Transforming Politics in a Digital Era

BRIE Working Paper 166

January 2004

Abraham Newman and John Zysman

Copyright 2005 by the authors

Please send comments to aben@berkeley.edu or johnz@socrates.berkeley.edu

This working paper will be the preface to How Revolutionary was the Revolution? National Responses, Market Transitions, and Global Technology in the Digital Era, A BRIE/ETLA/Helsinki Project, John Zysman and Abraham Newman, Editors, Forthcoming
With the rise of digital technology, advanced democracies are in the process of transitioning from industrial to knowledge-based economies. The combination of binary knowledge expression, immense processing power, and digital networks has created the basis for a fundamental shift in economic and political organization domestically and internationally. This digital revolution holds tremendous opportunity for society and the global economy as new markets, business models, and means of organization emerge. At the same time, however, innovation has an intensely destabilizing effect for broad societal bargains, such as the notion of property, as well as real competitive position, as new entrants take advantage of technology to challenge incumbents. Our concern is how politics shapes this global revolution in society and the economy.

Barrowing from Karl Polanyi, we employ the metaphor of a second Great Transformation to drive a discussion about the political economy of the digital era. By “Great Transformation”, we mean a fundamental and basic shift in the rules of society that alters the way economy and polity operate. There is one classic example, the Great Transformation that began in England in the 16th century. In this case, the creation by the state of the commodities for land, labor, and money defined the establishment of a market society. Before that transformation, markets were more of an adjunct to the society. Those early markets created by the traders and the burghers, were in a secondary position to the landowners. Peasants were tied to the land; and land was encumbered by its social position in a political order. For landlord, peasant, and burgher, position in a politically defined social community defined access to opportunities and to earn income. When the market system was endorsed by the state, it stood these relations on their head. Land and labor became commodities to be bought and sold in the market. Social position could move in relation to what was captured in the market.

While some technological fanatics have naively argued that politics has little role to play in the digital era, it is our contention that political actors – government, business interest, and public interest groups – serve an integral role in the evolution of the digital revolutions transpiring across the globe. Counter to claims that technology vitiates state power in the international economy, we believe that the state has a critical role to play. Just as in the classic examples, governments are actively involved in creating a market for the fictitious commodity of information. The crux of this essay is to use the metaphor of the Great Transformation to demonstrate how politics shape and influences the digital era. Governments have acted to
mediate the transformation: promoting the technological infrastructure necessary for the revolution, establishing the fictitious commodity of information through intellectual property, and embedding digital markets in social norms. Far from a neutral intervention, state actions influence the character of the revolution, including the political effects of the transformation. At the same time, governments have confronted well organized interest groups that have played an active role in influencing policy outcomes.

This essay analyzes the politics of the digital transformation in four parts. The first section describes the scope and scale of the technological change in more depth. This is followed by a brief presentation of the naïve technologist view that relegates politics to a peripheral role. The third section uses the lens of the Great Transformation to explore in more detail the means by which the state interacts with the digital revolution. The following section offers a set of policy strategies that governments may employ to resolve digital challenges. The fifth section highlights the dynamics of the political process that influence government policy before presenting some thoughts for future research.

Part I: The Renewable Revolution

Just as the industrial revolution rested on a revolution in tools and power, the core of the information technology sector is the creation and production of a new tool set, which Steve Cohen, Brad DeLong and John Zysman have termed “tools for thought” (Cohen, DeLong, and Zysman 2000, p. 7-8). These tools manipulate, organize, transmit, and store information in digital form, thereby creating a set of information services and information products. These services and products allow the application of information to industrial as well as machine processes (Weiner 1954). The digital revolution and the tools for thought can be broken down into three fundamental elements:

- **The concept**: The information revolution begins with the notion of information as something that can be expressed in binary form. Data ranging from supermarket purchases to fingerprints can be represented in digital code.
- **The equipment**: The software consists of written programs, including procedures and rules, that guide how the equipment processes information. The hardware, the equipment, that executes the processing instructions, has evolved from the era of vacuum tubes, to individual silicon transistors, to integrated circuits implemented on silicon wafers and may evolve into other physical manifestations.
- **The networks**: The data networks interlink the processing nodes of individual computers, and the network of networks together create a digital community and society.
The production of the equipment and networks, information technology (IT), has itself become a leading sector in the economy. Tools for thought create the capabilities to process and distribute digital data, multiplying the scale and speed with which thought and information can be applied. IT tools can affect every economic activity in which information sensing, organizing, processing, or communication is important – in short, every single economic activity.3

What seems most significant is that information technology represents not one, but a sequence of revolutions. It is a continued and enduring unfolding of digital innovation, sustaining a long process of industrial adaptation and transition. As Cohen, DeLong, and Zysman relate, IT has been a recurrent revolution:

In the 1960s Intel Corporation co-founder Gordon Moore projected that the density of transistors on a silicon chip—and thus the power of a chip—would double every eighteen months. Moore’s law, as it came to be called, has held. Today’s chips have 256 times the density of those manufactured in 1987—and 65,000 times the density of those of 1975. This continued and continuing every-eighteen-month doubling of semiconductor capability and productivity underpins the revolution in information technology. The increase in semiconductor density means that today’s computers have 66,000 times the processing power, at the same cost, as the computers of 1975. In ten years computers will be more than 10 million times more powerful than those of 1975—at the same cost. We now expect—routinely—that today’s $1,000 personal computer ordered over the Internet will have the power of a $20,000 scientific workstation of five years ago. And what was once supercomputing is now run-of-the-mill. The past forty years have seen perhaps a billion-fold increase in the installed base of computing power (Cohen, DeLong and Zysman 2000, p. 13-14).

