Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce

Detlev Zwick, American University
Nikhilesh Dholakia, University of Rhode Island

September 7, 1999

Introduction

> A child-directed site collects personal information, such as a child's full name, postal address, e-mail address, gender, and age. The site also asks a child whether he or she has received gifts in the form of stocks, cash, saving bonds, mutual funds, or certificates of deposit; who has given these gifts; whether monetary gifts were invested in mutual funds, stock, or bonds; and whether the child's parents own mutual funds (Federal Trade Commission report to Congress, 1998).
>
> To see without being seen is the definition of modern power (M. Foucault).
>
> You have zero privacy. Get over it! (Scott McNealy CEO Sun Microsystems).

Current discussions of the Internet, the Information Super Highway, Cyberspace, and increasingly, E-Business, involve the issue of privacy. Advances in information and communication technology are perceived to threaten the individual's privacy more consistently and pervasively than ever before (DeCew, 1997). Debates surrounding privacy protection in electronic environments, however, are not new. In fact, concerns about what the Americans call *privacy* and the Europeans *personal data*[1] (Lyon & Zureik, 1996) have been raised repeatedly since the invention of the modern computer. In Europe and the United States, elaborate bodies of law as well as a structure of non-legislative rules and regulations have formed around privacy issues.

Such debate notwithstanding, privacy issues were not very salient with earlier forms of information and communication technologies because such technologies could be described as closed systems (Sassen, 1999). This has changed dramatically with the advent of the Internet. The Internet is not only an immensely larger network than any previous communication network in history, it is also an *open* and *decentralized* system in which data protection and risk management are difficult to goals to achieve, for individuals as well as companies (Aspen, 1998).

Furthermore, the digitization of our communication environment must inevitably transform our notion of subjectivity and knowledge (Robins, 1999). Thus, instead of 'the consumer,' we should talk about 'the *digital* consumer.' Complex relationships between human beings and their digital representations are captured and transformed as "digital consumer shadows" by computers[2] (Agre, 1994a; 1994b). In the "knowledge space" of "cyberculture" (Levy, 1997), then, knowing the consumer becomes a matter of capturing bits and bytes (hardware and software profiles, click streams, previous visits or purchases at own and other sites, etc). Clearly, this is much easier for firms in an open and decentralized virtual marketplace than the conventional world of brick and mortar commerce. For consumers, however, protecting their personal information becomes increasingly difficult.

Consumers have met this new communicative situation with some worry, demonstrating that privacy is important to them. Recent polls asking citizens/consumers whether they believe that the advancement of new information technologies poses a threat to their privacy invariably find that people are concerned about losing control over their personal information[3] (e.g., Harris & Westin, 1991). In the 1998 round of the ongoing GVU surveys, for the first time privacy outranked censorship as the number one concern regarding the

Internet. Pursuing the meaning of privacy in this new brave world of computer power is important for consumers, marketers, and public policymakers. Indeed, despite definitional difficulties, privacy provides what Lyon and Zureik (1996, p. 16) call a "mobilizing concept to express real social anxieties and fears."

Privacy in the Age of *Dataveillance*

A debate about privacy is, of course, tightly linked to the "other side" of the same coin: surveillance. "The term *surveillance* typically implies the direct and physical monitoring of the behavior and communications of one or more persons" (Bennett, 1996). Traditionally, we think of surveillance in terms of spying and listening devices but the convergence of new information technologies and new communications media has created a novel, in a sense incorporeal, form of gathering personal data. Roger Clarke (1994) has coined the term *dataveillance* to describe the fact that the workings of this invisible surveillance are based on the facility of new technologies to collect and store enormous amounts of personal information. It is important to emphasize, however, that the practice of surveillance is much older than surveillance technology and thus not *caused* by such technology. It is the processes of modernization – formation of nation-states, growing population, increasing individual mobility, rise of bureaucracy and administrative power, increase in *indirect* or impersonal social relationships – that gave rise to the need for state control and to the collection of massive amounts of data on its citizens (see Foucault, 1977; Luhmann, 1997). The spread of dataveillance is indeed rooted in the modern rationalities of bureaucratic societies so cogently analyzed by Max Weber (1947). It is the complex dialectic between new technologies of surveillance and bureaucratic objectives that has created a form of mass dataveillance that warrants increased attention to privacy concerns.

