Ralf Bendrath, Jeanette Hofmann, Volker Leib, Peter Mayer, and Michael Zürn (i.E.), "Governing the Internet: The Quest for Legitimate and Effective Rules", in: Achim Hurrelmann, Stephan Leibfried, Kerstin Martens, and Peter Mayer (Hg.) Transforming the Golden Age Nation State, Palgrave: Houndmills.

## Chapter 7

**Ralf Bendrath, Jeanette Hofmann, Volker Leib, Peter Mayer, and Michael Zürn**

# Governing the Internet: The Quest for Legitimate and Effective Rules

## Introduction

More than anything else, the Internet has become a symbol of globalization. Emerging from military and academic efforts in the U.S. to create a highly robust communication system, the Internet is a huge 'network of networks' that links an ever growing number of computers all over the world and enables the simultaneous and instantaneous flow of immense amounts of information both within and across countries. Through its support of applications and services such as the World-Wide Web (WWW) or electronic mail, the 'Net' has dramatically reduced transactions costs for organizations, groups, and individuals situated in different parts of the world. Thus, it has contributed heavily to the unprecedented growth of transborder economic, social, political, and cultural interactions that has taken place in recent years. Indeed, the seemingly de-territorialized 'cyberspace' spanned by the Internet, in which ideas are supposed to travel freely with no regard for state borders, has often been celebrated – or deplored – as a powerful repudiation of sovereignty-based claims to social control.

In this chapter, we look at how political actors have responded to challenges posed by the Internet. The most important of those actors is the modern (Western) nation state, which until recently controlled most of the policies that are challenged by the rise of the Internet. This state provided its citizens with a set of *normative goods* of supreme social importance, including peace and physical security, liberty and legal equality, democratic self-determination, and economic growth and social welfare. Our goal is to examine the claim that this state is undergoing a far-reaching transformation, possibly indicating the transition from the familiar 'national constellation' to a not yet well understood 'postnational constellation' (Habermas 2001). The suggested transformation has at least two dimensions: First, there are instances in which – previously state-held – responsibilities for securing these normative goods are *internationalized*, *privatized*, or, if both processes are intertwined, *transnationalized*. Second, in such processes different *levels* of responsibility are potentially affected: the state may be complemented or supplanted by other public or private organizations with respect to (a) decision making, legislation, and oversight (*regulatory responsibility*), (b) the implementation of decisions and the immediate provision of services (*operational responsibility*), or even (c) its socially acknowledged right and duty to step in and take regulatory or operational action if one or several of the normative goods are at jeopardy (*outcome responsibility*). In addition, changes in these dimensions may either involve diminishing the role of the state, that is, public and national responsibilities are lost or *shift* to non-state actors; or the assumption by other organizations of state-like responsibilities may leave the state's powers and range of activities in a given area largely unaffected, that is statehood is not redistributed according to a zero-sum logic but *diffuses* beyond the state.

On the following pages, we analyze transformations of the state by looking at three policy fields either closely connected to, or deeply affected by, the Internet: (1) the administration of

the Domain-Name System (DNS) necessary for retrieving information and transmitting messages within the network, (2) the protection of informational privacy, and (3) the taxation of transborder business activities. For each case we ask whether, to what extent, and how the emergence and spread of the Internet, particularly since its popularization and commercialization in the 1990s, have spawned or reinforced a transformation of statehood in terms of the shift or diffusion of (previously) public and national responsibilities along either 'spatial' (internationalization) or 'organizational' (privatization) lines or both. The normative goods at stake in our cases vary; however, we are especially concerned in this chapter with a normative good that is involved in all three policy fields: *democratic legitimacy*. From the point of view of democracy, the Internet has given rise to ambivalent expectations: on the one hand, by virtue of its role as a key driver of globalization in recent years, the Internet is seen as contributing to the weakening of democracy by reinforcing the *incongruence* between the regional or global extension of social interactions and the national scope of democratically legitimized political decision making. On the other hand, the Internet has been acclaimed by many as a potentially crucial device for revitalizing and deepening democratic self-determination both within and across nations. We therefore ask, with respect to the three policy fields, how (if at all) the issue-specific transformations of statehood that we observe affect the normative good of democratic legitimacy. Which legitimacy problems arise and who takes care of them? Does the political responsibility for the provision of democratic legitimacy still rest exclusively with the state?[1] Which part does the Internet have in all that?

[1] Obviously, it is the *people* who grant or deny legitimacy to the state; at the same time, the state may have the socially acknowledged and legally enshrined obligation to provide for the institutions (e.g. elections) which enable the people to exert their right to democratic self-determination. It is in this sense that we talk of the 'Golden Age' nation state's responsibility for the provision of the normative good of democratic legitimacy.

In looking at these issues, we focus on four criteria which figure prominently in debates about the 'democratic deficit' of global governance, that is *congruence* between social and political spaces, *transparency* of decision making, *accountability* of decision-makers to stakeholders, and *participation* by stakeholders in decision making.

## The Administration of Internet Names and Numbers: Global Reach of Regulatory Authority under Unilateral Supervision

Communication services such as telephony or mail require universal addressing systems in order to work. Addressing systems are sets of globally standardized attributes like city codes or house numbers which permit messages to reach their destination. Addresses fulfill two functions, they determine the topological position of a communication device (localizing function), and they provide for a unique identity (naming function). Usually, each communication service comes with its own addressing system, and the introduction of a new service will call for a new addressing convention. Accordingly, the emergence of digital data networking in the 1970s created the need for a new address space that would provide users and services worldwide with unique digital identifiers.