The conventional economic explanation of a leading sector is that the original innovation creates a set of opportunities, somewhat like distributing money on the ground. Some radically valuable possibilities, the larger bills, are picked up first; the smaller opportunities are captured later. But the original technological revolution loses force, as the most valuable opportunities are picked up and implemented. The notion argued in this chapter is, of course, that the revolution is renewed – if not with each cycle of Moore’s law, certainly with the radical increases in computing power generated in a very few years. An original transistor, a single bit, bears little relationship to a 16 kilobit integrated memory chip. A gigabyte chip with a billion transistors is another thing altogether, and it is 7 Moore cycles, less than two decades along the road from the 16k. And Moore’s law has at least several more cycles to run. The technological revolution is
renewed every decade. The currency is redistributed on the ground, as the bills themselves get larger. The fundamental question, then, is to ask how these resources will be distributed.

**Part II. Putting the State on the Sidelines**

At the creation of the Internet, the U.S. and European governments effectively laid the foundation for self-regulating groups, who established and sustained markets in cyber space. For those earlier “net” pioneers, who were forging the system rules, setting the architecture of the early Internet, it seemed liked the government was an interloper in a system that was run by technologists for technologists. These technological enthusiasts argued that the architecture of the Internet made it impossible to regulate. The famous claim made by the early Internet advocate John Gilmore that, “the Net interprets censorship as damage and routes around it” epitomized the beliefs of many technologists.\(^4\) They viewed cyberspace as beyond the reach of state controls. National governments would be forced to cede much of their regulatory authority to the cyber community, eroding traditional notions of sovereignty (Post and Johnson 1996).

The digital revolution posed a dual challenge to the state. First, information technologically reduced the costs associated with conducting international business, part of a phenomenon popularly labeled globalization (Weber 2001). Firms that took advantage of digital technology to expand their geographic reach in turn limited the efforts of public officials to manage their economies. Stringent domestic regulations, it was believed, encouraged footloose capital to relocate to more hospitable institutional environments, forcing governments around the globe to engage in a race to the bottom in economic intervention (Tonnelson 2000). State autonomy fell victim in the digital era to firm mobility (Ohmae 1995).

Second, the decentralized, non-hierarchical character of digital networks was viewed as incompatible with the rigid, inflexible governance tools available to the state. As Virginia Haufler has argued in the case of information privacy, “The decentralized, open, global character of one of the main transmission sources for personal information – the Internet – makes it difficult to design and implement effective regulations through top-down, government-by-government approaches” (Haufler 2001, p.82). The governance problems raised by digital technologies threatened to further erode state autonomy, as non-state actors were empowered to resolve major societal disputes (Rosenau and Singh 2002). Operating from this perspective, Debora Spar describes a cyber world of state regulation displaced by industry self-regulation:
Fundamentally, I argue, governments cannot set the rules of cyberspace. That is because cyberspace, unlike governments, slips seamlessly and nearly unavoidably across national boundaries… With governments pushed effectively to the sidelines, firms will have to write and enforce their own rules, creating private networks to facilitate and protect electronic commerce (Spar 1999, p. 82).

On a policy level, politicians in the United States relied heavily on the private sector to navigate the first years of the digital revolution. A chorus of business lobbies argued that government regulation would crush this vital infant industry. The role of the government, if any, was to get out of the way of the sector’s development. The Clinton administration did not stray far from these concerns, insisting that the government should not interfere with the development of the information technology revolution. The administration believed that private sector self-regulatory mechanisms would guarantee the successful construction of information markets. In their 1997 *Framework for Global Electronic Commerce*, President Clinton and Vice-President Gore asserted that “the Administration […] will encourage the creation of private fora to take the lead in areas requiring self-regulation such as privacy, content ratings, and consumer protection and in areas such as standards development, commercial code, and fostering interoperability.” Echoing the US view, Europe’s then-Commissioner for Telecommunications, Martin Bangemann, suggested that business should take the lead in developing an “International Charter for Electronic Commerce” that would rely heavily on “market-led, industry-driven self-regulatory models” (Commission 1998).5

Of course, the early notions that the Internet should be free of government, like a mythical wild west community, ignored the fact that the western settlements required a local sheriff; they required governments. When the Internet was transferred to the commercial world, those requirements for legal structure in the operation of the network became more evident, more urgent, and the rule making for the Internet became, at least in part, rule making for the economy. The issues were no longer simply technical ones of how to operate the network or communicate across this global network of networks. Suddenly, all the questions of an operating marketplace had to be addressed; appropriate domestic and international rules had to be defined for domains from privacy to taxation. The results of these decisions have real distributional and societal consequences. And states were not about to abdicate this responsibility to private actors. In fact, despite the decentralized, international character of digital networks, governments have played an instrumental role in shaping the character of forming digital societies.
The emergence and evolution of the digital era has not been the product of purely neo-liberal strategies, on the one hand, nor of purely interventionist strategies, on the other hand. Governments acted simultaneously to subsidize infrastructure development, extract themselves from direct market control, and forge new rules to promote economic transactions. Framing the role of the state in ideological terms confounds the multitude and seemingly contradictory strategies governments undertook. Like all markets, cyber markets require definitions of property, exchange, and competitive market structure. And all of this requires rules.6

Part III. The Role of the State in the Digital Transformation

Barrowing from Polanyi, we use the metaphor of the great transformation to highlight the role of the state in the political economy of the digital era. Remember that the drama of the great transformation itself was the shift from a traditional society, in which markets fitted within social order, and economic activity bowed to the confines of social rules, to a market society, in which land, labor, and capital became commodities moving in response to price signals from the market. That transition was the product of a series of political battles that redefined England. They included the enclosures, the poor laws, and the repeal of the Corn laws. The enclosures transformed community public lands into private farming lands, beginning the creation of a market for land. The series of poor laws, culminating in the elimination of the Speenhamland system in 1834, created a labor market. The 1834 Poor Law Reform broke the link for survival between individual and local community, making the individual worker’s well being dependent on wages obtained in the labor market. The repeal of the Corn Laws in 1846 opened British agricultural markets, limiting trade protection, so that lower cost grain could feed the emerging industrial work force. That political decision marked a shift in power from the landed classes to the emerging industrial bourgeoisie (Polanyi 1944).