A frequent concern is that in "the age of [digital] marketing" (Firat & Venkatesh, 1993) personal information about individual consumers can be gathered, stored, and exchanged much more easily and freely. From a business perspective it is easy to discern the commercial interest in gathering consumer data electronically. Marketers need data for such tasks as market segmentation, profiling, personality projections, and database matching (Clarke, 1991). To cite a few examples:

- In 1991, Lotus Development Corporation marketed a CD-based database of household marketing data called MarketPlace:Household, which allowed easy access to the personal data of more than 120 million Americans (Kling & Allen, 1996).
- Microsoft's attempt to issue their Windows 95 operating system with a built-in mechanism that automatically accumulates data about users' hardware as they register their software brought sharp criticism from computer users.
- At one point in time, Intel's Pentium chip embedded a code that could transmit back the IP address of the computer to the manufacturer.
- For a while, Amazon.com published "profiled" buying habits of groups such as Microsoft employees or users at Stanford University.

Recent news about insurance companies, e-tailers, and banks that have sold consumer data from their massive databanks to third parties has added fuel to the debate about information proliferation. In the daily news media stories abound reporting yet another case

of data protection failure, "privacy invasion", or database sell-out. In almost Orwellian proportions, the consumer is depicted as the defenseless victim whose privacy is subjected to insurmountable corporate power and at the mercy of faceless data miners (The Economist, 1997). But why is privacy and personal information so important for consumers and marketers alike?

Purpose of the Paper

Privacy, Arnold Simmel (1971, p. 71, italics added) states, has a "ramified and intimate relationship to the whole structure of human interaction and values, and to the nature of individual personality […] *If privacy changes, much else will change.*" Thus, the implications of "Big Brother" narratives on the development of consumer anxiety and mistrust must not be underestimated. Consumers believe that in the maelstrom of digitalization and automatization they have lost control over their personal information (Reidenberg, 1995). Because of new technologies such as the Internet global interconnectivity has increased dramatically. It "allow[s] a more promiscuous range of connections among strangers on a global scale" (Aspen, 1998, p. 30) and a more diffuse quality of relationship as well.[4] To counter the erosion of trust in the new information technology, business – particularly the e-business sector – has embarked on the project of building a new "trust infrastructure".

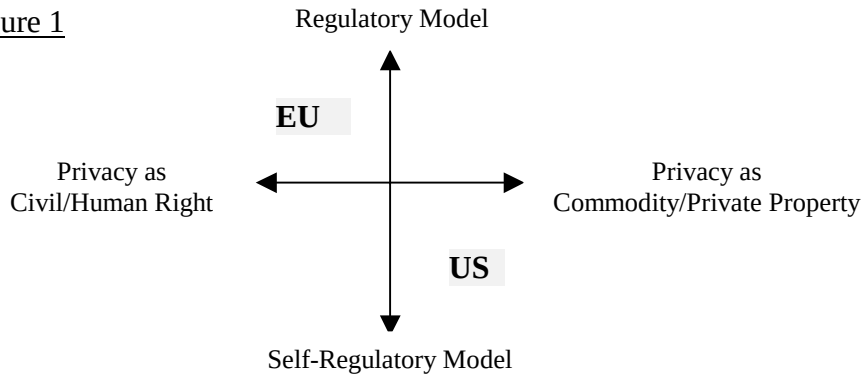
The obvious dilemma is that to conduct sound business, without delving into each other's private affairs, buyers and sellers must be able to authenticate each other's identity (Paquin, Zwick, & Dholakia, 1998). For this, information must be exchanged between the two parties. For consumers to develop trust in the transaction partner and the transaction itself, s/he must have ways to assess the reliability of the information exchanged. Also, the consumer "must feel confident that Web sites are not surreptitiously collecting private information about them or sharing it with third parties without authorization" (Aspen, 1998, p. 31). New interactive technologies, on the other hand, make it enormously seductive for marketers to do precisely that – collect information unobtrusively and use it for highly targeted marketing communications.

