presumption of signing and originals, duties and responsibilities of signature holders and CAs, and recognition of foreign certificates. See http://www.uncitral.org/en-index.htm for the Draft Uniform Rules on Electronic Signatures.

tronic transactions. A binding convention would embody principles of party autonomy and technology neutrality in choosing electronic authentication methods, as well as establish minimal rules that prohibit paperless records and signatures from being rejected in court simply because they are electronic.

In 1998, OECD countries adopted a Declaration on Authentication for Electronic Commerce at the Ottawa Ministerial Conference. The declaration stated principles encouraging the formulation of electronic authentication policies with minimal government regulation, technological neutrality, and party autonomy. The OECD has also addressed international interoperability and mutual recognition of CA. This is important because certifications issued in one country might not be recognized in another, especially if some countries require licensing and will not accept certifications from unlicensed foreign CAs. The OECD also prepared an Inventory of Approaches to Authentication and Certification in a Global Networked Society. Their survey found that most countries have taken one of two approaches: Comprehensive measures enabling digital signature technology, or a minimalist technology-neutral approach that simply establishes the legal validity of any kind of electronic signature.

The technical aspects of authentication and certification have been addressed by the W3C in its project to use digital signatures and certificates and other technologies comprehensively to help users find effective ways to represent digitally signed assertions and endorsements that extend beyond the identity and integrity functions. Meanwhile, the ISO and Internet Engineering Task Force have been working on technical standards development.

As with taxes (chapter 6) and contract law, nations that have both federal and subfederal jurisdictions are challenged to achieve consistent domestic solutions given the overlap in jurisdictions. The US and EU approaches represent two alternative strategies.

At the federal level in the United States, Congress passed legislation in June 2000 to establish a uniform national framework for electronic transactions. The legislation grants electronic signatures the same legal force as traditional paper signatures, endorses a technology-neutral standard for electronic authentication, provides that federal rules will not preempt state law covering electronic agreements, and provides certain legal protections for consumers.[13] For their part, the states have enacted or are working on legislation recognizing the validity of electronic signatures, with most states having adopted minimalist enabling proposals to ensure that electronic signatures are not denied legal effect simply because they are electronic.[14]

---

13. The Electronic Signature in Global and National Commerce Act 15 is expected to be adopted in 2000. See Olender (2000).

14. Forty-one states have taken some action to address electronic transactions. See Internet Law and Policy Forum (2000a).

The European Union has taken a different approach. Prompted by concerns that differing national standards, as well as a lack of mutual recognition, could fragment approaches to electronic commerce and online services within the European market, the European Union drafted initial measures on digital signatures in 1997. The proposal was modified and adopted in 1999 as the Directive on a Community Framework for Electronic Signatures, which establishes rules for security and liability for transactions in all the member states. While the European Union's objective is to recognize electronic signatures as legal irrespective of the technology used, the Directive may in fact create a preference for particular types of electronic authentication and a presumption that electronic contracts signed using the government-endorsed methodology are legally binding (Pincus 1999).

Many countries now have laws relating to electronic signatures, and even more have proposals pending. Such measures are increasingly important to the growth of electronic transactions, especially since many countries still require prior written agreement for contracts to be valid between parties not in the physical presence of each other.[15]

The most common approach, generally adopted before 1999 by countries such as Argentina, Colombia, Germany, Italy, South Korea, and Malaysia focuses on digital signatures only and a regulated approach to CAs. Similarly the Indian Parliament in May 2000 passed legislation to establish the legal validity and enforceability of digital signatures and electronic records. More recent initiatives like those in Mexico and Canada in April 2000 may indicate a trend toward addressing electronic authentication and certification issues more broadly and flexibly, rather than just endorsing digital signatures.

In sum, disparate approaches to electronic signatures can create obstacles to electronic commerce.[16] Clearly, there are differing standards on multiple levels—state, national, and international. Some entities—subfederal as well as national—have adopted measures favoring digital signatures to the exclusion of other technologies.

Given that the market has not coalesced around one authentication method, and given the pace of technological change, prescriptive legislative approaches to security, authentication, and certification are not optimal. They undermine the network benefits of global electronic commerce. Policymakers should provide a flexible legal framework that makes electronic signatures valid, and allow the market to choose the technical means of meeting consumer and business security needs.

---

15. Such is the case in Mexico, which necessitated the May 2000 amendments to its Civil and Commercial Codes regarding electronic transactions. See http://bakerinfo.com/ecommerce.

16. The OECD is surveying its members regarding national laws and regulations that may act as obstacles to the use of electronic signatures. The results, which are likely to be available late this year, could spur activity to harmonize national approaches.

The lack of a uniform international framework for electronic authentication and certification may well be slowing the widespread use of electronic signatures. As electronic transactions using authentication methods become more commonplace, problems with inconsistent approaches are likely to increase if key issues such as mutual recognition across borders are not addressed. International discussions like those in the OECD and technical bodies should be expanded to include more countries so as to promote consistent authentication principles and interoperable policy internationally. It is important that the private sector actively engage with policymakers to ensure interoperability of both technological solutions and policy approaches.

Standards

As noted previously, standards and protocols are an important part of a legal framework for electronic commerce that promotes an environment of certainty and trust. Standards may be national and international as well as formal and informal means to ensure the interconnectivity of computer and telecommunications networks. Collectively, these technical specifications allow different products and services to work together so users around the world can communicate independent of the type of computer, ISP, or network used. ''In effect, the global information infrastructure will be a federation of heterogeneous networks operating via standardized interfaces for the interconnection of networks and which allow applications to be run across them with seamless interoperability.'' (Arzano 1997).

How standards are developed varies from informal dialogues among industry representatives like the Internet Engineering Task Force (IETF) and W3C, to international bodies such as the ISO, the ITU, and the Internet Corporation for Assigned Names and Numbers (ICANN). For the most part, the private sector has led the way in setting the standards for electronic commerce, aware as it is of the danger of prematurely locking in standards that can be overtaken by technological advances and market preferences.

The standards process is necessarily dynamic, continually evolving as technology itself changes. Adaptability and dynamism is key:

> If several years ago, a standard-setting body or a government agency had sat down and tried to define electronic commerce standards or structures, no person, no matter how enlightened, could have hoped to envision the future and develop protocols to serve all the needs that have emerged. . . . No standard-setting body could hope to replicate the innovations that will be introduced according to the demands of commerce itself (Hillebrand 1999a).

Examining the approaches of the United States, the European Union, and Taiwan offers insights on why different sets of policymakers choose

one type of intervention over another. These alternative approaches may yet yield interoperable outcomes.

The US government has consistently promoted the position that the marketplace, not governments, should determine technical standards (A Framework for Global Electronic Commerce 1997). While encouraging the private sector to take the lead in setting standards, the US government informally works with industry, primarily through the Commerce Department's National Institute for Standards and Technology (NIST). NIST is a neutral forum for bringing together broad industry representation and facilitating the dialogue necessary to address standardization.

This informal process of dialogue with industry stands in marked contrast to the EU system. With a long history of regulatory barriers as a result of the diverse manufacturing standards within European countries, the European Union relies on more formalized structures and a centralized process to help set European standards. As a result, European countries have tended to dominate the ISO process. American companies have expressed concern that European countries may be using the standards-setting process to favor European manufacturers. But US firms gain global recognition and reach when they conform to ISO standards. So, it is the neutrality of the standard-setting body that is at issue.

In some countries, such as Taiwan, the government has thought it desirable to choose among standards that are being set by the private sector internationally and exhort domestic entities to adopt that standard. The belief is that this approach will save time and effort for the domestic private sector, which can then expend its energies on innovation in other areas.[17] To the extent that there is an internationally agreed standard, this approach—where the government informs the domestic private sector of the outcome of the international contest—may be valid. Once a country reaches the international technological frontier, this approach is less viable.