In the contemporary era, as in the industrial revolution, the state has played a vital role in the construction of the digital economy through policies of deregulation, market-making, and re-regulation. This effort has focused around two central questions. First, what are the rules that should underpin the new digital markets? As digital technologies diffuse, businesses in industries ranging from financial services to telecommunications search for market advantage. At the same time, these innovations have the potential to disrupt the current distribution of power within a sector and across polities. Incumbents simultaneously see lucrative market potential and
economic disruption in digital advances. Market rules, drafted and enforced by the state, fundamentally shape the distribution of economic gains and modulate the extent of the revolution domestically and internationally.

The second question confronting state authorities concerns the implications of new market rules for society more generally. As the digital economy is constructed, decisions about market rules inherently structure information flows, thereby influencing the character of the political community. The state must manage the social externalities that arise in parallel to the digital economy. Even without an intentional shift in our views on privacy, for example, information technology changes the balance of who can know what about whom. Suddenly, information technology tools for collecting personal information become so powerful that credit cards companies can predict divorce from expenditure patterns, and insurance companies can readily access medical records to assess health risks. Legislation that spells out how personal information may be collected and deployed in the economy become necessary to address these negative social externalities.

Additionally, it is important to note that in the digital era, quick adjustments to rules or laws often have significant, sometimes unintended, consequences. Old questions are posed in quite fundamentally new ways. Take for example the domain of digital content. Establishing a new rule, the Digital Millennium Copyright Act (DMCA), in the name of an old notion, intellectual property, is not a neutral extension of the original principle. The law, which criminalizes the production and application of circumvention software, imposes tighter restrictions on the use of digital content than previous legislation, re-setting the balance between users and providers of intellectual property in favor of the providers. Digital innovations have opened the possibility that the prior battles could be refought and prior, seemingly settled outcomes could be altered. Rather than a simple addendum to an old deal, the new formulations often require conceptual innovation and political entrepreneurship and may redistribute power and benefits significantly.

The role of the state in the digital debate has a peculiar form, in that the rules of digital information, hence of a digital polity, are embedded not only in convention or in the law, but in the computer code itself (Lessig 1999). Just as highway architecture dictates where you can get on and off the freeway, the computer architecture and the code implementing applications dictate what is and isn’t possible in a digital era. In the early years, of the Internet, the open and user-
controlled architecture led to the sense of Cyber space as a domain outside the control of governments or physical communities. Hence Stewart Brand’s infamous remark, that “Information wants to be free,” reflected the particular architecture of the early Internet. But that early Internet was only one potential architecture; other more controlled or restricted networks are also possible. Digital information wants nothing at all; it flows where the network architecture permits. And the network architecture is a product of the code writers. To say that we must regulate the code, hence the code writers, is not to say that there is a single technologically dictated outcome. While politics is always about values and outcomes, about who gets what, for such choices to have meaning in a digital world, they must inevitably be embedded in code and respect the technological logic of the “tools for thought.” Law and code then interact to establish the rules of the digital era.

At the dawn of the digital era, governments have played a critical part in the creation of the fictitious commodity of information. In this effort, they have used public policy to build the infrastructure for and remove barriers to the new market. Government legislation has shaped the way that information technology has interacted with production patterns, influencing the success of emerging business models and modes of industrial organization. At the same time, state initiatives have been instrumental in navigating the complex political fights that surround the digital transformation. Government legislation is critical to embed the new markets in social norms and to limit the inevitable pushback by the losers of the new era. In short, the character of the information revolution has been modulated by government interventions. The following section highlights several pathways by which the state has shaped the digital transformation. Chief among these are: establishing the infrastructure and removing barriers to market evolution; constructing the commodity of information; embedding new markets in social norms.

Building the Infrastructure and Removing Barriers to New Market Evolution

In the case of Polanyi’s England, the government promoted the enclosure at the same time that it repealed protections that hindered the market’s development. Similarly, in the case of the digital era, governments have simultaneously developed the infrastructure for and removed barriers to commodified information markets. In the US, the creation of the Internet was the product of both purposive intervention, government action by the Defense Department’s Advanced Research Projects Agency (DARPA), and aggressive deregulation/re-regulation.
Seeking to protect communications from nuclear interruption, DARPA funded the creation of the underlying conception and protocols of the Internet in what was called ARPANET (Hafner and Lyon 1998). This Internet prototype refined the technology necessary to transmit data through packets of information, providing the fundamental architecture of the current Internet. In contrast to telephone lines, which traditionally used switches to directly connect the receiver to the sender, packet switching decomposes information into its components, sends them through the network, before recombining them at their destination. The government managed ARPANET through the National Science Foundation, then prepared it for transfer to commercial use.