### National versus Global Regulation of Address Spaces

Before the deregulation of postal and telecommunication services in the late 1980s and 1990s, address spaces formed an integral part of state-run communication services. Telecommunication networks were typically operated as public monopolies with a few selected firms as technical suppliers. This 'ancient regime' (Drake 1994) attributed all three levels of responsibility – for outcomes, rules, and operations – to national governments. Incompatible technical standards ensured that both technical infrastructure and services were

shielded from international competition. The international telecommunication infrastructure was characterized by fragmentation, and international standard setting efforts focused on specifying gateways between autonomous, national networks. National sovereignty formed the constitutive principle of international collaboration. The International Telecommunication Union (ITU), a UN agency, based its decisions on the ‘one nation, one vote’ rule. Participation by companies and non-state experts depended on their government’s authorization. Agreements could only be achieved through consensus; countries could not be forced to adopt standards. The sovereignty-based regime slowly faded in the OECD world in the 1990s, but some of its characteristics have persisted. The telephone system’s number spaces, for example, are still kept under state regulatory responsibility.

The onset of data networking not only created the need for a new addressing system, it also brought about new design options, which suggested a departure from the traditional model. It is noteworthy that the Internet’s addressing system consists of two parts, numeric addresses and the more user-friendly domain names (for example: www.uni-bremen.de), which keep the numeric addresses (in this case 134.102.20.226) hidden from users. The Domain Name System (DNS) differs in several ways from traditional forms of addressing. Most relevant in this context, is that the DNS constituted a global (single, unified) name space from the beginning. The Internet name space does not consist of autonomous, national addressing systems like the telephone network, which subsequently are connected to allow for international calls. Even the reference to the territorial nation state contained in country code Top Level Domains such as ‘.de’ is merely symbolic.

The name space is organized as a tree shaped hierarchy. The tip of the hierarchy consists of the ‘root’, the authoritative source from which all Internet users, directly or indirectly, retrieve

information on the location of a given website or mailbox. The root thus constitutes a central point of control of the DNS. While the territorial telecommunication regime allocated operational and regulatory responsibility on the national level, the DNS organizes oversight over the root as a central task to be performed *by one single agency*. In the telecommunication world of the past, global connectivity was reached through bilateral contracts between national PTTs (Postal, Telegraph, and Telephone Organization). On the Internet, it is the distribution of the authoritative 'root zone file' that provides for global reach of a specific service.

The DNS root was initially administrated by a single person, the Californian computer scientist Jon Postel. The funding of the so-called 'Internet Assigned Numbers Authority' (IANA) initiated and headed by Postel came from the U.S. Department of Defense. In the mid-1990s, after the privatization and commercialization of the Internet infrastructure, this informal arrangement reached its limits. Pressing problems such as escalating speculation with domain names, property rights conflicts over famous names, and monopoly profits from skyrocketing domain name registrations made it clear that the DNS needed a more formal regulatory framework. The institutional foundation for the present name space administration was laid in 1998. The U.S. government acknowledged the 'Internet Corporation for Assigned Names and Numbers' (ICANN) – a private not-for-profit company based on Californian law, but internationally composed – through a Memorandum of Understanding (MoU). The MoU was initially limited to a period of two years after which a full privatization of DNS administration was to take place. This was, however, on the condition of ICANN accomplishing several tasks as specified in the MoU: privatizing domain name registration, forming contract-based relationships with various DNS operators, and last but not least developing a legitimate process of decision making.

Two years after its inception, ICANN initiated a first reform process because the bottom-up process of policy making in the spirit of private self-governance had proven more difficult than expected. Many key actors such as the operators of root servers (which enable computers worldwide to exchange information with other computers in the network) refused to contract with ICANN in order to preserve their regulatory autonomy. To date, ICANN has still not fully succeeded in establishing a contract-based regulatory authority over the Internet's name space, and in October 2006, the U.S. Government has amended the MoU for the seventh time.

**Spatial and Organizational Transformations of Statehood in Telecommunication Policy**

Reviewing telecommunication infrastructures over the last 30 years, we observe major changes, particularly in the spatial dimension of addressing systems, which refers to the level (local, national, international etc.) at which decisions are made and implemented. The poly-central, sovereignty-based address space interconnected through multi- and bilateral agreements typical of the 'ancient regime' was dismissed as a model for digital data networking and replaced by a global structure with just one point of control at the tip of its hierarchy. The Internet thus involves a shift of political responsibility away from the national constellation – it is not territorially confined nation states that control the infrastructure, but one government (the United States) which holds supervisory authority over a globally acting organization (ICANN). With regard to the organizational dimension, however, the degree of transformation is less clear since the precise role of private and public actors in Internet governance is still a contested issue both in the U.S. and in intergovernmental forums.

The root, the authoritative heart of the Internet's name space, is subject to regulatory responsibility of the U.S. government, which also claims outcome responsibility. All other governments are relegated to a mere advisory role vis-à-vis ICANN. Regulatory responsibility thus has indeed shifted but not quite in the assumed way. Instead of the heralded complete privatization, we have witnessed the transition from a partly national, partly intergovernmental arrangement to a *unilateral regime* which works through a private organization.[2] Steps towards private, transnational self-governance have been taken with regard to policy development and the implementation of one section of the name space, the so-called generic Top Level Domains such as '.com' or '.org'. (In addition, some of the national registries entrusted with managing the country code Top Level Domains are private entities.) Yet, ICANN, the private agency supervising the generic Domain Name space, remains itself under tight supervision by the U.S. government (Goldsmith and Wu 2006: 169). Whereas the spatial shift of digital addressing towards a global system seems to some extent irrevocable, the degree of organizational transformation remains up to negotiation and therefore somewhat instable.