To address these and other consumer concerns about data protection and privacy, two opposing models have emerged from the current debates (see Swire & Litan, [1998] and our more detailed discussion below):

1. The "regulation model" proffered by the European Union (EU) administration. Here, the EU representatives believe that standardized privacy protection regulations (eventually on a global scale) are necessary in order to guarantee security for consumers. Moreover, because security and privacy protection issues concern the status of the *individual as citizens* before they concern the status of the *individual as consumer*, these regulations must be developed in the political arena (as the representation of the citizens' will) and then imposed onto the economic sphere. In other words, privacy is regarded as a basic civic right.
2. The "self-regulation model" supported by the business communities in USA and the EU as well as the Federal Communications Commission in the United States. This view holds

that the best way to secure consumers' privacy in cyberspace is via the virtual marketplace itself. Instead of government regulations, self-regulation is the preferred way to address and enforce the multitude of privacy concerns. In other words, competition and free market will encourage consumers to make deliberate choices favoring businesses that differentiate themselves by their high privacy protection standards. Under this model, privacy is to be seen as the property of the individual (see Figure 1).

Figure 1



In this paper, we interrogate the differences of the regulation and the self-regulation model by asking:

1) What does it mean for consumers and marketers when a particular model of privacy protection (i.e., Regulation vs. Self-Regulation) is combined with a particular definition of privacy (Human or Basic Right vs. Commodity or Private Property)?
2) What are the consequences of one model as opposed to the other for marketers and consumers?

Before we can answer these questions, we first have to outline the role new information technologies have played in bringing the concept of privacy so forcefully back into the public discourse. Then, we turn our attention to the concept of 'privacy' itself, by looking at its historical, anthropological, and legal roots. Next, we outline the two competing privacy models by focussing on their key texts, the *EU Directive of Privacy Protection* and the *Federal Trade Commission 'Online Privacy' Report to Congress*. Finally, we discuss the implications for marketers and consumers.

Information Capitalism and Marketing

Rob Kling and Jonathan Allen (1996) have detected that the exchange of information dominates the contemporary market place. However, they regard the expansion and use of computer technologies for large-scale record keeping not as the central mode of capitalist production but as a by-product of what they term *information entrepreneurism*. In *information capitalism*, then, marketing managers are trained to exploit information systematically, thus becoming information entrepreneurs. Kling and Allen believe that a general cultural shift has taken place in the economic field, including business schools[5], to teach and pursue marketing and management strategies that depend upon data-intensive analysis techniques. Expert information systems are now in place in many companies helping

them focus their production and marketing. Put simply, computer power has become synonymous with economic power and competitive advantage.

Information entrepreneurial companies, by aggressively developing and adopting commercial surveillance technologies such as the ill-fated Lotus MarketPlace:Household database (Kling and Allen, 1996), develop a “superpanopticon” of surveillance. This superpanopticon, Mark Poster (1990a) explains, effects its working almost without effort. But what are its workings? The superpanopticon, derived from Foucault’s (1977) notion of the panopticon, is used as a metaphor to describe the role that surveillance plays in the new information capitalism. According to the theory of the panopticon, databases, communication and information technologies, and two-way streams of data have implicated the individual into a web of electronic surveillance, unbeknownst to him or her in many instances (Poster, 1990). This modern form of surveillance differs therefore from earlier forms quite dramatically. Now, “the target of surveillance initiates the cycle of observation by his or her own actions, for example, placing a card in a reading device, signing on to a database service, calling a toll-free phone number, or mailing a response card or form” (Gandy, 1996, p. 138). As Gandy (1996) points out, marketers are at the forefront of these new developments. Every time a consumer interacts with the market system, he or she leaves valuable traces about purchases, investments, mortgages, and debts. These traces become the basis for the “panoptic sort” (p. 134, emphasis added):