The balance is between interoperability and dynamism. Interoperability need not mean that single, uniform solutions are applied to electronic commerce (Pincus 1999a). Local requirements dictate differing implementation, but the more interoperable these different approaches are, the more electronic commerce will be facilitated. Industry representatives have worked effectively in international standards-setting organizations to set voluntary standards. To achieve network benefits (discussed in chapter 2), the private sector has a strong incentive to set standards to enable interoperability as well as dynamic change. Government-mandated approaches tend to remove incentives for private-sector innovation. Consequently, policymakers should facilitate private-sector efforts within an

17. Field research by Catherine Mann and colleagues, August 1998.

international, voluntary, and consensus-based environment. They should not mandate standards for electronic commerce.

Intellectual Property

Generally, the architects of intellectual property protection laws must balance the need to protect intellectual property that is expensive to produce but easy to replicate with the desire to promote competition and further innovation.[18] Characteristics of the Internet and electronic commerce—information rich, network effects, global reach, rapid technological change—accentuate the importance of and challenges to intellectual property protection.

Consequently, an analysis of intellectual property protection must proceed along several fronts at once. Intellectual property law needs to address the *extension* of protection to materials transmitted over the Internet, as well as the delivery mechanics. It needs to address the *scope and length* of protection for business methods used to conduct electronic commerce and to collect information into databases. While the way forward for policymakers is convoluted and murky, suggesting a considered approach, technology and businesses are galloping forward at breakneck speed. Will the pace of technology and business obviate or undermine policymakers? Or will policymakers misjudge the extent, scope, and length of protection needed to support innovation, impeding the growth of global electronic commerce?

Intellectual property protection for software related to the Internet and electronic commerce is increasingly exposing issue convergence and jurisdictional overlap. For example, the approach to intellectual property protection affects other policy concerns, including consumer protection. In addition, just when international cooperation on intellectual property protection has started to bear fruit in the context of WIPO and WTO Trade Related Intellectual Property (TRIPS), such agreements may be so broad as to stifle the dynamic e-commerce environment and, in particular, the prospects for developing countries and new business.

Although e-commerce policies across the board are in a state of flux, policies for protecting intellectual property are in a particularly dynamic phase. Several examples will help show the different angles that policymakers must face and address. These examples suggest that a single approach that covers all types of intellectual property related to electronic commerce will be very difficult to craft.

---

18. See Keith Maskus (2000) for a remarkably comprehensive analysis of the economics of intellectual property, subsequent policy issues, and empirical analysis.

Why Raise the Issue of Intellectual Property?

As discussed in Part One, information is an increasingly important component of the product bundle, and information, by itself, has the attribute that it is noncontestable (the information can be used by more than one person without being used up). As discussed in Part Two, digital delivery of perfect copies is increasingly possible and indeed desirable. Looking at intellectual property law and electronic commerce through this lens, the enormous potential of electronic commerce cannot be realized without assurance that a seller's intellectual property will not be stolen, and that buyers are confident they are obtaining authentic products. Clear and effective copyright, patent, and trademark protection are necessary to protect against piracy and fraud on the Internet (see box 8.4 for more discussion).

On the other hand, interoperable computer methods that build on existing platforms for electronic commerce increase the value of the network to everyone. Indeed, such open standards and protocols have spurred the exceedingly rapid development of the Internet and electronic commerce thus far. Similarly, because of network effects, information can have increasing value, as more people have access to it, use it, and augment it (consider an auction site, for example). Therefore, IP protection that limits the ability of firms to create interoperable software will constrain the value of the whole network, as well as keep out new firms and participants. This kind of intellectual property protection could not only slow the growth of electronic commerce generally, it could exacerbate the divide between early adopters and later entrants.

Issues for Transmitted Materials

The issue of intellectual property for transmitted materials is probably more clear-cut, in that the nature of electronic commerce and the availability of new technologies make it relatively easy to circumvent controls and to widely distribute illegal duplicates. Consequently, this issue was the first that national and international bodies addressed. However, there are still numerous questions about the reach of this protection.

In December 1996, under the auspices of the WIPO, nations joined to create the foundation for strong IP protection on the Internet. Two treaties updating the Berne Convention—the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty—were negotiated. These treaties require adequate and effective protection for copyrighted works and sound recordings in cyberspace, including the communication, reproduction, and distribution of electronically transmitted data. Both treaties cover technological protection, copyright management information, and the right of communication to the public. The treaties also permit countries to implement provisions in accordance with differing national legislation, and provide for exceptions to rights in certain cases that do not conflict

with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author (e.g., fair use). The treaties will enter into force upon ratification by 30 states.[19]

However, key elements of implementation of these agreements were not addressed in the new WIPO treaties, including third-party liability, application of the fair-use doctrine, and limitation of devices to defeat copyright protection. In these three areas, the pace of technological change is forcing signatories to figure out how to adjudicate protections within the realm of intellectual property itself, and moreover, how to balance IP protection and other protections with policy mandates, such as consumer protection.

For example, what rights and obligations are associated with having links to sites that facilitate decoding of copyrighted data? Can companies that link to other sites be prosecuted for violating a law, even if the company itself does not violate any law? The case at issue now in US courts is software (DeCSS) that decodes the protective devices that limit the copying of DVD format material (Kaplan 2000).

Are companies violating fair use doctrines when they cache information (hold it or replicate it so that it can more efficiently use Internet technologies as well as quickly deliver the requested information). Does it matter whether caching is on a satellite or a server?

Whose responsibility is it to properly account and pay for use if financial obligations result from digital transmission of copyrighted material? The Secure Digital Music Initiative (SDMI), an international consortium of 120 companies and organizations, has already crafted a specification for delivery of digital music that is interoperable with existing formats. SDMI is now working on a set of principles that will embrace interoperability of formats, ensure copyright and certification (via digital watermark), and also fulfill the desire to have unprotected formats.[20] It does not appear that SDMI would be the financial arm or watchdog, however. Instead, offshoots of existing financial clearinghouses (BMI and ASCAP) are strengthening their on-line presence.

Issues of Business-Method Software

Patent rights for software is a fundamental question.[21] Because of recent court decisions, US legislation, and new policies of the US Patent Office

19. As of 21 June, 2000, 18 nations had ratified the Copyright Treaty, and 15 had ratified the Performances and Phonograms Treaty. See http://www.wipo.int/eng/ratific/doc/u-page.doc. The United States ratified and passed implementing legislation in 1998 and deposited its instruments of ratification with WIPO in September 1999.

20. See http://www.sdmi.org.

21. For a legal perspective on these issues, see Groff (2000), http://www.gabar.org/ga_bar/febcov3.htm.

(USPTO) and the European Patent Convention that expand subject matter eligibility, business-method software is now the fastest-growing category of new patents.[22] In the fiscal year ended September 1999, computer-related software patent applications to the USPTO doubled to 2,600 and about 600 were granted. The potential for a proliferation of patents for basic e-commerce software, which already includes Amazon.com's One-Click feature, Priceline.com's reverse auction method, and Mobjob.com's group-buying technique, is viewed by Lawrence Lessig, one of the world's experts in Internet law, as ''the single greatest threat to innovation in cyberspace.'' (Gleick 2000).

The economic issue is how to balance protection so as to maintain innovative activity with the potentially anticompetitive effects of such protection, which may be more severe in the e-commerce world because of network effects. In addition to this inherent difficulty, business-method patents expose the jurisdictional tensions between US and European national approaches and commitments and obligations under international agreements in TRIPs.

Specifically, TRIPs patent protection extends 20 years and allows reverse engineering of software; neither of these provisions makes sense for business-method software. On the one hand, reverse engineering allows new entrants to build on and augment existing platforms, which can yield the tailored approaches that benefit classes of users, and also furthers network benefits by ensuring the interoperability on which those benefits depend. But reverse engineering scuttles the very protection that is being granted.