The government laid the groundwork for the digital era through regulatory reform as well as infrastructure investment. The aggressive introduction of competition in the telecommunications sector, highlighted by but not confined to the break-up of AT&T, unleashed user-led and consumer-based innovation in data networks. Inexpensive local flat-rate fees, for example, gave consumers the ability to experiment with data networking at relatively minimal cost. That opened the way to user-generated networks and facilitated the radical and rapid spread of Internet technology (Hafner and Lyon 1998).

The European story likewise displays these twin roles of the state. Simplified, one part of the story is the deregulation of the telecommunications system led by the European Commission. The Commission created national coalitions for European-wide rules that would compel the transformation of state administrations responsible for post and telegraph into regulated companies in at least partly competitive markets. The other side of the story is an array of directed state actions intended to develop and diffuse digital technology. The foundations of the World Wide Web were developed at CERN, the Center for Nuclear Research in Geneva, Switzerland. A pan-European nuclear physics lab, CERN faced the dilemma of bringing together a highly geographically dispersed European nuclear physics community. An information systems scholar from CERN, in response to this organizational demand, developed the architecture of the World Wide Web based on a language to construct Web pages, the protocol to transmit these pages, and a browser system to read the transmitted information. It was this innovation that resulted in the highly accessible browser system that has facilitated the rapid diffusion of the Web (Gribble 2004).
Government intervention has continued, but taken on a different flavor, with the state-sponsored transition to high-speed broadband connectivity. The original consumer use of the Internet could expand so suddenly because it could be deployed over the existing telephone infrastructure. However, new uses of the Internet, such as downloading music or playing videos, require a different infrastructure. That infrastructure is loosely called broadband, with broadband typically referring to anything faster than telephone lines, whether a network of fiber or DSL technology. The fact that the next generation consumer network requires an infrastructure other than the traditional copper-wire phone system has posed new policy problems.

While there is international agreement on the need for rapid deployment of broadband data networks for consumer use, the policies to accomplish that rapid deployment vary radically by country. The question remains whether this build-out should be a purely private decision of local providers or should be encouraged and subsidized by the government. The answers around the world are quite varied. To capture the range, consider Korea and the United States. Korea is a story of stunning penetration of broadband services into the society. Of the 16 million Korean households, 78 percent have broadband access, compared to roughly 20 percent in the United States (Shameen 2004). The broadband build-out was consciously subsidized by redirecting funds from the wireless spectrum auctions. In total, the Korean Government has spent nearly three billion dollars on broadband diffusion. This effort has been carried out through an aggressive campaign, including direct subsidies, loan programs, and research and development funding. The government has even adjusted its housing ratings system, so that units with broadband systems may be priced at a higher rate (Richardson 2002). In the United States, we have left the effort to a competition amongst the cable TV companies, generating a cable TV infrastructure, phone companies offering DSL services, and potentially even power companies offering access over electricity lines. The result is less overall coverage, but more diversity in network forms. In both the US and Korea, government policy has been instrumental in shaping the technological infrastructure for information markets, albeit in very different ways.

Commodifying Information

Cyber law has for the most part focused on creating a market world in cyber space, on the particulars of transaction and property, in the new digital network society. Intellectual property (IP) is central to this effort and a critical feature of an information society. We know
that property is always a legal fiction, involving the specification of enforceable rules about what
a person can have, hold, and dispose. Hence, in a fundamental way, property and its rules of use
are always a political creation.

We also know that physical property and intellectual property have different
characteristics. In the case of tangible goods with a physical existence, the rules of property set
the terms of use and disposition. Since physical property cannot be simultaneously shared, some
rules of use and disposal are necessary, whether those rules constitute private property or not.
With the great transformation in England, the enclosure movement closed off common public
lands, converting them into private holdings. By contrast, intellectual property is a non-
excludable good. In other words, it is not something that one holds, carries about, or physically
denies to others. Nor if one uses it, is it unavailable to others. Hence, intellectual property as
economic property, that is something one is willing to buy because one cannot have its use
without payment, is an entirely political creation, a fictitious commodity. The very “good” is a
product of a rule. The rules of intellectual property in an information society are thus absolutely
central.

Digital technology radically changes the logic of control and distribution of intellectual
property. Whatever the cost of developing intellectual property, be it a movie or a software
product, the marginal cost of precise reproduction and distribution is almost zero. Since media
products are so immediately affected, it is evident why media companies have driven the
reformulation of intellectual property law to permit them to recreate control over the distribution
of their products.

The most blatant example of the effort to recreate traditional notions of property in the
digital era is the Digital Millennium Copyright Act of 1998. Faced with the challenge of precise
reproduction at zero cost to distribution, content providers ranging from Hollywood to the
publishing industry lobbied to rebuild walls around their intellectual property preserves. The
DMCA contained two critical provisions. First, it created criminal penalties for the
circumvention of encryption programs. These encryption programs hide the underlying software
code from the user, preventing the reproduction and distribution of the purchased product.
Second, the DMCA outlaws the manufacturing or sale of code-breaking software. The digital
nature of the medium, however, does not just recreate past IP protection. Regulating code has
broader implications for society more generally. The notion of “fair use,” which allows the
holder of intellectual property to make that information available in a non-commercial manner, has been severely curtailed. A digital recording or book for example may be encrypted, so that it can never be duplicated, eliminating the consumer’s ability to share a purchase with friends or colleagues, even though the practice is fully legal. Digital rights management software may stop the consumer from duplicating downloaded music, preventing the customer from listening to the recording on multiple personal entertainment devices – another legal practice. Implanting intellectual property protection into the product through encryption systems permits the perfect control over use, replication, and distribution.11