> [It], as a complex technology, includes not only the computers and telecommunications systems that facilitate the collection, storage, processing, and sharing of personal information, but also *the analytic approaches that differentiate, classify, segment, and target individuals and groups* upon the basis of models, assumptions, and strategic orientations that demand the maximization of profit and the minimization of risk.

Thus, the superpanopticon erected by the new information entrepreneurs allows personal data to play a distinctive role in the modern STP (segmenting, targeting, and positioning) marketing process (Kotler & Armstrong, 1996). With such a powerful tool at their hands, marketers are able to identify and classify prospective customers with tremendous accuracy. As a result, marketers can administer rewards and punishment to the market participants in order to reduce uncertainty about the future behavior of consumers (Gandy, 1996). On the other hand, the real and potential threats to consumer privacy are clearly evident, particularly when the operations of the World Wide Web are inserted into this existing panoptic structure of technological power and culture of informational entrepreneurism.

Space and Subjectivity in the Digital Age

The digital age has transformed our understanding of producing, storing, accessing, and sharing information. "Being digital" means first and foremost the transformation of matter[6] into electronically generated binary structures of zeros and ones (Negroponte, 1995). Once matter has "gone digital" it can also be *stored* and *transferred* at the level of numbers or digits (Lunefeld, 1999). This is the crux of the digital revolution because at the level of the code a vast variety of different information becomes reduced to the "same." At this point, all information can be stored, accessed, and exchanged by the same equipment and digital matter (i.e. information) becomes free-floa(t)ing. This fluid nature of data accounts for the efficiencies of electronic information networks interconnecting universities, government institutions, corporate players and individuals.

In the age of digital networks (Sassen, 1999), consumers have come to understand space as divided into the physical and the virtual, the material and the electronic (Mitchel, 1999). The production of virtual space, as the production of any space before, must be followed by the production of new consumer ontologies (see Lefebvre, 1991), where the experience of consuming and being a consumer is distinctly different from any other "consumptionscape" (Ger & Belk, 1996). Indeed, Turkle (1995) demonstrated that cyberspace not only creates new ways of being-in-the-world but that these new modes of existence can be as real (if not realer) as life in physical space.[7] Thus, even on the Internet, we are dealing with complete consumer subjects in the modern sense.[8]

In addition, digital networks are mapping out electronic spaces in a traditional geographical sense, thus creating openness as well as segmentation, decentralization as well as monopolization (Cowhey, 1995; Luke, 1999). Digital geographies are connected through large streams of data, which must be organized. An array of increasingly sophisticated "autonomous agents" (AA), a sort of "software robots" and so-called knowbots, software and interface agents, which "inhabit" the digital world of computer networks take on the role of organization (Rotzer, 1995). Fields of application for such autonomous agents are literally unlimited. For example, AA's have been developed to oversee and control digital spaces such as the World Wide Web as well as monitor streams of communication like email. Thus, while the ability for data exchange has increased with the digital age, so has the capacity for surveillance.

Clearly, nothing has shaped our view of network power and electronic space more than the properties of the Internet. Since the mid-1990s, after an initial period of innocent exploration dominated by the computer hacker culture[9], business has discovered the Net and successfully begun to commercialize its chief properties: speed, simultaneity, and interconnectivity (with other businesses and consumers). Especially, when the World Wide Web became available in 1993, commercialization exploded on the scene. Therefore, at the end of the millennium we find ourselves in a particular moment in the development of digital networks. As Saskia Sassen puts it (1999, p. 52/53), "[S]uddenly, over the last few years, the two major actors in electronic space - the corporate sector and the civil society - which until recently had little to do with one another in electronic space, are running into each other."