**Legitimacy of Transnational Regulation under U.S. Control**

Around the time ICANN was founded, state-centered forms of legitimacy were widely dismissed as inadequate for administrating the Internet infrastructure (for a critical account see Lessig 1998). Private forms of regulation with provisions for direct participation by

[2] Note, however, that not all regulatory functions related to the DNS are centralized. The country code Top Level Domains, while in principle dependent on the central root zone file, are operated and administered more or less autonomously on the national level, notwithstanding ICANN's Internet-wide authority claims.

stakeholders promised to be more efficient and legitimate than ‘closed’ intergovernmental regimes. The ambitious goal in those years was to compensate the demise of nation state-based legitimacy by creating a bottom-up policy process, which would involve all affected parties present on the Internet, including individual users. It was expected that self-governance by the private sector and civil society would provide for greater transparency in decision making and presumably also for more user-friendly policies than sovereignty-based arrangements. The belief in the superiority of private regulation of the Internet was shared by a coalition of liberalization oriented governments, the Internet industry, and interested users (Mueller 2002).

While the U.S. government claimed authority to define the basic mechanisms for ensuring the legitimacy of the governing arrangement for the Internet’s name space, the task of implementation, in other words the operational responsibility, was delegated to ICANN. Reflecting the MoU between the US-Government and ICANN, the latter’s original bylaws stipulated that nearly half of its board seats would be filled with individual users while the remaining seats would represent various operative functions of the Internet’s address spaces. Governments and international organizations were to participate in a mere consultative capacity through a Governmental Advisory Council. The one exception has been the U.S. government, which arranged for itself a special supervisory function to be held until the privatization of the DNS administration.

ICANN’s tasks included the creation of a membership mechanism that would represent ‘the global and functional diversity of Internet users and their needs and at the same time ensure accountability (DOC 1998). To that end, in the year 2000, ICANN set up a global organization for individual users, the so-called ‘At-Large Membership’, and initiated the first

global online elections for five seats of the ICANN board (rather than nine as originally stipulated). However, the legitimatizing impact of the participation of Internet users and online elections on the (semi-)private governance arrangement proved to be a contested issue. On the grounds that users from a few countries had dominated the elections, a majority of the ICANN board and ICANN administration dismissed elections as a mechanism for representing geographic and functional diversity on the Internet. Still in 2000, in the course of ICANN's organizational reform, the ICANN board discarded the concept of a balanced board representation between industry stakeholders and individual users. The ICANN administration's vision of 'ICANN 2.0' was a public-private partnership that would acknowledge and involve in a decision making capacity governments as true representatives of the public interest.

The idea of a public-private partnership and its failure – governments rejected the offer to share operative responsibility with the private sector – demonstrate some of the dilemmas involved in achieving legitimacy in a transnational setting. The shift of regulatory responsibility from the national and international level to a global private authority (albeit under unilateral state supervision) reopens basic questions of democratic legitimacy which had been settled with the consolidated nation state. These questions concern the design of transparent and accountable procedures but also the adequate definition of the boundaries of the new constituency – who should have a say in the regulation of the Internet's address space and who shouldn't? To date, ICANN still struggles for legitimacy. Practically all developing countries criticize the violation of the principle of sovereignty inherent in the centralized governing arrangement of the Internet. Accordingly, the violation of this fundamental principle of the national constellation undermines the democratic notion of self-determination. The Internet stakeholders, on the other hand, keep complaining about intransparent and

inefficient procedures. As long as ICANN remains subject to U.S. government control, the outcome responsibility for its overall performance including its legitimacy will also rest with the U.S. government, although some ambiguity remains in this regard which may be typical for transnational arrangements under state control.

## The Emergence of a Hybrid Global Privacy Regime

The regulatory idea of protecting citizens' privacy was originally formed with a view to unreasonable police searches of private property, but soon extended to the control of *information about persons* in the hands of governments and private entities (Warren and Brandeis 1890). In 1948 the right to privacy was internationally codified in the Universal Declaration of Human Rights (Art. 12). The idea of 'data protection' in the more narrow sense emerged with the spread of automated data processing in the 1960s. Not only were computers used to store and retrieve vast amounts of personal data, they were also able to correlate, evaluate, and sort them – which in the end came down to sorting persons (Lyon 2003). Although emphasizing different means, both American 'informational privacy' and European 'data protection' policies share the fundamental goal to ensure that individuals know about, and can control, which computer-processed information others have about them. With the growth of transnational trade, the regional integration of markets, and the emergence of multinational corporations, a second, derivative goal became an integral part of data protection efforts: permitting the flow of personal data across multiple jurisdictions, while preserving the protection level for individuals.

Since the first data protection law was enacted in the German Land of Hesse in 1970, data protection legislation has spread around the world, mostly through policy emulation and

diffusion (Bennett 1998). In the ‘Golden Age’ of the nation state, the overall regulatory model was state-interventionist and closely linked to the specific technical structure of the problem. Computers in the 1960 and 1970s were mainframes in the hands of huge bureaucracies or corporations, and the regulatory model applied was direct government oversight and intervention using instruments such as registration or licensing mechanisms for databases or access controls. While in Europe all processing of personal data was regulated, U.S. privacy regulation only applied to governmental agencies. Moreover, in the American model there was no counterpart to the European data protection commissioner (an independent public oversight body); instead, courts were relied upon for individual enforcement.