The digital revolution allows new forms of intellectual property to be created. For example, many types of data can now be easily packaged and sold. Expressed in digital form, information becomes a commodity that can be transmitted, manipulated, stored, and sold as an object. Argued most generally, in a digital era, commodified explicit knowledge becomes pervasive. As knowledge, including digital instructions for physical control, becomes explicit and explicitly expressible in useful ways, the possibility and importance of protecting that knowledge as property increases. Hence, it is not just the media industry which turns to copyright for protection, but also semiconductor designers, who wish to protect the design and production processes. Patent law has played a critical role in transforming the intellectual property regime of the digital era. As the patent office recognized the legitimacy of business model patents, processes increasingly expressed in digital form have become property. The patent disputes over the eBay auction or the Amazon checkout strategy provide troubling examples of how previously shared knowledge may become commodifiable through law. The process of establishing a checkout procedure on the web, rather than the intellectual property behind the book which is being purchased, receives proprietary protection (Preston 2004). The fight over what can and cannot be protected is critical in daily business; for our purposes, the seemingly inexorable expansion of the protectable is the issue.

Intellectual property rules inevitably affect more than just the media industries or the business possibilities of sectors that use digitized information and programs. Intellectual property has always been about balancing the need to reward those who generate knowledge against the desire for widespread distribution and use. Digital technology makes more information more easily accessible; offsetting that, technology and law create new boxes to control that information. The texture of social and political debate is powerfully influenced by who owns and
can use content generated by others. The political community is thus shaping and shaped by the rules of intellectual property.

**Embedding Markets in Social Norms**

The digital revolution has radically altered the types and amount of information in the economy as well as the ability of actors to transmit and use that information. With data cheaply passing over digital networks, long nourished business dreams become reality. Yet the question arises: who will capture the benefits of these innovations, and what threats do they pose to society? Government stands at the crossroads of the digital era, constructing the rules that underpin these emerging markets and mitigating the negative social externalities. As in the case of the industrial revolution, the immensity of the technological change creates tremendous instability and displacement, which could derail the transformation. The state then plays a critical role in steering Polanyi’s “self-regulating market” so as to assure its viability. What is “new” about the digital state is less some technologically augmented or vitiated state authority than the ability of the state to influence the resolution of fundamental societal bargains that have been reopened by changes in information technology (Weber and Zysman 2000).

Two debates appear most critical. The first is privacy – that which permits us to remain in our personal domains secluded from the view of others. The second debate concerns speech – that which we can say and debate in the public arena. These debates began in the marketplace, how to use information to economic advantage, and spilled over into society, how our communities and political processes will be organized. A failure by the state to address these conflicts risks derailing the transformation and therefore demands government attention. Although the state has long been seen as the number one enemy of civil rights, such as privacy and free speech, the digital transformation has ironically positioned the state as a critical defender of these very freedoms. As businesses augment their power to collect data and control the dissemination of information, new private sector threats emerge. While fears concerning potential government abuse persist, the state also has the capacity to construct the rules to mitigate individual exploitation, formulating a consumer protection regime for the digital world.

The rules and norms associated with the collection, processing, and exchange of personal information, which fall under the banner of privacy, are essential to the digital world. With the rise of digital technologies, both the quantity and quality of personally identifiable information
have shifted. As each credit card purchase, web visit, and mobile phone log create a new bit of data, behavior becomes easily tracked. New moments of personal life become monitorable. From the webcam in the taxi to emerging genetic tests, these technologies erode the barriers between knowable and unknowable. They also permit the networking of previously discrete data. Information-intensive sectors, such as telecommunications, banking, and health care, are the first to rely on this wealth of personal information to customize products, rationalize costs, and minimize fraud. The supermarket clubcard typifies this line of innovation. With each swipe, the company is better able to target customers and lock in loyalty. The shift in a range of service industries, from marketing products to marketing customers, further demonstrates this trend. Where once an insurance firm marketed home policies, it now attempts to understand individual customer needs across a wide array of company products.

Improved consumer differentiation goes beyond mere efficiency gains, creating whole new potential markets. The emergence of sub-prime credit in the US, which allows financial service firms to offer high-interest rate credit to high-risk customers, is just one example. It is only in the early 1990s that personal credit information combined with complex computational programs permitted banks to differentiate interest rates across consumers. Similar information products are emerging in the insurance sector, with the rise of customized health care products. Reversing the logic of traditional credit cooperatives or risk pooling efforts, complex individuation offers firms the ability to profit from extreme differentiation.

The opportunities inherent in personal information processing threaten to erode personal privacy, however. As digital technology expands the quantity and quality of personal information available, individuals lose the capacity to control information flows. The boundary between public knowledge and private secrets shifts, leaving less and less room for the private. What worries privacy advocates most is the networking of formally discrete personal information for third-party economic gain. Information privacy deals fundamentally with an individual’s ability to control what is know about him/her not what is published about him/her. And therefore, it addresses at root how individuals construct their identity. If credit data banks cement early risky consumer behavior into a widely distributed consumer report, it is difficult for individuals to be free of the negative data profile. In short, a major concern of the digital age is the inability to forget, a fundament of most healthy societies.
Not only does digital technology shape an individual’s ability to construct his or her personal identity, but it risks creating, in turn, new brands of economic discrimination. Credit card firms amassing hundreds of interactions sub-sorted by purchase types could link their databanks with travel patterns available from electronic toll systems. This might be done innocently to offer a valuable customer an appropriate discount, but could easily be used for monitoring purposes. Similarly, one could imagine car insurance firms using mobile phone logs to track commuting patterns and potentially changing rates of individuals traveling through high-risk areas. The flipside to customization and risk reduction is the potential discrimination against those who are most vulnerable (Lieber 2003).