Of course, companies in the past have had private computer networks in which data was generated, stored, and exchanged, such as Electronic Data Interchange (EDI) or Direct Data Interchange (DDI).[10] But only the Internet caused the polarization between the public (civil society) and the private (economic activity) sphere to become blurred, creating a mixed public-private sphere. The increasingly global electronic sphere of the public-private brings to the fore that information previously shared only among a small group of people of a certain age, class, ethnicity, gender, or any other subgroup has now been thrown into a public forum (Meyrowitz, 1985). This hybridization of electronic communication, bringing the private to the public and the public into the private, is driven to a large extend by the forces of commercialization (Bondebjerg, 1996). For Habermas (1990) the hybridization of the public and the private has a negative connotation. It means that the commercial forces have succeeded in suppressing the vibrant intimacy of the life world.

Not surprisingly, the formidable invasion of everyone culture by the new information technologies (Kroker & Kroker, 1996) causes a particular type of "privacy mistrust" that can be understood in the larger context of "civilization skepticism" questioning the metanarratives of progress and modernity (Jones, 1997). The fear, expressed by citizens,

workers, and consumers, concerning the symbiosis of new information technologies and capitalism, is that it creates a new infrastructure of surveillance (Andrews, 1996; Bogard, 1996). As digitized information in the government's or direct marketers' databases, a citizen or consumer is never "outside of reach." This concern for privacy issues demonstrates that even in the new brave world of digital databases and the Internet, individuals distinguish between their private and public existences and wish to keep them separated.[11]

Critically, for the purpose of our paper, where we look at the struggle over **models of privacy protection and definition**, it is irrelevant whether these claims about fear and surveillance are "true" or not. Singularly important is the fact that the fear of "losing one's privacy" is **real** among consumers using new communication technologies such as the Internet and that this fear must be addressed. In other words, not whether consumer privacy is or is not actually imperiled but how it should be defined (civic right or commodity/personal property) and protected (e.g., regulation or self-regulation) is the focus of our analysis. To understand why privacy is so important for consumers and consequently plays such a central part in the recent discussion surrounding e-business, it is instructive to take a look at the origin of the concept and its current meaning.

Origin and Meaning of Privacy

A Brief Social History of Privacy

Privacy cannot be discussed without at the same time looking at "publicity" or the public sphere (Habermas, 1991). The distinction goes back to the Greek and Roman civilizations of the antiquity. However, while the Greek honored the public sphere and sacrificed the private to the life in and for the *polis*, the Romans believed that the public life of *res publica* could only thrive in a synergetic coexistence with the private. Thus, as Hannah Arendt explains (1998, p. 59), "[T]he full development of the life of hearth and family into an inner and private space we owe to the extraordinary political sense of the Roman people." The Romans saw the private as the place where one feels sheltered against the world. Indeed, to be political (i.e., participating in the public discourse) in Rome meant to attain the highest contemplation of human existence, "*to have no private place of one's own meant to be no longer human*" (Arendt, 1998, p. 64).

After the antiquity, Christian morality continued to uphold the high esteem for personal privacy. While Christianity's fundamental religious perspective is one of public service (the duty of *Caritas*), it has always "insisted that everybody should mind his own business and that political responsibility constituted first of all a burden" (Arendt, 1998, p. 60). Interestingly, as Arendt points out, the secular modern age did not abandon this essential Christian morality. Marx for example, surely no supporter of the private *per se*[12] believed that the purpose for privacy (protection from the public) would disappear with the withering away of the state, i.e., the whole public realm. As the state did not wither away but developed huge bureaucracies of public administration (Weber, 1947), the public sphere gained increasingly on importance.