Outcome responsibility for data protection resided with the nation state. Some European countries reacted to this expectation by even including clauses in their constitutions to ensure the privacy rights of citizens, and national courts were the last resort for their enforcement. Regulatory responsibility – the competence to make more concrete rules for the protection of data – was also borne by the state, although international harmonization efforts, in particular the 1980 OECD Guidelines and the 1981 Council of Europe Convention, foreshadowed a process of internationalization, which culminated in the EU’s 1995 Data Protection Directive. Operational responsibility in the early years was held by governmental regulatory authorities. Meanwhile, the German institution of the corporate data protection commissioner (or chief privacy officer) has spread across the globe, giving significant operational responsibility to the private sector itself.

**New Challenges in Protecting Online Privacy and the Transformation of the Global Privacy Regime**

When the personal computer hit the market in the mid-1980s, the use and processing of all kinds of data – including personal data – was already growing beyond the reach of effective government oversight. This was aggravated with the advent of the Internet as a mass medium in the 1990s, when the number, diversity, and options of data-collecting agents increased dramatically. The types of information collected were no longer restricted to *transactional* data, such as data accruing with purchases or other business exchanges (credit card numbers, delivery addresses, and so on). In addition, users' online *behavioral* data (websites visited, search keywords used, etc.) could be automatically collected through web servers even without users completing any forms. Specialized customer profiling and advertising companies were able to aggregate user data across several websites and develop fine-grained profiles.

The Internet also made it difficult to apply and enforce national data protection laws. Transnational transfer of personal data between corporations became a matter of seconds now. And it was not clear anymore which law should apply when a European citizen entered his personal data into a website hosted in the United States. If the local PC of the user were regarded the locus of data processing, encompassing European data protection legislation would apply. If the web server were considered the machine where the data collection takes place, the data would only be subject to private sector self-regulation in the United States.

The Internet breakthrough coincided with the adoption of the 1995 EU Data Protection Directive, whose third-party rules helped to create some dynamic in the United States and eventually in Europe as well. The EU Commission now could issue 'inadequacy' ratings about countries which lacked comprehensive data protection legislation, thereby prohibiting the transfer of personal data from within the internal market to these countries. Since the U.S.

lacked an omnibus privacy act, the Clinton administration feared that American companies might be locked out of the European market for e-commerce. After protracted negotiations, the EU Commission and the U.S. Department of Commerce in July 2000 sealed a ‘Safe Harbor’ agreement (Farrell 2003; Heisenberg 2005). This accord links the two regions’ regulatory approaches – the European, law-based and comprehensive privacy regulation and the American, private sector-based and sectoral model – by making companies rather than countries the object of ‘adequacy’ rating. As a result, the U.S. could keep its data processing industry unregulated by law, and the EU could allow data transfers to American companies provided they subjected themselves to the Safe Harbor principles. Containing regulations on notice, choice, onward transfer, security, data integrity, access, and enforcement, these principles roughly mirror the international consensus on fair information and data protection goals and procedures.

In the course of transatlantic negotiations, EU data protection officials came to appreciate the self-regulatory instruments developed in the United States, which since have gained more acceptance in Europe as well (Farrell 2003). In recent years, a number of industry associations have developed privacy ‘codes of conduct’, and many of them now award ‘privacy seals’ to websites that publicly declare their adherence to a specific data protection standard. Other approaches include privacy contract clauses on personal data flows in transnational business networks. Most of these private governance instruments were introduced on the national level and subsequently transnationalized. Some privacy web seals developed in the United States for a Safe Harbor adequacy rating are now used in East Asia and elsewhere. The latest development is the practice of embedding in a legal framework and certifying by public authorities privacy codes of conduct that were established by business associations. The EU directive mentions this option, but regards it as an exception. Since the Safe Harbor

breakthrough, however, European data protection commissioners have turned to actively promoting this form of public-private collaboration in data protection.

**The Organizational and Spatial Diffusion of Privacy Protection**

The emerging global or at least OECD-wide regulatory arrangement is a transnational-intergovernmental combination of the European law-based and comprehensive data protection regulation and the American self-regulatory approach. Outcome responsibility still seems to reside with the nation state, although the European Union legally took over this function from its members in 1995. In contrast with the 'Golden Age', regulatory responsibility is now organized in a multi-layered, hybrid way. Minimal privacy protection levels are defined internationally, the most important documents being the EU directive and the EU-U.S.-Safe Harbor agreement. But whereas public regulation differs along territorial lines (nation, Europe, OECD), private self-regulatory instruments apply to companies or branches and tend to ignore geography, thus making for global regulation within organizational or sectoral limits: DaimlerChrysler's binding corporate rules for privacy are valid all over the world, yet apply only to the corporation's employees and subcontractors. Operational responsibility is now by default organized through chief privacy officers. They are supplemented by privately organized certification and seal schemes, which have established their own compliance and arbitration mechanisms and only to a lesser extent rely on public oversight authorities or courts.

Altogether, we find a significant growth in importance of transnational mechanisms in the regulation and operation of privacy protection. It is not a complete takeover, though, as the self-governance of privacy continues to take place within national or supranational legal

frameworks – privacy laws or laws against unfair and deceptive trade practices – and within a network of international rules that defines minimal levels of protection. The emerging global privacy regime is decentralized, heterogeneous, and multi-facetted, with the EU directive as its legal core and the Safe Harbor agreement as the dominant model of hybrid regulatory patterns. The general picture is therefore one of a diffusion of statehood in privacy protection, although within the EU responsibilities have partially shifted from the national to the supranational level.