As the amount of information held by the private sector rises, the possibility also exists that governments will look to private sector data warehouses to enhance public sector surveillance needs. The recent JetBlue scandal vividly illustrates the potential harm that exists in the linkage between private sector firms collecting information and government bureaucracies hoping to advance security interests. In this case, the airline transferred millions of personal customer files to a defense department contractor, who linked the airline data to commercial databanks in order to construct risk profiles (New York Times 2004). Far from an isolated incident, governments across the globe are looking to private-sector data files like telephone or ISP records to monitor citizen behavior. As the line between public and private enforcement breaks down, traditional checks against government abuse are neutralized. The traditional fear of a government dominated Orwellian world is replaced by the specter of public/private partnerships of control.12

Such partnerships can operate in both directions. If the JetBlue scandal is a case of personal information gathered by a company being made available to the state, public policy has also compelled companies to make private information available to other business actors. For example, in attacking music downloading, the Recording Industry Association of America entered a series of lawsuits. To obtain the information on which the suits were based, the trade associate required access to the records of the Internet Service providers, the ISPs. The law as now written, the Digital Millennium Copyright Act, compels the ISP to provide access to that information on the basis of suspicion of IP violations, without court authorization or review. This constitutes the creation of a private posse enforcing its will in civil courts.
Such threats have not gone unnoticed by state authorities. Since the 1970s, with the proliferation of computer technology, lawmakers have recognized the danger inherent in the collection and storage of personal information. In response, nations across the industrial world adopted data privacy legislation. These rules have varied considerably, with the US focusing on public sector data usage and Europe constructing comprehensive regulatory institutions for the public and private sector (Bennett 1992, Regan 1995). As data processing has left the confines of a small number of government agencies in the mainframe era, the comprehensive structure has shone itself better suited at dealing with the explosion of data collection inherent in the digital era. In European countries, for example, it is very difficult for private sector companies to routinely share personal information with government security agencies. Data protection rules often prevent the collection of detailed information by firms, limiting the amount of information available for sharing. Recent disputes between the US and Europe over data privacy issues, ranging from telecommunications information to passenger flight records, demonstrate the importance of government policy in the development of very distinct information societies (Newman 2005).

Like notions of privacy, questions concerning free speech have been reopened by the emergence of digital technologies. While receiving fewer headlines than the economically more potent cases of property or privacy, speech issues lay at the cornerstone of modern political communities. By defining what can be said to whom, free speech rules shape an individual’s ability to express him or herself, maintain social networks, and organize politically. Free speech is invariably included in the catalogue of basic democratic rights, as the most critical arrow held by opponents of established power. Yet free speech is far from uncontroversial.

By altering patterns of communication and the capacity to transmit content, digital technology has transformed global debates about free speech. With the rise of international Internet connectivity, a resident in the US can as easily transmit information to a fellow netizen in Europe as to a local neighbor. As a result, differing cultural norms concerning criminal speech have come into conflict with one another. Most common among these are forms of obscenity, hate speech, and political protests. As digital connectivity permits citizens from one nation easy access to the media of another, jurisdictional conflicts emerge (Harvard Law Review 1999).

Technology has changed not only patterns of communication, but also the ability to control content. As previously described in the intellectual property discussion, digital goods are
naturally non-rival and replicable at no marginal cost. This has challenged traditional business models, spurring industry to use digital tools to increase the controllability of content. Through legislation and code, content providers have attempted to minimize the amount of IP available in the digital commons. This “second enclosure” restricts the fair use of information and in turn limits the free flow of ideas essential to free speech (Boyler 2003). It becomes much more difficult for activists to circulate news updates, for example, when they have to pay distribution fees to use this digital information. The state is left in the delicate position of determining which types of content individuals should be allowed to share.

Asserting control over content dissemination has been a critical feature of public policy in the digital era. The most famous case concerns the previously described DMCA. By criminalizing decryption technologies used to protect intellectual property, the US government hindered an individual’s ability to take advantage of fair use privileges. Many contend that by limiting fair use, the law will prevent the circulation of ideas necessary for democratic debate and political freedom (not to mention future rounds of IP innovation).

Potentially equally important for free speech have been policies concerned with harmful content. A distinct feature of modern society is the belief that certain information is dangerous and should be controlled through public policy. European governments, including Germany and France, have applied existing content laws to the digital era, for example, banning the sale of Nazi paraphernalia on the Internet. The firms selling such products are often located in countries with different laws. As a result, the application of content laws can take on an extra-territorial flare (Beesom and Hansen 1997). Far from technologically driven race to the bottom in standards, firms playing in international markets have been confronted by the projection of national rules through digital networks.

At the same time that governments have moved to control content, they have also actively participated in the dissemination of information technology. Access is no doubt a precursor for communication and participation. In the US, the E-Rate program was established, which subsidized broadband technology access in schools and rural communities (Newman 2003). Similarly, as discussed previously, the Korean government has been active in subsidizing the roll-out of broadband technology. While access is a critical component in overcoming the digital divide, the dissemination of digital technology should not be strictly equated with the promotion of free speech. It is still the case, that governments can promote technology diffusion,
while at the same time controlling (or supporting companies to control) the manner in which it is used (Kalathil and Boas 2003).