The emergence of stock market and print media caused increased traffic in goods and news forging new social and economic relationships of private power, which confronted the public power of the state administration. As a result, society, for the first time in history, came to be differentiated from the public power. Finally, in the developing liberal model of

public sphere, basic rights were worked into the first modern constitutions guaranteeing society as a sphere of private autonomy (Habermas, 1991).

Definitions of Privacy

Patterns of privacy, as evidenced by anthropological research, may differ significantly from society to society (see Roberts & Gregor, 1971). In other words, what people esteem to be private matter and what not depends on social, cultural and political factors. However, while the components of privacy may be a question of cultural particularity, the definition of privacy can be expressed in general terms as the restriction of information diffusion. Here, we follow Alan Westin (1967, p. 7) in our use of the term "privacy," who said that "privacy is the claim of individuals, groups or institutions to determine when, how, and to what extend information about them is communicated to others."

Such a definition, of course, would remain anemic without a clearer understanding of what exactly counts as *private information*. Stanley Benn's (1971) example of a couple kissing in the bushes to hide from the public, thus acting *privately*, or *in private*, is instructive in delimiting the terms private information, private affairs, or privacy. Although the couple's act may have meant to be a private affair, the two could later decide to share this experience with someone else at which point the private matter becomes public. Moreover, the couple could have been watched by a passer-by all the while they were kissing in the bushes at which point their sensation of privacy would have been a fallacy. But, Benn (1971, p. 2) believes that one's private affairs are private in different sense:

> It is not that they are kept out of sight or from the knowledge of others that makes them private. Rather, they are matters that it would be inappropriate for others to try to find out about, much less report on, without one's consent; one complains when they are publicized precisely because they are private.

Such a definition of privacy is norm-dependent because private affairs cannot be identified without some reference to norms. Such a norm would restrict unlicensed watching, listening, or reporting by someone uninvited.

This is an important qualification because there is nothing inherently objectionable about observing the world, writing down and disseminating one's findings, unless it is being done without the permission of the observed. Furthermore, of course, there is always the possibility hat the information may be used to harm someone, although this is not a necessary requisite. Thus, scrutiny as such may not be offensive but unlicensed scrutiny, whether harmful or not, could still be regarded as an impropriety.[13]

Benn (1971, p. 8) suggests that a general principle of privacy might best be grounded on the more general principle of respect for a person. By tying private affairs directly to the concept of "person," Benn convincingly argues that a person's privacy means the control over one's *personal information*. In Western consumer cultures such as the U.S. and Europe where a person's possessions are regarded as an extension of him- or herself (Belk, 1988), personal information has at least two important components: 1) demographics and psychographics as well as 2) personal consumption practices (Solomon & Englis, 1997). Consequently, within the normative structure outlined by Benn, unlicensed watching, listening, reporting and sharing of a person's consumer behavior clearly accounts as a violation against respect for privacy. As Jones (1997, p. 135) asks with some apprehension:

> Will just any one be able to mine the streams of data that contain our account balance or medical files? Will he [sic] be able to intercept my credit card information while it is being sent from virtual store to virtual store? How can we prevent that? What is going to happen with all the data that we send out? Because data are relatively easy to safe, will every message we sent out and receive be stored in a big universal archive?

Of course, such concerns are not new and have followed every new development in communication technology from the introduction of the press to the invention of television, as people actually believed that someone on the other side could see you in your living room.

An interesting thesis advanced by Walter Ong (1987) suggests that underlying all the concerns with new technologies is the increased "duration" of communicated data except the one transmitted orally. Once a word is spoken it is gone, except in our memory (which evidently we trust less and less[14]). But information conveyed in written form can be stored in databanks and archives for a long time. Thus, one's concern with privacy is actually one's concern to externalize personal information for a more or less extended period of time. Once our information is outside ourselves it is also out of our control just like the picture, taken from us no longer belongs to us but the photographer (Jones, 1997).