On the other hand, nearly everyone agrees that 20 years is too long for business-method software; Jeff Bezos, CEO of Amazon.com, has suggested shortening patent life to 3 to 4 years. But because of the TRIPs provision, the United States has little incentive to change its own laws, and certainly no ability to change the length of patents agreed to in other jurisdictions (Sandburg 2000). The USPTO plans a ''partnership roundtable'' in summer 2000 to include the full range of stakeholders to discuss business-method patents.

Issue Convergence: Intellectual Property and Consumer Protection

Because it is so easy to transact business over the Internet, issues of intellectual property protection and consumer protection are colliding in both domestic and international jurisdictions. A US example is the Uniform Computer Information Transaction Act (UCITA), written under the auspices of National Conference of Commissioners on Uniform State

22. The relevant court decision was *State Street Bank & Trust Co. v. Signature Financial Group* in July 1998. The relevant US legislation is the American Inventors Protection Act of 1999. The European patent convention is expected to in effect legitimize patenting of business-method software later in 2000. For more discussion, see *The Economist* (18 April 2000), Horvath (1999), and Fried (2000).

Laws. The essence of UCITA is that software and other forms of digital information are neither a good nor a service but a transfer of a right to use intellectual property.[23]

Although still under legal review and comment, some argue that UCITA would void or weaken many of the consumer protections offered to buyers under existing defect and warranty laws. It would affect what buyers could do after having ''bought'' a product, since in effect they are not buying but renting it; for example, buyers would have to remove the software if they gave away their computers. Moreover, the vendor could under some circumstances void the software remotely—the mere ability to do so causes much angst among privacy advocates.[24]

An international example of how consumer protections and intellectual property are colliding is on-line sales of prescription pharmaceuticals. The ''grey-market'' trade in prescription pharmaceuticals is not new (Maskus 2000). However, reduced frictions between geographical markets, polar opposite governmental approaches to the pricing and availability of pharmaceuticals, and the increased anonymity of the Internet accentuate its possibilities. The US Customs service seized 4½ times as many packages containing prescription drugs in 1999 than in 1998; they confiscated abou2 million pills (Pear, *New York Times*, 10 January 2000). Nonetheless, the level of capture is small, pointing to the difficulty of sorting through the huge volume of international small-package flow.

This trade undermines the patent protection given to prescription pharmaceuticals. Moreover, some drugs are misbranded, which in itself undermines the value of the company when the drug does not perform as expected. However, there is also the fact that some drugs do not meet US quality standards or are illegal, putting consumers at risk. In some cases the imported drugs are identical in every way except price, with the price difference resulting from different government regulations of pharmaceuticals. On balance, the United States is more concerned with fraudulent activity and has proposed extending federal jurisdiction to on-line drugstores—but they have official jurisdiction over only US drugstores. There is no international consumer protection, and the international intellectual property protection is being ignored.

Trusted Environment

The legal and technical aspects of creating a predictable legal environment discussed in the previous sections are the necessary foundations for elec-

23. See the discussion of this distinction (between buying and renting) in the context of tax liability in chapter 6.

24. The governor of Virginia has signed UCITA into law; many other state legislatures are considering it. Some see the refusal to sign this legislation as an indication that these states

tronic commerce to flourish. Governments must therefore give them high priority in the near-term if electronic commerce is to take hold. Generally, these aspects call for consistent approaches by governments.

However, other aspects of establishing an environment of certainty and trust that governments will be forced to address—such as protection of individual privacy, consumer protection policies, and approaches to objectionable content on the Internet—are more complicated. How can the benefits of electronic commerce be balanced with the need to protect individual and societal values, for instance? Because a government's policies will be based on political culture, legal tradition, and values, issues of trust are more likely to generate differing national approaches—there is no ''right'' policy. Yet, national policies will require international coordination, as well as ways to resolve conflicts, if network benefits are to be enjoyed. Technology, too, is important in establishing trust, and empowering individuals to make choices about how much security, privacy, and access they desire.

To a great degree these issues of trust deal more with B2C transactions than with B2B transactions, where the fastest growth is expected. Therefore, it may be less urgent to address these issues than to put in place the basic legal and technical infrastructure. However, the promise of electronic commerce will not be realized unless consumers feel safe and secure.

To a greater or lesser degree, governments traditionally champion consumer interests as a result of the fundamental asymmetry of market power discussed in chapter 2. The point was broached there about how much the new environment of the Internet and electronic commerce might accentuate or reduce this asymmetry. On the one hand, the environment is more global, more anonymous, and faster paced, which might tend to accentuate the power of business over consumer. On the other hand, thanks to technological innovation, it has never been easier for consumers to get information about businesses and to ''click'' away from unresponsive ones.

The key questions are: Will a government approach that emphasizes self-regulation and technical innovation meet the demand for privacy, for consumer protection, and content? If the answer is no, how can the threat to electronic commerce posed by nationally mandated solutions be minimized? And how important is the human factor in these assessments?

Privacy

With the many benefits of electronic commerce comes the challenge of how to manage personal information. Electronic commerce creates information

are ''unfriendly'' toward technology companies. One way or the other, the patchwork quilt of legislation will undermine both consumer and producer protections.

trails that allow transaction information to be tracked, collected, and compiled, providing vast amounts of information about personal details of people's lives. While personal information has been tracked for years, through barcode scanners, credit cards, and the like, what is fundamentally different today is the ease with which data can not only be gathered and compiled electronically, but also manipulated and used. Data collection on the Internet has become widespread (and big business), with 92 percent of all commercial Web sites collecting some personal identifying information (Georgetown Survey 1998) (also box 7.2).

While the on-line market is still growing, consumers increasingly are concerned about the vast amounts of personal information available in the electronic world, and how it is used. In a recent poll, 85 percent of those surveyed cited the privacy of information transmitted online as the most important issue related to the Internet (overtaking censorship).[25] If consumers fear that the information they provide online may be used inappropriately, they will hesitate to participate, thereby slowing the growth of electronic commerce and limiting the many benefits of its full realization. How governments respond to this lack of consumer confidence—specifically, whether they adopt market or mandated policy approaches will have a significant effect on the future of electronic commerce.

Privacy stirs deep concerns. Some interest groups respond with moral outrage, noting that most countries in the world recognize privacy as a fundamental human right. The most recent constitutions specify rights to access and control of one's personal information (Privacy and Human Rights 1999). Some groups advocate that countries worldwide adopt comprehensive privacy and data protection laws.

In trying to produce better-tailored products, industry highly values the collection of information from everyone, and may undervalue the demands of users who want less personal data collected. But industry does not want to scare away users and reduce the network benefits. Groups like the Alliance for Global Business and the Global Business Dialogue on Electronic Commerce (GBDe) have called for a flexible approach to the protection of personal information, ''including the acceptance of self-regulatory solutions and technological innovations that empower the user'' (Global Business Dialogue 1999). The Transatlantic Business Council also supports industry-led, market-driven privacy protection principles, and suggests that national privacy protection allow for differences based on national political systems and local culture.

International Initiatives

Even before the advent of the Internet, the OECD in 1980 promulgated the Guidelines on the Protection of Privacy and Transborder Flows of

25. @plan (2000), Schwartz (*Washington Post* 20 May 2000, E1). Similar figures have come out of other surveys.

Box 7.2 The DoubleClick imbroglio and information gathering practices

The challenge to privacy today comes primarily from the advent of powerful technologies that allow an unprecedented amount of information to be gathered, stored, analyzed, and manipulated efficiently and inexpensively. Browsing the Web can divulge a significant amount of information to the Web sites visited, in most cases without the user's knowledge.