**Part IV. Government Efforts to Mediate the Transformation**

Given the continued importance of the state in the political economy of the global digital era, it is important to consider how state intervention shapes markets and societies. We identify three basic strategies that states have adopted in response to the challenges posed by information technology. First, governments may intervene to promote competition in the new marketplace, as technological change disrupts existing business strategies. States intervene to secure fair ground rules for the fights between dominant players and new entrants. These rules may emphasize equal market access, level regulatory playing fields, and transparency. The European Union convergence effort in the communications regime typifies this policy strategy. As media including telecommunications, radio, cable, and satellite compete head-to-head with one another for core digital products, market disruptions result from regulatory legacies. Telecommunications companies, for example, face very different regulatory burdens when entering new markets than cable companies. Universal service requirements mandate that telephone companies guarantee access to underserved communities, a cost not faced by cable companies looking to compete in broadband markets. The convergence process attempts to smooth over these regulatory differences and create a comprehensive regime for the digital communications industry. This strategy of getting the market rules right prioritizes procedural neutrality and long-term market competition over attempts to shield specific national champions.

In the second policy strategy, governments intervene to reassert incumbent market power. Digital innovations have the potential to upset existing business dynamics in a sector, threatening powerful industry groups. Policies in this strain attempt to shore up the pre-digital distribution of resources and prevent political coalitions from shifting. The DMCA offers the prototypical example of this form of state intervention. The DMCA criminalized the development and use of devices that may be used to break encryption systems. Technological solutions to intellectual property rights questions received legal support, consolidating the entertainment industry’s effort to reassert property rules in the digital environment. Despite intense lobbying efforts by new entrants from the information technology sector to curb the legislation, the government attempted to reassure the entertainment industry as a critical interest group. Similar international
efforts have been carried out by Western powers. The WTO’s Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) and WIPO agreements further insulate the intellectual property warehouses of incumbent players. The agreements provide firms international commitments and credible enforcement mechanisms to protect their intellectual property globally. Potentially viewed as a reactionary strategy, the second approach steers the political character of the digital transformation in favor of existing power centers.

A third strategy likewise attempts to shape the substantive character of emerging digital markets. Instead of bolstering existing interest constellations, however, the state recasts the balance of power in favor of public interests. The citizen consumer is empowered in the new digital environment, receiving increased control over information resources. Most easily identified with the mission of consumer advocates, this third strategy attempts to promote the public interest more broadly and to prevent digital innovations from further concentrating power in the hands of economic and government elites. Often motivated by political fears that individuals will reject new technologies and thereby stall economic development, this approach emphasizes state safeguards that protect and assure citizens. The European Union data privacy directive provides an important international example. With the explosion of personal information in the digital age, the directive provides individuals with a clear level of control over industry and government data processing. Before a company or a bureaucracy may transmit personal information to a third party, it must obtain consent from the individual in question. If an organization fails to obtain consent, that organization can be punished by the data protection agency. While not eliminating the commodification of personal information, European regulations reset the default position in favor of consumers. Governments, promoting the third potentially populist or progressive option, channel the transformation so as to rebalance societal relationships prioritizing citizen concerns.

Part V. The Politics of State Regulation of Digital Technologies

The digital revolution has reopened fundamental societal debates and in turn brought a reexamination of the role of the state in the emerging political economy. As firms use digital technologies to create advantage or position in their markets, old political economy bargains are undermined. Often, new entrants see opportunity in the technological disruption, incumbents struggle to hold onto old business models, and public interest groups fight to maintain or expand
consumer rights. Amidst the commotion, governments, as explained in the previous section, begin to formulate policy strategies that inevitably implicate the distribution of business opportunities.

The dynamics of these political debates are complex. In addition to the state, business lobbies and public interest groups struggle within a given political institutional environment to construct the emerging rules of the digital economy. In order to understand the variation in policy results across countries and internationally, it is vital to identify the roots of business sector and public interest preferences. In short, we contend that the organization of economic and public interest sectors influences their preference formation and their relative stake in digital debates.

Several caveats about business and public interests are important to keep in mind, as we examine the preferences of various political actors. Business interests may be driving the process of reformulating rules for a digital age, but there is no unified business position. There is certainly no “digital sectoral” interest, let alone a class interest. To start, firms have different preferences and positions on the same issues; competitors in networks seek to turn the rules to their advantage; companies building and using different technologies, or at different positions in the market, have quite distinct needs.

But there is more to the story. As Abraham Newman has shown in his work on privacy, the business interests of financial institutions depend not only on the market problems alone, but also on the corporate organization of the firms themselves (Newman 2005). This organization is partly a business choice and partly a result of regulation. Integrated financial institutions, as in France, do not depend on information commodity markets to gather the information they need to market to their customers. French financial institutions rely instead on their internal warehouse of information to target customer needs. By contrast, the highly fragmented character of financial services in the US reinforces demands for a market in commodity information. So interests may be definable, but they cannot be read off a market map in any simple way.

Similarly, public interest groups have been at the forefront of many digital policy debates across the globe. But their level of engagement, their policy goals, and their lobbying strategies differ dramatically across countries. Compare the work of the most active public interest groups in the US, such as the Electronic Privacy and Information Center and the Electronic Freedom Foundation, to that of their counterparts in Europe, like data protection or consumer protection
bureaus. While the goals appear identical, guaranteeing a social agenda for an information society, the logic of their tactics (e.g. class action suits and media scandals versus negotiated technocratic bargains) vary and are in a very real sense shaped by their institutional settings.

Not only do their tactics differ, but the capacity of players to influence legislative debates varies across policy landscapes. In the US, broader public interests are represented in only a limited way in the struggles over digital rules. Certainly, the narrow business story of the emergence of electronic commerce and the tools to conduct commerce using networks has become entangled with the broader political struggle over fundamental values, goals, and processes and jurisdiction. But at least in the United States, oversimplified, it is a story of business seeking new rules to implement the digital technologies, with public interest groups seeking to influence the character of those rules. More often than not, groups defending general principles, such as privacy or consumer protection on the network, enter the fights in response to business-initiated or -proposed rule changes. None have mobilized effectively on a mass basis and, as a result, there is no digital equivalent of the environment movement.