**The Legitimacy of the New Regime**

The emerging global privacy regime faces three kinds of legitimacy problems, all of which have been addressed in different ways and by different actors. The first is typical for international policy-making. International harmonization generally limits the accountability of the governmental rule-makers to their societies through prolonged chains of representation as well as reduced transparency. The Internet helped address this problem by making new forms of transparency and stakeholder participation possible. Drafts of official regulatory instruments are now routinely being made available online, and the EU, the OECD, or the Council of Europe regularly conduct online consultations in this policy field. Interestingly, international organizations seem to be more strongly motivated to provide for transparency and stakeholder inclusion than national governments. They have started online consultations much earlier, their policy development processes are generally more comprehensively documented online than on the national level, and they sometimes actively reach out to civil society groups. This may be taken as an indication that international organizations see the need to compensate for their ‘distance’ to the ordinary citizen and to some extent assume

responsibility for securing or enhancing the democratic legitimacy of international policy-making (see Steffek in this volume).

The second legitimacy problem stems from the privatization of former public duties. The private sector privacy instruments are developed by business associations, service providers, or technology vendors, which are neither transparent in their work nor accountable to the public. While some of these forums have recently seen an involvement of privacy advocacy groups, most are closed shops, accessible only to a small number of insiders and experts. Governments and public data protection authorities respond by mandating minimal privacy thresholds for the private instruments, be they technical solutions, codes of conduct, or contractual clauses. They do not take steps to ensure greater transparency, accountability, or participation in these forums. Nor do they seize full operational or regulatory responsibility again, thus (re-)subjecting privacy protection to the state's democratic, parliamentary process. Nor do other actors assume a responsibility for tackling this 'democratic deficit', which may indicate that privacy protection is a policy field in which 'output legitimacy' (effectiveness) dominates 'input legitimacy' (democratic decision making).

The third legitimacy problem is concerned with the congruence of rule-makers and ruled. Because of the EU's market power, its rules on data transfers to third countries have become the de facto standard for global privacy governance. Other countries face high costs if they ignore the regulations developed in Brussels and put in place rules of their own choosing. Insofar their autonomy is restricted. Some have therefore openly questioned the legitimacy of the EU rules. The Australian government, for example, protested that there was 'no need for any externally-imposed test of 'adequacy' (McGinness 2003). Asian countries have developed regional privacy guidelines in the APEC framework, which are considered more

corresponding to the ‘Asian way’ based on encouragement, voluntary mechanisms and no legal obligations (Greenleaf 2005). While this has enhanced regional congruence and therefore legitimacy, it may be short-lived. The countries will still have to adapt to the EU rules if they want to tap into the growing market of e-outsourcing, including e.g. call centers and other processing of customer data.

The global development of privacy governance takes place in this interplay of regional and global as well as public and private mechanisms. Its legitimacy is challenged, but the relevant public bodies – foremost international organizations – are trying to secure it in new ways. The Internet is helpful for ensuring transparency and public participation here.

## Electronic Commerce and the Transformation of the International Tax Regime

Taxes are the most important resource for the nation state to fulfill its functions. Because taxation means expropriation for the common good, tax rules require high legitimacy. It is hard enough for state authorities to perform their duty to collect taxes in a single territory. Additional difficulties arise whenever two or more countries are involved in the taxation of multinational firms: conflicts are bound to arise about which portion of the profit was produced – and hence is taxable – in which state. The globalization of the economy aggravates the problem that several states may claim the right to levy taxes on the same income. Furthermore, there are different principles of taxation that collide unless they are brought into line by a joint effort. The ‘residence principle’ aims at the place where a company has its domicile (identification of which may be controversial as well), whereas the ‘source principle’ targets the place where income is created. If states do not coordinate the liability to pay taxes and the principles they apply, double taxation or non-taxation result.

Both damage the legitimacy of the tax state. Therefore, the aim of international tax coordination is to grip taxpayers' money only once and to assign the tax base to the respective states according to mutually agreed rules.

Up to the 1970s, the tax state enjoyed a 'Golden Age'. Fiscal sovereignty was extensive, tax systems were nationally confined, and firms resided in their mother country. Alongside effective national tax systems, an international tax regime, which placed no formal constraints on states' tax policies, had slowly emerged. In the 1920s the League of Nations promoted the idea of a multilateral treaty against double taxation and tax evasion. Member states, however, wanted to keep their fiscal sovereignty and thus settled for a non-binding document. This 'Model Convention', which was published in 1928, contained draft models for bilateral tax treaties between states. After the Second World War the OECD continued the task and published a new Model Tax Convention in 1963, accompanied by a comprehensive Commentary. Thus, the basic architecture of international taxation – a multilateral convention and many bilateral treaties – was confirmed. It is still in place today. The dominant role of national fiscal authorities notwithstanding, the institutionalization of the international tax regime has progressed, and the OECD's Committee on Fiscal Affairs has become the most prominent multilateral forum for international tax policy matters (Rixen and Rohlfing 2005). Participation has widened to non-OECD member countries and to the private sector, which is represented in the Business and Industry Advisory Committee (BIAC). In addition, the International Fiscal Association, a distinguished global organization of tax experts, maintains close contact to the OECD. The Model Tax Convention and the Commentary serve as a standard and are recognized by the whole tax community including courts. The network of bilateral double taxation agreements has become more and more dense. Normally, the negotiators of an agreement adopt the Convention's text verbatim and add some extra articles.

Thus, the OECD Model Tax Convention provides a ‘focal point’ for the agreements but leaves control at the national level. (Tax policy within the EU is subject to integration and requires separate consideration, see Uhl in this volume).