Profiling refers to the practice of aggregating information about consumers' interests and preferences gathered by tracking their movements online, and using the resulting profiles to create targeted advertising on Web sites. ID cards, advertisements, and Web bugs are means by which information is exchanged automatically when individuals visit Web sites.[1] A common practice is the use of ''cookies''—data files that sites embed on a user's browser when users visit Web sites. Each cookie contains a tracking number, thereby identifying the computer, though generally not the user. However, if a user gives his/her name to a site during a transaction, or visits multiple sites that subscribe to the same tracking system, a common cookie can cross-reference information, thereby revealing even more personal information. Usually these processes take place without any notification of or awareness by the consumer.

This type of information-gathering has been ongoing for years. However, when the US firm, DoubleClick, the biggest supplier of on-line advertising, acquired Abacus Direct Corp., a database firm with information on millions of consumers gathered through direct mail marketers, and announced plans to target advertising to Internet customers, there was a strong public outcry.[2] The combination of the databases would link anonymous visits to a Web site with a person's real name and address. Even though DoubleClick asserted that the connection would only take place with the users' permission, privacy advocates argued that such permission was gained indirectly, and filed complaints with the US Federal Trade Commission. The states of New York and Michigan opened investigations; Michigan directed the company to suspend its practice of sending cookies to consumers' computers without their explicit permission and commenced legal action.

DoubleClick responded to the criticism and pressure by committing not to link personally identifiable information to anonymous user activity ''until there is agreement between government and industry on privacy standards.''[3] To deal with the public outcry, it also organized a self-regulating coalition of 26 Internet advertising firms known as the Personalization Consortium.[4] The consortium has drafted guidelines for fair access by individuals to their information, redress to change information, and criteria for options to allow users to ''opt-in'' rather than ''opt-out'' of providing personal information when visiting Web sites. Industry representatives are negotiating with regulators over new voluntary restraints on online profiling and reforms of information-handling practices on the Internet.[5] DoubleClick also appointed an independent privacy advisory board of prominent security and privacy experts, as well as consumer advocates to review the company's practices for potential privacy violations.[6]

The revelations concerning DoubleClick and similar information-gathering trends have focused greater public attention worldwide on the implications for privacy on the Internet. As a result, privacy and consumer advocates internationally have mobilized to push for greater legal protections for privacy, not only in the United States but also in other countries emphasizing self-regulation, such as Australia and Canada.[7] The Canadian government recently dismantled a database of information

(*continued next page*)

Box 7.2 (*continued*)

supplied by citizens to the government in large part due to public concerns for privacy, even though there were no known breaches of security.[8]

1. Andrea Petersen, ''A Privacy Storm at DoubleClick,'' *New York Times*, 23 February 2000.

2. DoubleClick's announcement in June 1999 was not the first to generate such a response. In early 1999 Intel faced strong public criticism when it became known that its new microprocessors contained an embedded serial number that could be used to identify individual computers on the Internet; it was forced to offer software to disable the feature.

3. Chet Dembeck, ''Online Privacy Inside and Out,'' *E-Commerce Times*, 25 April 2000.

4. See Laurie J. Flynn, ''Web Privacy Group to Offer a Seal of Approval,'' *New York Times*, 3 April 2000, and Robert Conlin, ''Industry Leaders Tackle Online Privacy Issue,'' *E-Commerce Times*, 5 April 2000. The Personalization Consortium is developing guidelines on the collection of data on users and their surfing activities and a Web seal program.

5. Glenn Simpson, ''Online Advertisers Are Negotiating Deal on Privacy Rules with US Regulators,'' *Wall Street Journal,* 13 June 2000, 8.

6. Chet Dembeck and Robert Conlin, ''Beleaguered DoubleClick Appoint Privacy Board,'' *E-Commerce Times*, 17 May 2000.

7. Adam Creed, ''Australian Government Introduces Privacy Legislation,'' *E-Commerce Times*, 13 April 2000.

8. Steven Bonisteel, ''Canadian Government Kills 'Big Brother' Database,'' *Newsbytes*, 30 May 2000.

Personal Data to embody established principles of fair information practices, and provide a basis for data protection that ensures the free flow of information (see box 7.3). While there is general consensus among OECD members on the validity of the principles,[26] there has been renewed concern about their implementation.

At their 1998 Ottawa conference, for example, OECD Ministers adopted the Declaration on Protection of Privacy on Global Networks, reaffirming their commitment to effective privacy protection and committing to ''build bridges between different national approaches based on law and self-regulation.''[27] The OECD also produced a comprehensive survey of national, regional, and international privacy mechanisms, both legal and self-regulatory instruments (OECD 1999c).

While the OECD has served as a useful venue for discussion among its members, the guidelines are nonbinding and countries have taken different approaches to the implementation of privacy protection. The

26. Citing their use in national and international instruments, the OECD decided in 1998 that it was ''not necessary'' to make revisions.

27. See ''Progress Report on the OECD Action Plan for Electronic Commerce,'' 23 September 1999 at: http://www.oecd.org/dsti/sti/it/ec/act/paris_ec/pdf/progrep_e.pdf.

Box 7.3 OECD privacy guidelines

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

***Purpose Specification Principle*:** The purposes for which personal data are collected should be specified not later than at the time of data collection and subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: with the consent of the data subject; or by the authority of law.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Openness Principle: There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use as well as the identity and usual residence of the data controller.

Individual Participation Principle: An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or her;
b) to have communicated to him or her, data relating to him or her within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him or her;
c) to be given reasons if a request made under subparagraphs *(a)* and *(b)* is denied, and to be able to challenge such denial; and
d) to challenge data relating to him or her and, if the challenge is successful to have the data erased, rectified, completed, or amended.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.[1]

---

1. OECD, ''Guidelines on the Protection of Privacy and Transborder Flows of Personal Data'' (Adopted in the form of a Recommendation by the Council of the OECD on 23 September 1980), http://www.oecd.org/dsti/sti/it/secur/prod/priv-en.htm, 4-5. Twenty-eight countries and the European Union belong to the OECD.

methods/models, some of which can be mixed and matched, include (Privacy International 2000):

- A comprehensive approach, generally with omnibus data protection legislation that governs the collection, use, and dissemination of personal information. Countries taking this line typically name a Commissioner for Privacy to monitor compliance (European Union, Taiwan, Hong Kong, and New Zealand).

- Coregulation, a variation of the comprehensive approach entailing industry enforcement with government oversight (Australia[28] and Canada[29]).
- Issue-specific legislation to protect certain areas, such as financial information, or restrict certain practices, such as unauthorized use of IDs and passwords (United States, Australia, and Japan).
- Self-regulation, in which companies and industry bodies establish codes of conduct (United States, Japan, and Singapore).
- Promotion of technologies and standards that allow consumers varying degrees of privacy and security, including encryption technology, smart cards, and the W3C's Platform for Privacy Practices (P3P) standard.[30]

More than 25 countries have adopted comprehensive legislation, and more countries are considering such laws (Privacy and Electronic Commerce 1998).

Governmental Approaches and Consequences

National approaches to electronic commerce generally reflect differing legal and cultural traditions. The United States and the European Union exemplify two alternative responses to privacy protection.

Relying on market mechanisms and self-regulation, the United States has taken a hands-off approach that emphasizes private-sector leadership and minimal government intervention. This market-driven, self-regulatory model has garnered support in Australia and Japan, among other countries.

The primary alternative is the more regulated model, the mandate approach. With a tradition of comprehensive legislation, the European Union has approached electronic commerce with a more regulatory stance and with a series of directives addressing specific issues. This mandated approach has been embraced in part by Canada, among others.

Either approach must, at some point, be enforced by government or the courts if it is to succeed in its objective of enabling an environment of certainty and trust.

---

28. Australia specifically restricts the government's use of personal information. See http://www.doc.gov/ecommerce/privacy.htm.