The US debate is driven by markets and market actors and therefore has the flare of business dominating the political debate. Elsewhere, public interest voices are fitted differently into the political system, either through a formal institutional position or through political parties. This positioning may force trade associations to respond to legislative agendas pushed by consumer interests. Two examples prove illustrative. The role of the Green party in Germany has radically altered the place of consumer groups. This small party, a member of the governing coalition since 1998, has successfully raised consumer protection to a cabinet responsibility. At the European Union level, consumer interests have been institutionalized in the consumer protection directorate, elevating public interest demands within European policy debates. As a result, industry is stuck in the position of responding to positions placed on the table by consumer advocates, who at the same time often have an ear of the European Commission or national governments (Young and Wallace 2000).

These differences force us to at least open the basic question of how political groups form and how their interests are defined. Because business now operates globally, because markets and products cross borders, these domestic battles for values and principles, from privacy through the right to expression, will have to be fought again and again -- and the terrain of political battlefield will be much more varied, more complex. Political strategies will now
involve cross-national coalitions and deals in international institutions to settle what were once exclusively domestic decisions. Indeed, the creation of interests in the whole array of digital cases emphasizes that interest groups are never mechanical functions of markets or institutional structures, but rather the product of political struggles.

**Part VI. Conclusion**

It is clear that new deals are being struck, but the content of these deals is not compelled in any consistent way by the digital tools and networks themselves. Rather, the state finds itself struggling to manage digitally-inspired conflicts fueled by business and public interest groups. As technology reopens debates, governments have varying policy tools at their disposal and confront distinct policy legacies. One should, therefore, expect to see different government approaches to basic digital fights. Not only will proposed government solutions vary, but these proposals will be filtered by each country’s unique political configuration. The cross-national diversity of policy debates will reflect market conditions and problems, but more fundamentally the distinct organization of the public and private sector lobbies involved. Owing to the transnational character of digital markets, these varying state positions will naturally shape international negotiations.

Information and how it is used is the very substance of communities, polities, and markets. Communities can be conceived and indeed expressed as the character and flow of communications amongst members, polities as systems of decisions based on information, and markets as architectures for exchange based on information. Consequently, even the technical rules about digital technology and the digital market are directly and simultaneously decisions about the very nature of the community and the polity.

The state has played a fundamental role in the emergence and development of the digital era. As in the case of the great transformation, government policy has created the infrastructure for the fictitious commodity of information. Through a series of deregulation, market-making, and reregulation, public policy has constructed the rules for the new market and managed conflicts that threatened to derail the digital revolution. These efforts have had important political consequences for the character of the contemporary transformation. And given the differing ways governments have dealt with the various challenges posed by this digital transformation, several distinct information societies will no doubt emerge.
Bibliography


Bennett, Colin, Regulating Privacy (Ithaca: Cornell University Press, 1992)


Lewis, Peter, "Limiting a Medium Without Boundaries: How Do You Let the Good Fish Through the Net While Blocking the Bad?," The New York Times January 15, 1996.


Marsden, Christopher, *Regulating the global information society* (New York: Routledge, 2000)


Richardson, Tim “South Korea Broadband in League of its Own,” *The Register*, October 14, 2002. Available at www.theregister.co.uk


---


2 The work of Claude Shannon and Norbert Wiener in a real sense defines the information age. Those notions precede and underpin the computer itself. Weiner defines cybernetics, or the theory of messages, as the “entire field of control and communication theory, whether in the machine or in the animal.” The development of messages and communication facilities, both man to machine and machine to machine, will play an ever-increasing role in our society. In cybernetics, Weiner argues that the “structure of the machine or of the organism is an index of the performance that may be expected from it.” Analogous to humans, communication machines use feedback mechanisms to reduce entropy and maintain effective communication (Weiner 1954, 1965). Shannon contends that predictable symbols can be omitted from communication. Information, or “those symbols that are uncertain to the receiver,” measures an information source’s entropy. Entropy, in turn, “determines the smallest number of bits per symbol that is required to represent the total output” (Shannon 1993).

3 The use and application of transformative technologies alter the array of activities in the economy as a whole. The diffusion of these transformative technologies is undoubtedly the critical step. It is not just the fortunes made as the leading sector expands, but also the industrial development that transformative technologies engender, as Brad DeLong points out (see endnote 2).

4 See John Gilmore as quoted in (Lewis 1996). See also (Barlow 1996). Manuel Castells makes a more nuanced argument that the rise of complex networks has limited the power of the state (Castells 1996).

5 For a more general discussion of the role of self-regulation in the early years of the Internet, see (Marsden 2000). For the role of the state in shaping the character of self-regulatory efforts, see (Newman and Bach 2003).


7 Thanks to Steve Weber for the reference to Stewart Brand.

8 For the important role states have played in resolving international challenges posed by digital technologies, see (Drezner forthcoming).
For a discussion of the political development of telecommunications liberalization see (Cowhey 1990).

Our thanks to Jonathan Sallet for this point.

For a discussion of the DMCA as well as its implications for fair use, see (Pamela Samuelson 1999, David Nimmer 2000).

For a review of privacy concerns in a digital age see (Newman and Bach 2003).

There are exceptions, of course. One is the present debate about the effort to restrict telemarketing calls in the United States, which has mobilized a broad constituency. But even this issue, which receives almost universal popular support, has faced a harrowing road to implementation, including multiple court injunctions that threaten to derail a consumer-friendly outcome.

Our thanks to James Boyle for this observation.