**The Challenge of the Internet and the Adaptation of the International Tax Regime**

The Internet came as a threat to the tax state. The prerequisites of taxation – reviewable transactions, identification of involved parties, and the nexus to a territory – were put into question by myriads of transborder data flows. The dispersed and ubiquitous network of networks undermined the existing system of territorially confined tax jurisdictions. Governments feared big tax losses in view of the opportunities of doing business in cyberspace. The Internet multiplied the options for legal tax planning and illegal tax fraud. Tax administrators worried about the possibility of e-commerce being carried out from tax havens depriving industrial countries of a large part of their financial resources.

With hindsight, the years from 1995 to 1997 appear as a phase of uncertainty, speculation, and learning how to come to grips with the Net. It was unclear whether current tax systems could cover the electronic business models or new taxes like the ‘bit tax’ on data transfers were needed. While several national task forces were trying to figure out the Internet’s effect on taxation, governments refrained from taking legislative action. The aim was to reach an international consensus on taxation of e-commerce *before* mutually contradictory national laws had been passed (Sprague and Boyle 2001). Policymakers and stakeholders turned to the OECD and its proven and widely accepted procedures of defining tax concepts. This was a remarkable novelty in the tax policy world.

Amid the soaring ‘dot.com boom’ the OECD began to examine the area. Prospects of how the Internet would transform the economy rocketed high, but tax experts became increasingly confident that the problems of Internet taxation could be tackled with existing taxation rules. The OECD addressed the subject in a series of conferences. At the 1998 Ottawa conference, the Taxation Framework Conditions for Electronic Commerce and a comprehensive post-Ottawa agenda were agreed. The institutions of the OECD’s Committee on Fiscal Affairs expanded when several new advisory groups were set up to implement the framework (OECD 2001). National governments supported the efforts since the Ottawa conditions assured fair sharing of tax bases from e-commerce and maintenance of fiscal sovereignty. The position that the Internet could be managed with the established tax concepts became the prevailing opinion. The phase of adaptation of tax rules to the Internet took five years and resulted in the adoption of an updated Model Tax Convention and Commentary in 2003. Of course, this revision did not settle Internet tax rules once and for all, but the essential steps were made.

One of the most important issues was how an Internet server should be classified so as to fit in the established tax rules. More specifically, it had to be defined under what circumstances a server is a so-called ‘permanent establishment’. This concept refers to the location of a commercial activity and is used to attribute profit to a particular place of business. The tax experts at the OECD worked out a catalogue of qualifications according to which, simply put, a server constitutes a permanent establishment for a firm if it simultaneously meets four conditions: it is owned, controlled, and maintained by the firm and is of vital importance for its business. In contrast, a website or other immaterial applications fall short of a permanent establishment. Consequently, it is not so easy to move an e-commerce business to a tax haven. If a company resides in an industrial country and has an online shop hosted on an offshore server, the income from this server will nonetheless be taxed in the firm’s home country.

Furthermore, even if a server located in a foreign country is recognized as a permanent establishment, the profit attributed to this place of business will be small because the creation of value consists in the development and production of a good or service, not in transmitting data. The location where the revenue is generated is not necessarily the place where it is taxed. This example illustrates how the Internet was integrated in international tax rules.

Although the expert community managed to keep up the principles of taxation, the rise of the Internet fuelled the internationalization of firms, the division of production, and intelligent profit shifting. Tax administrations became aware that closer cooperation was necessary. Therefore, the OECD created new transgovernmental institutions to bring together tax administrators of member and non-member countries and of international organizations. The agenda comprises information exchange, use of technology, and best practice in tax administration. Notably, the use of the Internet has become an important tool for tax collectors, too.[3]

**Transformation of the Tax State?**

At first glance, the adaptation to the Internet effected little change in the international tax regime. The main features remained unaltered: national fiscal sovereignty, a multilateral convention, and a network of bilateral tax treaties. So far, there is little evidence to support the prediction that e-commerce will lead to a shift of taxing authority to a new global tax arrangement (Paris 2003: 177). Nevertheless, the fact that, in the phase of uncertainty, nation

[3] Due to restrictions of space, the chapter leaves aside sales taxes or value added taxes, which cause similar problems in transborder e-commerce. As with income tax, officials responded by developing closer transgovernmental cooperation.

states did not act on their own but called on the OECD to handle the problem brought up the view that tax policy-making on e-commerce made the OECD an ‘informal “world tax organization”’ (Cockfield 2006). So, does a closer look reveal some kind of transformation of the tax state? As mentioned above, states preserved their fiscal sovereignty, that is outcome responsibility remained at the national level. But the OECD’s definition of the Internet-issues for taxation and their incorporation in the updated Model Tax Convention and the Commentary show that regulatory responsibility for tax matters has partly moved to the international level. The new bodies set up in the process strengthened the OECD’s Committee on Fiscal Affairs. This institutional empowerment amounts to a diffusion of statehood. Since representatives of national governments form an essential part of the OECD’s tax institutions membership, the regulation of e-commerce taxation is interlocked with the respective government departments. The operational responsibility of national tax administrations as such is not challenged. Change occurred, however, with respect to the means and procedures of tax collection and tax computation. The function to provide the state with money stayed at the national level, but transgovernmental cooperation of tax authorities has intensified. Again, this points to a (tentative) diffusion of statehood in tax matters. In sum, the internationalization caused by the need to regulate e-commerce taxation was a reaction of the states to the Internet, formulated by an intergovernmental organization, implemented at the international and the national level, and triggering an ongoing transgovernmental process.