29. Canada also restricts the government's use of information. Canada is currently considering comprehensive legislation protecting privacy generally. *Ibid*.

30. The Platform for Privacy Practices (P3P) is a software that converts a company's privacy statements into a machine-readable format, allowing users to be warned if a site gathers more information than they are willing to divulge.

Is there a ''best'' approach to resolving privacy concerns? What happens in the cross-border context when two large trading partners take different approaches? The US-EU differences offer insights into what will become more pervasive questions of overlapping jurisdictions in the global context and is another example of issue convergence.

The Market-Oriented Approach: US Example

The market-oriented approach followed by the United States relies on a mix of legislation, regulatory enforcement, and self-regulation to assure the protection of personal privacy online. Federal and state sector-specific legislation (e.g., information related to children, medical records, or financial information) is combined with private-sector self-regulatory mechanisms. The US system polices self-regulatory commitments through the Federal Trade Commission (FTC). In 1999, the United States created the position of Chief Counselor for Privacy within the Office of Management and Budget to coordinate privacy policy throughout the government.

Self-regulatory efforts have sought user-friendly mechanisms for facilitating awareness and the exercise of choice online, for the adoption by the private sector of fair information practices and for dispute resolution. The objective is to ensure that consumers know the rules, companies comply with them, and consumers have access to personal information in a company's possession, as well as recourse when injuries result from noncompliance.

There has been substantial innovation among private-sector groups to respond to the demands for privacy online. The Online Privacy Alliance has led the way in protecting private information transmitted electronically. Companies and business associations have adopted guidelines for posting privacy policies online, and led a campaign to inform Internet users on how to shield their personal data on the Internet. Several organizations such as BBB*Online* (see box 7.4) and TRUSTe provide an enforcement mechanism through the use of Web site privacy seals. Codes of conduct, such as BBB*Online*'s Code of Online Business Practices, drafted in cooperation with consumer representatives and government, also give merchants guidance on consumer protections.

In the past year, 88 percent of commercial sites surveyed have posted privacy policies or statements, up from nearly two-thirds the previous year (US Government Working Group on Electronic Commerce 1999 and FTC 1998). Some Web sites also offer consumers a choice through click boxes of how much personal information to divulge, although the opting out feature has been criticized as too complicated for many on-line users. A variety of other methods to give users options for personal data disclosure are also in use or under development. However, with increasing public concern for privacy, and the evidence of both domestic and international fraud, the US model has come under greater scrutiny (see box 7.5).

Box 7.4 Industry self-regulation–BBB *Online*

Prominent among private-sector self-regulatory initiatives to promote trust and confidence on the Internet is BBB*Online*.[1] Launched in 1999 as a wholly-owned subsidiary of the Council of Better Business Bureaus (CBBB), the BBB*Online* program builds on the experience and long history of the CBBB in fostering ethical relations between business and consumers through voluntary self-regulation and education. The CBBB provides dispute resolution services, including mediation and arbitration, to corporations and customers, reports on how well companies protect consumers, refers cases of illegal practices to the FTC, and grants the over 250,000 local business members nationwide use of a BBB trustmark.

BBB*Online* has established similar services through its BBB*Online* Reliability and BBB*Online* Privacy Programs. Three difference seals—which are posted on Web sites—are awarded to companies meeting certain rigorous standards, such as a satisfactory complaint record, participation in BBB's advertising self-regulation program, and agreement to dispute resolution at the consumer's request. The Reliability program has enrolled more than 5,000 businesses, making it the most significant Web site trustmark program.[2] The Privacy program awards seals to businesses that clearly post privacy policies meeting rigorous standards, such as notice to consumers, disclosure, choice and consent, and security, and agree to consumer dispute resolution. The Kid's Privacy seal, part of the Privacy program, recognizes businesses that are in full compliance with even more extensive requirements concerning children's privacy online, such as obtaining parental consent before any personal information can be collected or used. The BBB*Online* trustmarks, which readily identify responsible online businesses, have become the electronic equivalent of the Good Housekeeping Seal of Approval for Web sites.

Seeking to internationalize and harmonize the online privacy seal effort, BBB*Online* recently announced a joint initiative with the entity responsible for privacy seals in Japan to develop reciprocal seals that will be easily recognizable by consumers in both countries.[3] Similar efforts are underway in Europe. BBB*Online* has also drafted a Code of Online Business Practices in cooperation with consumer representatives and government to give merchants guidelines to implement consumer protections.

While efforts like BBB*Online*, TRUSTe, and CPA Webtrust provide only a partial response to consumer concerns, they do hold promise as effective and enforceable means of business self-regulation.

---

1. See http://www.bbbonline.org.

2. ''BBB*Online* Reliability Program Reaches 5,000 Businesses,'' press release of BBB*Online*, 16 May 2000. See http://www.bbbonline.org/about/press/051600.html.

3. ''New Online Privacy Protection Tool to Transcend Borders,'' press release of BBB*Online*, 18 May 2000. See http://www.bbbonline.org/about/press/051800.html.

The Mandate Approach: EU Example and Cross Border Implications

European countries generally have comprehensive privacy systems with explicit laws requiring gatherers of data to register with government privacy offices. They prohibit or limit certain data uses, such as direct marketing, that are routine in the United States. In 1995, the European Union adopted the Directive on the Protection of Personal Information

Box 7.5 Changing US environment and emerging trends

As a result of the DoubleClick controversy and increased concerns about privacy on the Internet, a shift in public opinion is underway in the United States regarding the adequacy of the industry's self-regulatory efforts. The credibility and effectiveness of industry self-policing efforts have been significantly damaged, with some analysts predicting that government regulation of electronic commerce privacy issues is a ''foregone conclusion.''[1] The implementation of the Children's Online Privacy Protection Act in April 2000 (see Content section in this chapter), as well as financial services legislation, is seen by many as the first in a series of efforts to regulate consumer privacy online.

As a result of growing consumer concerns, numerous legislative restrictions on Internet privacy have been proposed by Congress and individual states. A House subcommittee recently approved a bill to establish a privacy commission (modeled on the Advisory Commission on Electronic Commerce that addressed the taxation issue) to examine online privacy, identity theft, and the protection of personal records as well as make recommendations on whether additional legislation is necessary.[2] Other legislation would require companies to disclose how they collect and use personal information or prohibit the disclosure of such information without consumers' permission; still other measures would create a new federal seal program to certify Web sites that adhere to fair information practices. Members of Congress even formed a Congressional Privacy Caucus to advocate for personal privacy. Underlying the proposals and new focus on privacy issues are public opinion polls that ranked the loss of personal privacy as the number one issue of concern regarding the Internet.[3]

In addition, the FTC has been more aggressive in promoting privacy, rapidly moving to center stage as the main US government agency addressing Internet regulation; electronic commerce has become the agency's primary concern.[4] Its role will be even larger when the US-EU privacy accord is implemented and the FTC is required to monitor compliance by US firms. The FTC has undertaken a number of initiatives, including a review of the information-sharing practices of health care Web sites, proposed rules for the protection of consumers doing business online with bank and other businesses involving the transfer of money, and establishing an Advisory Committee on Online Access and Security.[5]

Most notably, however, the FTC's position on the adequacy of the current system has changed. Until May 2000, the FTC supported a self-regulatory approach, recommending against new privacy legislation and greater regulation. However, even though new survey results show continued improvement in the number of Web sites that post privacy policies (90 percent), it indicated that only 20 percent meet FTC standards for adequately protecting consumer privacy.[6] With the release of its third report to Congress on the state of online privacy, the commission concluded that legislation is necessary to ensure adequate protection of consumer privacy online.[7] While applauding private-sector self-regulatory initiatives, the report concluded that ''industry efforts alone have not been sufficient,'' and recommended a legislative framework for basic privacy protection for consumer-oriented Web sites.[8]

Even before the FTC decision, the Clinton administration forcefully called on companies to adopt stronger policies to protect user information: ''We must do more to uphold Americans' high expectations that their right to privacy will be

(*continued next page*)

Box 7.5 (*continued*)

protected online.''[9] On 1 May, President Clinton announced new legislative proposals to protect financial privacy.[10] Reflecting growing consumer concerns and citing technological advances that outpace measures to protect privacy online, the initiative would require companies to give customers a choice of whether or not firms can share sensitive information such as medical and financial data with third parties. While still endorsing industry self-regulatory efforts and not embracing the FTC recommendation, the administration has called for additional legal protections for certain sensitive information, warning that it would promote stronger legislation if industry's self-regulatory initiatives fail.

Taken together with other developments, including the proliferation of tough state privacy laws, these actions portend a move in the United States away from a self-regulatory approach toward increased government intervention. Even advocates of self-regulation recognize the shift in attitudes and are softening their opposition to greater federal oversight. In fact, concern for the proliferation of tough state privacy laws could actually encourage industry support for preemptive national privacy legislation.

While it is unlikely that Congress will enact the FTC proposal in 2000 due to the short legislative session and opposition from Republican lawmakers, it could lend support for strengthening the FTC's ability to fight fraud on the Internet.[11] Privacy concerns are registering high in political polls and focus groups, making it clear that policymakers will be forced to address the issue. With the growing consensus in the United States that industry self-regulation is inadequate, increasing government legislation is increasingly likely. But, at what cost?

---

1. Bob Tedeschi, ''Electronic Commerce Report,'' *New York Times*, 6 March 2000, and Chet Dembeck, ''Internet Self-regulation Dead on Arrival,'' *E-Commerce Times*, 31 March 2000.

2. See H.R. 4049 at http://thomas.loc.gov/cgi-bin/bdquery/z?d106:h.r.04049:

3. See Glenn Simpson, ''Electronic Commerce Firms Start to Rethink Opposition to Privacy Regulation as Abuses, Anger Rise,'' *Wall Street Journal*, 6 January 2000. The article cited a late 1999 *Wall Street Journal*/NBC News Poll in which Americans were given a list of eight concerns that might face them in the new century and were asked to rank them; 29 percent of respondents ranked the loss of personal privacy at the top.

4. *Ibid.*

5. See http://www.ftc.gov.

6. John Schwartz, ''FTC to Propose New Online Privacy Rules,'' *Washington Post*, 20 May 2000, E1, and Paul A. Greenberg & Chet Dembeck, ''FTC Seeking Net Privacy Regulation,'' *E-Commerce Times*, 22 May 2000.

7. FTC (2000). *Privacy Online: Fair Information Practices in the Electronic Marketplace* (2000 Report) (May). http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

8. *Ibid.*

9. Remarks by President Clinton to the Forum on Communications and Society on the Information Age Agenda, Meeting of the Aspen Institute, 3 March 2000.

10. ''The Clinton-Gore Plan to Enhance Consumers' Financial Privacy: Protecting Core Values in the Information Age,'' White House, 1 May 2000.

11. John Schwartz, ''Republicans Oppose Online Privacy Plans,'' *Washington Post*, 21 May 2000.

(95/46/EC), which required EU member states to enact laws prohibiting the transfer of personal data to nonmember states that fail to ensure ''adequate'' privacy protection.[31] The directive gives European consumers unprecedented control over the data collected about them and requires companies to get explicit permission from consumers before using personal data (Swire and Litan 1998). European countries are still passing laws to implement the directive, and questions about its enforceability persist.

What happens when the government-mandate approach to privacy protection butts up against the economic realities of the global marketplace? When the European Union passed the directive, it clearly implied a substantial economic effect from embargoing personal data from Europe to the United States if the European Union determined that US firms following the US approach did not provide adequate privacy protection (Dennis, *E-Commerce Times*, 6 April 2000). To prevent this outcome, the United States and European Union promptly began negotiations on how to bridge their different approaches.

The United States argued that US companies adhering to voluntary privacy guidelines should be given a ''safe harbor'' from legal challenge under the directive. Agreement was finally reached in March 2000 which assures the European Union that information sent by firms to the United States will be protected. The regulatory safe harbor arrangement includes principles, the effect of which is to allow American firms receiving personal data from the European Union to subscribe to self-regulatory organizations such as BBB*Online*, provide reports to a European data protection authority, and be subject to legal action by the US FTC if they do not adhere to the rules (Mitchener and Wessel, *Wall Street Journal*, 24 February 2000). The data privacy accord also allows Europeans to inspect and change data that is collected about them, and to veto any transfer to third parties (Simpson, *Wall Street Journal*, 15 March 2000). The 15 EU member states approved the agreement in May, and after European Parliament consideration in the summer, the agreement is expected to be formally adopted in fall 2000.

Despite the accord, the issue is not fully resolved. Key questions concerning compliance, enforceability, and the effect on firms outside the United States must still be addressed. The compromise has been criticized by both consumer and industry groups—for lessening protections Europeans are guaranteed by law, and for importing EU privacy standards into the United States. A new group, the National Business Coalition for E-Commerce and Privacy, has raised questions of national sovereignty and characterized the agreement as a kind of nontariff barrier (Dennis, *E-Commerce Times* 6 April 2000). The issue is likely to be revisited as part

31. See http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

of further negotiations with the European Union to address data privacy for the financial services sector.[32]

Nevertheless, the accord represents the start toward an interoperable approach to the problem of conflicting legal and regulatory systems. The workout leaves European privacy standards in place, but allows for private-sector trustmark assurance and enforcement under US laws and policies. Some analysts have predicted that the proposal may develop into rules of privacy that could be applied internationally (Burgess, *Washington Post*, 24 February 2000). The accord, something of a hybrid between the market and mandated approaches, possibly portends a merging of the two approaches in future treatment of e-commerce issues.

Market vs. Mandate: Is There a ''Right Way''?

Privacy protection represents one of the most contentious policy issues facing governments as they seek to balance the objective of promoting electronic commerce with citizens' desire for privacy. The problems will only get worse, as even more products—phones, TVs, cars—are connected to the Internet and the technology that enables data mining and profiling evolves.

How should governments balance these conflicting objectives? Does the comprehensive mandate model better protect privacy online? Or is the market approach combining laws and self-regulation preferable, since it preserves incentives for the private sector to continue to innovate for technologically superior solutions to satisfy government and consumer needs?

There is no right answer. Privacy involves sensitive individual values and, more broadly, how different societies perceive themselves. As discussed in chapter 2, privacy as an e-commerce issue is also marked by the difference in market power between those collecting information (industry) and those using the Internet (individuals), and perhaps also by an unsolvable divergence between social values and industry values. These market imperfections may mean an enhanced governmental role in setting privacy rules and either balancing interests or protecting Internet users.

Will a solution mandated by a government be worse economically than a solution that depends on market incentives? The economic ''theory of the second best'' shows that market and mandated solutions cannot be ranked by which comes closer to achieving the greatest economic well-being for a country as a whole. However, increased government intervention likely will mean less innovation by industry, and thus an Internet

32. US negotiators have argued that financial services should not be subject to the data privacy accord because specific legislation, the Financial Services Act, provides adequate protection. EU officials have not agreed. See *Inside US Trade*, 31 March 2000.

that might not satisfy user values as much as if government intervention was avoided.

On the other hand, increased government intervention may respond to important societal demands and there will be political pressure for intervention—although the cost to a country's development and engagement in electronic commerce should be fully acknowledged, as well as the potential for Balkanization of the Internet, which reduces network benefits for all. The key public policy question is less about the costs and benefits of different approaches than about how the threat to electronic commerce of government intervention can be managed and, hopefully, minimized.

The Role of Technology

Technology is both the cause of the problem and an important way to ameliorate it. Without question, the increasingly sophisticated means of collecting personal data exacerbates privacy issues. Yet technology also empowers individuals to make their own choices about how much privacy they demand.