**States Ensure the Legitimacy of International Taxation**

Just as the international tax regime did not change significantly in response to the Internet, its legitimacy was not impaired. In some respects it may be said to have increased. Like other international organizations, the OECD – the institution facilitating and shaping international

tax cooperation – has enhanced transparency by documenting its work online. The website contains many documents on taxation but no minutes of meetings. The Internet's communicative possibilities were sparsely used in the formulation of the rules, whereas networked computers became more important for the exchange of information between tax administrators. The OECD has established stakeholder relationships since the 1960s, especially to business and industry but recently also to consumer groups. Thus, the groups directly affected by practical tax matters were enabled to participate in the formulation of the e-commerce taxation framework.

The tax regime's architecture of multilateral standard setting and bilateral negotiations provides for the congruence of political and social spaces in international tax policy. Thus, the efforts of states to avoid double taxation and to reduce tax evasion are legitimate in the sense that they aim at taxpayers that have a link to the territory of the involved states. Although the democratic accountability of the OECD's committee members is only indirect, the involvement of national government officials makes the process accessible to parliamentary controls. Nevertheless, bilateral tax treaties can only be approved or rejected as a whole – a well-understood legitimacy problem that parliamentary democracies have to put up with. The fears that e-commerce would cause tax losses and unequal taxation of the online and offline economy were dissolved by the rules adopted by the international tax community. The states' abstinence from producing an incomprehensible diversity of national laws in favor of a common OECD standard for e-commerce taxation reflects their awareness that the Internet requires international solutions to some extent, but not necessarily a 'world tax organization'. Overall, states have stabilized their position as main actors in tax policy by international and transgovernmental cooperation *and* as providers of legitimacy to the international tax regime.

## Conclusion

Nothing comes closer to a completely denationalized social space than cyberspace. This makes the Internet and policy areas which are in one way or another strongly impacted by it a ‘most-likely case’ (Eckstein 1975) for the hypothesis that globalization pressures cause the modern Western nation state to transform by internationalizing or privatizing some of its wide-ranging responsibilities. In the three cases reviewed in this chapter, we indeed found evidence to support this hypothesis, although the extent of the transformation is smaller and more variable than might have been surmised. Thus, in each of our cases international institutions – including supranational (EU), intergovernmental (OECD), and transnational (ICANN) bodies – gained in importance since the advent of the Internet, eliminating, circumscribing, or qualifying the autonomy of the nation state in the issue-area at hand. Moreover, in two cases (‘DNS’ and ‘data protection’) the (self-)regulatory efforts of private corporations and associations are now much more critical than before for the provision of the normative good in question. In both cases this resulted in the emergence of a hybrid mixture of public and private arrangements and authorities – taking the shape of a unilateral-transnational regime in ‘DNS’ and of a multilayered intergovernmental-transnational regime in ‘data protection’.

Outcome responsibility usually remains with the nation state, although the U.S. claims the role of a global warden over the Internet’s name space, and the members of the EU have delegated their sovereignty in the area of privacy protection to the supranational level. Both regulatory and operational responsibilities in the three policy fields are no longer monopolized by the nation state (as they indeed were in the 1960s and 1970s). At the same

time, nowhere has the state ceased to make and implement rules altogether – the single partial exception being the DNS where, in the case of generic Top Level Domains, privatization (under the auspices of the U.S. government) has prevailed 'all the way down'. At both levels of responsibility, international and private actors now play important roles in the provision of the normative good in question. As to the nature of the reconfiguration of statehood, the bulk of the reshuffling of responsibilities that can be observed is more adequately described as a diffusion than a shift, that is the powers and efforts of the nation state in these areas tend to be complemented rather than replaced. Again, 'DNS' turns out a special case, though: taking the 'ancient regime' of international telecommunications as a baseline, nation states (except for the U.S.) have indeed lost most of their responsibilities with respect to a specific part of the telecommunications infrastructure to a private institution with global reach (ICANN).

The three cases vary significantly with regard to the extent of transformation that has taken place. The most radical deviation from the status quo ante of the 'Golden Age' occurred within the policy field of international communications, where we focused on the administration of a new name space (the DNS). Not only is this the case where the role of the nation state (in general) has been most drastically curtailed; it is also here that we find the most innovative (though ill-fated) experiments with novel ways of securing legitimacy for a transnational authority, culminating in the 2000 global online elections of Internet users' representatives to its oversight body. By contrast, despite the wide-spread fears for, and speculations about, the future of the tax state that were aroused by the advent of the Internet in the mid-1990s, comparatively little has changed in the way that states, individually and collectively, seek to secure access to their tax base and to avoid double- or non-taxation in international commerce. The international tax regime appears to have 'absorbed' the shock that came with the rise of e-commerce, although the OECD's regulatory responsibility has

slightly increased and transgovernmental cooperation to improve states' ability to exert operational responsibility has intensified in the process. Finally, 'data protection' occupies a middle position witnessing both continuity and change in prevailing practices of statehood.

These differences can be accounted for by a combination of closely-related factors: first, the observed variation reflects the policy-typological differences between the three cases and the degree of 'intrusiveness' that comes with them: 'market-making' policies such as 'DNS' tend to be less conflict-prone than 'market-braking' policies such as 'privacy protection' or even 'market-correcting' endeavors such as 'taxation' (Streeck 1995); therefore, states will guard their sovereignty and their means of social control less jealously in such fields and institutional arrangements will be more flexible. Second, the three issue-areas differ considerably in their 'age', with 'taxation' being the oldest and 'DNS' being the youngest. This is significant and helps to explain the variation observed in that 'older' policy fields will tend to have given rise to stronger path dependencies, habits, and vested interests that resist change. Third, it seems plausible to assume that the novel features of the Internet which, as many observers pointed out, have a considerable *potential* for re-organizing and democratizing politics will play out the more strongly the 'closer' and 'essential' a policy area is to the Internet. Again, this correlates nicely with the features of our three cases.