When finalized this year, P3P, a specification being developed by W3C, will translate privacy statements on Web sites into machine-readable form. Users will then be able to specify the types of information they are willing to divulge, as well as whether the information can be shared with third parties. When a user visits a site that fails to meet the user's criteria, notice is given that allows users to block access. Thus privacy protections are being built into the on-line experience. Microsoft's announcement that it would include P3P in free Internet tools to be released in 2000 may go a long way in promoting its widespread use. Other approaches include W3C's Open Profiling Standard that allows users to determine what kind of information to reveal to Web sites. Widely available and inexpensive software programs like Guard Dog, Internet Junkbuster, Anonymizer, and others let users block sites from sending cookies.

Technology is not ''the'' answer to the privacy dilemma, but it is part of an effective industry response. It is a tool that allows individuals to make decisions based on their own preferences. ''P3P is not a panacea for privacy, but it does represent an important opportunity to make progress in building greater privacy protections in the Web experience'' (Center for Democracy and Technology 1999). Will governments accept technology as a sufficient solution, or will they argue that individuals need a champion?

A key component of the answer is education. Consumers need to understand the elements of their choices—in terms of both the technology available and industry self-regulation—in order to exercise their right to choose the protection they want. More information and public education,

as well as an expansion of self-regulatory practices like BBB*Online* and TRUSTe should be promoted.

There is obviously no one-size-fits-all policy appropriate for all governments. Countries adopt policies that reflect their own legal traditions, political culture, and economic status, especially as it relates to access to technology. At the same time, governments seeking to improve the environment for electronic commerce would be wise to limit their intervention by pursuing an approach that combines instruments, including legislation, government-private sector partnerships, industry self-regulation (with monitoring and enforcement), and the promotion of privacy-enhancing technology. The challenge for government is to get the mix right for both national traditions and technological realities. Intensified international efforts to promote interoperable approaches to privacy would be useful.

Consumer Protection

The Internet offers consumers unparalleled opportunities of choice and access and, with more than 304 million users expected to be online in 2000, the potential for new business is extraordinary.[33] However, in the borderless, anonymous world of the Internet, buyers and sellers interact across national borders, making fraud and deception even more challenging. For the promise of electronic commerce to be realized, buyers and sellers need to have confidence that products they buy and the firms they deal with are fairly represented, they will get what they pay for and be paid for what they sell, and that legal recourse is available if they do not.

Government has encouraged consumer confidence through laws and regulations to protect consumers against fraud in the physical world; adapting policies to the electronic world has become an increasingly important priority. Protection for consumers online to date has been an extension of national laws and regulations. New laws specifically directed to electronic commerce do not seem needed, and until they are, policymakers should resist the temptation to legislate e-commerce-specific solutions.

But with cross-border electronic commerce, consumers and businesses face the differing laws of numerous countries. While B2B transactions often choose the law that applies through contractual terms, using the country of origin's laws as the default, this is not likely to be satisfactory for consumer transactions. The disputes that arise from on-line consumer purchases are likely to be of relatively small dollar value, making it difficult and expensive to pursue legal action. Consumers need affordable and simple ways to resolve disputes.

---

33. US Department of Commerce, Digital Economy 2000. June 2000 at: http://www.esa.doc.gov/.

A fundamental problem faced by consumers in electronic transactions is the absence of clear information. On-line contracts need to state the basics: seller's identity and location, total price, payment and shipping arrangements, any conditions on purchases, including warranties and return/refund arrangements, and mechanisms for addressing complaints.

The electronic medium also makes fraud and deception (in contrast to honest mistakes) easier. Marketing messages that entice consumers into impulse buying, get-rich-quick schemes, and copycat (fake) Web sites make it difficult for consumers to differentiate between scam, fraud, and the real thing.

Overall, policymakers must decide how to provide simple and interoperable approaches to consumer protections without emasculating enforcement of national protections against fraud and deception. The first step is to acknowledge what common approaches already have been embraced, since these are the foundations for any necessary multilateral enforcement efforts. The next step is to determine whether differing approaches represent fundamental disagreement on societal values and how best to bridge such differences.

As with privacy protection, the OECD has been the primary international forum to discuss consumer protection issues. In December 1999, the OECD adopted the Guidelines for Consumer Protection in the Context of Electronic Commerce to ensure that consumers are no less protected when shopping online than when they buy in the physical world. Intended to help governments formulate and implement consumer protection policies, as well as to provide guidance to businesses and consumers on fair business practices, the guidelines represent an international consensus on core principles to govern the relationship between buyers and sellers in the electronic world.[34] Although nonbinding, they help guide governments to provide consumers with basic protections. The goal is to eliminate uncertainties for both consumers and businesses in trading online and to help clarify their rights and responsibilities. Work within the OECD is now directed at getting the guidelines implemented, and educating consumers and business of their rights and responsibilities, and on alternative dispute resolution mechanisms.

As discussed in the privacy section, the United States employs a market-oriented approach to consumer protection online—primarily by applying

34. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce is at http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines.htm. The guidelines reflect existing consumer protections. They also encourage private-sector initiatives that include consumer representatives and emphasize the need for cooperation among governments, businesses, and consumers. They address a broad range of issues, including advertising and marketing practices, information about an online business's identity, contracting terms and conditions, secure payment mechanisms, consumer redress and dispute resolution, privacy protection, and consumer and business education.

and enforcing existing laws, and by promoting self-regulatory initiatives. To back up the market, the FTC has devoted substantial new resources to consumer protection on the Internet, setting up a new office to oversee Internet transactions, electronic commerce, and advertising. Educating business and consumers in the ''rules of the road'' for electronic commerce has been a priority; the FTC has generated extensive information about on-line practices, such as pyramid schemes, lottery scams, Internet auctions, and medical billing schemes, as well as safe shopping guidance.[35] The FTC is also exploring the use of alternative dispute resolution mechanisms for consumer transactions online.

The FTC's main tool is the aggressive enforcement of existing consumer protection laws. In 1999, nearly 18,000 Internet consumer fraud complaints were submitted to the FTC. Since 1994, the FTC has brought over 100 Internet-related cases, stopping the illegal conduct in every case (FTC 1999). Enforcement has centered on technology-based scams such as spam, hijacking, and ''web cramming,'' as well as traditional scams—credit scams, and fraudulent auctions, business and investment opportunities, and health claims. In response to increasing allegations of internationally based Internet fraud, the FTC initiated an ambitious international project, in cooperation with law enforcement, governments, and consumer protection groups in 28 countries. As a result of a recent sweep of Web sites offering get-rich-quick schemes, the FTC put 1,600 sites on notice for alleged fraud (Clausing, *New York Times*, 13 March 2000). The action included participation by both public and private entities around the world. The Justice Department has also stepped up efforts to address Internet crime, launching the Internet Fraud Complaint Center in May 2000 (*E-Commerce Times*, 9 May 2000). The center will give consumers a place to lodge complaints and provide a centralized database to assist local, state, and federal law enforcement officials.

To address consumer protection issues, the European Union has released a Directive on Information Society Services, which includes electronic commerce, and clarifies the regulatory framework and safeguards the rights of consumers. The directive harmonizes rules to ensure that industry and citizens can supply and receive electronic commerce throughout the European Union. It builds on existing European Union rules for consumer protection, which cover contracts, electronic transactions, unfair terms in consumer contracts, misleading advertising, and consumer credit (European Union 29 February 2000).

Beyond governments, businesses, and consumers there are other ''players.'' For example, consumer advocates from Europe and the United States, through the Transatlantic Consumer Dialogue, have recommended standards to give protection in the on-line world that matches protection

35. See http://www.ftc.gov/bcp/menu-Internet.htm.

in the off-line world. These standards include simplified contracts, limits on consumer liability, recourse to laws and courts in home countries, and cooperation among governments in support of legal redress (Transatlantic Consumer Dialogue 1999).

Regulatory bodies in most countries appear to have adequate authority to address fraudulent and deceptive practices online; enforcement of those laws for Internet-related issues will go a long way to reassuring consumers that protections do exist in the electronic world. Moreover, greater efforts by businesses to develop and adhere to self-regulatory guidelines and codes will also help address consumer concerns.

To the extent that self-regulatory approaches to consumer protection are deemed inadequate, however, governments will come under pressure to adopt new policies to fill the perceived regulatory void. Consumers must believe that they are afforded an equivalent level of protection as is available in traditional forms of commerce. Striking the appropriate balance between governmental intervention and self-regulation will remain a challenge for governments. Enhanced education of consumers, as well as development of new processes for alternative dispute resolution for on-line consumer transactions can help create an environment of greater confidence for consumers.

Content

While most governments support the free flow of information across national borders, the growth of electronic commerce has forced them to examine issues related to Internet content. Along with the many benefits of the Internet come the potential for it to carry unlawful and offensive activity. Child pornography, fraud, gambling, and material fomenting racism, hate crimes, violence, or other illegal activities are examples of the harmful or offensive content now readily accessible. Governments are increasingly challenged to try to strike a balance between limiting the use of the Internet for purposes contrary to societal values and security on the one hand, and freedom of expression on the other. Moreover, how or whether to mesh policy approaches across borders is an issue.

For most countries, existing laws that ban fraud or child pornography or those that regulate gambling, firearms, alcohol, or intellectual property seem sufficient. The US Justice Department in its new report, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, found that, for the most part, existing laws are adequate to address unlawful activity on the Internet (US Department of Justice 2000). (See box 7.6.)

The European Union has an ambitious action plan to promote safer use of the Internet by combating illegal and harmful content (European Parliament 1999). The objectives of the four-year plan are to encourage industry and users to put in place systems of self-regulation, create filter-

Box 7.6 Legislating safe surfing for children: The US approach

The United States has made two attempts to legislate an approach to content objectionable to children.[1] The Children's Online Privacy Protection Act (COPPA), which took effect 21 April 2000, authorizes the FTC to set rules regulating data collection on Web sites targeted at children under the age of 13. Web-sites must notify parents of the site's information practices, obtain verifiable parental consent before collecting personal information on children, and give parents a choice as to whether their child's information will be disclosed to third parties.[2]

Not only does COPPA run the risk of court cases based on free speech, it also has direct economic implications. It is estimated that COPPA requirements will cost firms between $60,000 to $100,000 a year, leading a number of Internet companies to eliminate services to children under 13 rather than risk lawsuits (*Wall Street Journal,* 24 April 2000).

In addition to legislation, the United States has promoted a self-regulatory, local approach to content by empowering parents and teachers with the tools to protect children in a manner consistent with their values. The United States embraced this approach as the most effective and most compatible with the First Amendment; government and businesses have worked closely to give parents resources to promote safe online experiences for children.[3]

For example, the primary way citizens, especially parents, have addressed the content problem is through software that blocks or filters content deemed offensive or inappropriate. Software programs such as CYBERsitter and Net Nanny block access to Web sites based on certain words or phrases; filtering software, available through many ISPs, block sites containing certain keywords or sites with a particular label or rating. In addition, there are services like SafeSurf and RSACi that allow publishers to self-label, thereby allowing Web sites to be blocked based on their own ratings.

1. The Communications Decency Act to limit obscene material on the Internet was struck down by the Supreme Court in 1997 as infringing on free speech, and therefore, ruled unconstitutional. *Reno v. ACLU.*

2. See http://www.ftc.gov/kidsprivacy.

3. See http://www.GetNetWise.org.

ing and rating systems, promote awareness, and encourage coordination and compatibility between European and other approaches. European firms have formed the coalition INCORE, the Internet Content Rating for Europe, to promote self-regulation and create a rating and filtering system to meet the needs of European users.[36]

The OECD addressed the issue in 1998 through a Forum on Internet Content Self-Regulation, jointly sponsored with the Business and Industry Advisory Committee to the OECD, as well as in an inventory of national approaches to content on the Internet. In addition, W3C has set specifica-

36. See http://www.incore.org/what/what.htm.

tions for an Internet rating system known as Platform for Internet Content Selection (PICS), providing both self-labeling (by author or publisher) and third-party labeling, as well as accommodating a range of rating systems available to different countries and cultures.[37]

Industry has embraced technological solutions empowering users to control their own access to content as a way to forestall government regulation. In late 1999, the Bertelsmann Foundation, a nonprofit group associated with the German media conglomerate Bertelsmann A.G., unveiled recommendations for a global system that would include codes of conducts and rating systems that, among other purposes, parents can use with filtering software to protect children from harmful material online.[38]

The plan and the growing support for rating and filtering systems generally have raised serious concerns among civil libertarians and others that content filtering will lead to censorship. Groups like the American Civil Liberties Union and the Electronic Privacy Information Center fear that such systems threaten free expression on the Internet more effectively than national laws could. In some countries (including the UK and Australia), governments are already trying to mandate the use of PICS-facilitated systems, with penalties for companies that rate themselves incorrectly.

The same technologies that allow parents to filter information also allow government officials to embargo sensitive or subversive information. The Chinese government screens for politically sensitive words and has implemented regulations to control citizens' access to the Internet. New rules issued in January 2000 and designed to prevent the spread of ''state secrets'' via the Internet, are seen as a clear attempt to censor on-line content (Dembeck 2000). Moreover, ISPs operating in China can be held accountable for illicit material on the Internet, which is something that has happened in other countries as well.[39]

In Syria, before becoming president, Bashar Assad had been promoting Syria's advancement into the electronic world but said that local traditions may require ''guidelines'' for deciding if there should be controls on Internet access (Schneider 2000). Vietnam has announced its intention to control the Internet for security and cultural reasons, and the country's

37. See http://www.w3.org/PICS/Activity.

38. ''Memorandum on Self-Regulation of the Internet'' located at: http://www.stiftung.bertelsmann.de/Internetcontent/english/frameset_nojs.htm.

39. China is not the only country to hold ISPs liable for content on their servers. Liability concerns among ISPs have been growing, as some countries (UK) have sought to prosecute ISPs for distributing harmful content, with the end-result being closer cooperation with law enforcement, and adoption of self-regulatory plans. Germany, too, threatened to hold an AOL executive responsible for material in AOL chat room.

Ministry of Culture and Information plans to monitor on-line content.[40] In Malaysia, while ISPs are not required to monitor the Internet, they must limit public access to 100 high-impact pornographic sites identified by the government, as a statement of societal values.[41] And in March 2000, Zimbabwean President Robert Mugabe got a special bill through Parliament allowing government access to and control over e-mail content (Internet News South Africa, 24 March 2000).

Content on the Internet raises many of the same issues as the protection of privacy rights. Both entail individual and societal values. As with privacy, technology provides part of an effective government response and empowers individuals to make choices. Notwithstanding censorship concerns, governments and businesses worldwide will continue to embrace the use of technology as a large part of the answer to the problem of sexually explicit material on the Internet. Unlike with privacy, however, it appears that the content issue currently is being successfully managed at the national level, though with the potential that differing national approaches will lead to conflicts, possibly even trade barriers. Greater discussion and cooperation in national approaches to content are helpful in preventing differences from becoming significant barriers to electronic commerce.

40. The Internet Law and Policy Forum Working Group on Content Blocking at http://www.ilpf.org/work/content/htm.

41. See the Web site of the Singapore Government, Frequently Asked Questions for E-Commerce Business Policy, at http://www.ec.gov.sg/13081999/helpdesk_faq.html.