It is part of the logic of most-likely case studies that we *expect* the hypothesis to pass the test posed by the selected cases clearly and unambiguously and that whenever it fails to do so we should become more cautious about it. Against this background, it is important to reiterate that the transformations of statehood we observed in our cases were less far-reaching and pronounced than might have been expected – and indeed often *was* expected only a few years ago. What is more, there are indications that the transformation may have topped out and we

are witnessing a *return of the state*. Thus, the nation state has recently begun to intervene more vigorously in private self-regulation activities in the area of 'data protection', and during the World Summit on the Information Society, many states (including the EU) voiced concerns about the unilateral character of present-day Internet governance that clearly breathed nostalgia for some of the constitutive features of the 'ancient regime'. (There is no such trend in 'taxation' for the simple reason that here the nation state had never shown signs of retrenchment.) Interestingly, this return of the state has been facilitated by the difficulties the new post-national arrangements faced securing the normative good of *democratic legitimacy*. This is somewhat ironic given that issue-specific transnational arrangements were often expected to be more congruent, transparent, participatory, and accountable to stakeholders and also to be more effective in terms of problem solving than traditional intergovernmental regimes. As our review of the three cases has indicated, the political arrangements in the three fields are – and, in varying degrees, are *perceived* to be – wanting in each of these respects, although some advances have been made in recent years (not least thanks to the Internet) in particular with regard to transparency. Moreover, disappointments about the legitimacy ('DNS') and doubts about the effectiveness ('privacy protection') of the privatized regimes currently in operation have contributed to the nation state now being in a position to reclaim increased responsibilities in the respective issue-areas. Even though it seems safe to be predict that a restoration of the 'national constellation' will not take place, the future division of labor between the nation state, private bodies, and international institutions in these three Internet-impregnated policy fields is far from settled and hence the search for a new stable order is likely to continue for some time to come.

## References

Bennett, Colin J. (1998), 'Convergence Revisited: Towards a Global Policy for the Protection of Privacy?' in: Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: the New Landscape*, Cambridge, Mass.: MIT Press, 219-241.

Cockfield, Arthur J. (2006), 'The Rise of the OECD as Informal "World Tax Organization" through National Response to E-commerce Tax Challenges', *Yale Journal of Law and Technology* 8 (2), 136-187.

DOC (1998), 'Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers' (Online: http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm, last access: 23 November 2006).

Drake, William J. (1994), 'The Transformation of International Telecommunication Standardization', in: Charles W. Steinfield, Johannes Bauer and Laurence Caby (eds.), *Telecommunications in Transition: Politics, Services, and Technologies in the European Community*, Thousand Oaks, Cal.: Sage, 71-96.

Eckstein, Harry (1975), 'Case Study and Theory in Political Science', in: Fred I. Greenstein and Nelson W. Polsby (eds.), *Handbook of Political Science*, Reading: Addison-Wesley, 79-138.

Farrell, Henry (2003), 'Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Agreement', *International Organization* 57 (2), 277-306.

Goldsmith, Jack L. and Tim Wu (2006), *Who Controls the Internet? Illusions of a Borderless World*, New York: Oxford University Press.

Greenleaf, Graham (2005), 'APEC's Privacy Framework: a New Low Standard', *Privacy Law and Policy Reporter* 11(5) (Online: http://www.austlii.edu.au/au/journals/PLPR/2005/1.html, last access: 23 November 2006).

Habermas, Jürgen (2001), *The Postnational Constellation: Political Essays*, Cambridge, Mass.: MIT Press.

Heisenberg, Dorothee (2005), *Negotiating Privacy: the European Union, the United States, and Personal Data Protection*, Boulder, Colo.: Lynne Rienner Publishers.

Lessig, Lawrence (1998), 'Governance', Keynote: CPSR Conference on Internet Governance, 10 October (Online: http://www.lessig.org/content/articles/works/cpsr.pdf, last access: 23 November 2006).

Lyon, David (2003), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London: Routledge.

McGinness, John (2003), 'What's up in the Asia-Pacific? APEC Privacy Initiatives', Paper for the 'Privacy Issues Forum', Wellington, 28 March (Online: http://www.knowledge-basket.co.nz/privacy/media/McGinness.pdf, last access: 23 November 2006).

Mueller, Milton (2002), *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge, Mass.: MIT Press.

OECD (2001), *Taxation and Electronic Commerce: Implementing the Ottawa Taxation Framework Conditions*, Paris: OECD.

Paris, Roland (2003), 'The Globalization of Taxation? Electronic Commerce and the Transformation of the State', *International Studies Quarterly* 47 (2), 153-182.

Rixen, Thomas and Ingo Rohlfing (2005), 'The Political Economy of Bilateralism and Multilateralism: Institutional Choice in International Trade and Taxation', *TranState Working Paper* No. 31, Bremen: TranState Research Center.

Sprague, Gary D. and Michael P. Boyle (2001), 'Taxation of Income Derived from Electronic Commerce: General Report', *Cahiers de Droit Fiscal International* LXXXVIa, 21-63.

Streeck, Wolfgang (1995), 'From Market-Making to State-Building? Reflections on the Political Economy of the European Social Policy', in: Stephan Leibfried and Paul Pierson (eds.), *European Social Policy: Between Fragmentation and Integration*, Washington, D.C.: The Brookings Institution, 389-431.

Warren, Samuel D. and Louis D. Brandeis (1890), 'The Right to Privacy', *Harvard Law Review* 193 (4), 193-220.