Personal Information: Individual Strategies for Protection

Privacy, it is important to understand, is not only the attempt to protect the personal information that is somehow "in" a consumer, but to control what "leaves" the consumer to enter territories that are external to their private sphere. Moreover, as Jones (1997) points out, at the core of privacy protection is to control that, which indeed enters someone's private space. The Internet, as general metaphor for the penetration of the information age into consumers' lives, threatens the protection of their personal information (DeCew, 1997). Participation in the networked (online) society divests every consumer of both much control over the flow of externalized information and its metamorphosis in the commercial electronic space (Cavoukian & Tapscott, 1997; Lyon & Zureik, 1996). To overlook this fact would mean to ignore that consumers are public beings regardless whether they use our scanner card in the local supermarket or browse the World Wide Web.

With or without some kind of regulation, consumers, attempting to reclaim some control over their personal information in the networked society, are to a degree always left "to their own devices" (Lievrouw, 1998). There are many reasons, why consumers might be concerned about constructing a particular virtual self and engage in a specific form of impression management.[15] Whether for protection or impression management, consumers adopt various strategies that allow them to control the *amount* and the *accuracy* of personal information they externalize (see Goffman, 1959, p. 141-166). Building on Gary Marx's (1999) conceptualization of "identity knowledge" we propose four different strategies consumers apply to protect and manage their virtual selves (see Figure 1)[16]. First, *identifiability* refers to the consumer's disposition to disclose all personal information with high accuracy, thereby allowing others to acquire a high degree of identity knowledge. Identifiability is therefore the least powerful strategy for protecting personal information. *Confidentiality* denotes the disposition that supports the externalization of a restricted but highly accurate amount of information. It is based on trust between two or more parties. *Pseudonymity* is the strategy that enables the consumer to externalize infinite[17] amounts of inaccurate personal information, while *secrecy* expresses a disposition toward the sharing of little and potentially inaccurate information.

a)

Figure 1:

Amount of Personal Information Externalized	Accuracy of Personal Information Externalized: High	Accuracy of Personal Information Externalized: Low
High	Identifiability	Pseudonymity
Low	Confidentiality	Secrecy

Apart from secrecy perhaps, individual strategies of protection should not be overestimated. While dispositions of confidentiality and pseudonymity allow the individual to safeguard some types of personal information such as demographic and, to a degree perhaps, psychographic data, they can hardly keep behavioral information from being gathered. In other words, even without personal information, marketers can still trace and analyze a consumer's "click stream" on the World Wide Web, devise a user profile of preferences, interests, and tastes and link it to a (still unknown) person. But a consumer can only remain unknown as long as no transaction is being made. Thus, behavioral data is the most precious data "out there" and all marketers really need in the electronic environment to link digital consumer shadows to real persons. In the World Wide Web's transactional space, the consumer has to revert to identifiability or confidentiality at which point information is out of the consumer's control.

In sum, current individual strategies of privacy protection outlined above offer only a partial solution to the imposing loss of command over personal information in digital networks. It seems that no complete privacy control can ever be attained by the consumer him- or herself. Therefore, other ways of coping with consumer privacy must be found. Two models, the regulation model and the self-regulation model, have been introduced as possible solutions. In the following section, we introduce these models in more detail and discuss their fundamental meanings for consumers, marketers, and the interaction between them.

Models of Privacy: Regulatory versus Self-Regulatory

The two models of privacy protection that have evolved on either side of the Atlantic are based in two different philosophies. The European Union has taken the stance that regulation is essential to provide protection for citizens in the marketplace, e-commerce and regular commerce. The United States on the other hand has so far largely refused to pass legislation to regulate privacy in commercial areas. With a few notable exceptions, the FTC and the White House have both issued strong statements favoring self-regulation for commercial privacy issues. Based on Swire's (1998) framework, regulation and self-regulation can be distinguished along the three traditional components of separation of power: legislation, enforcement, and adjudication. Legislation refers to the question of who should define

appropriate rules for protecting privacy. Enforcement refers to the question of who should initiate enforcement actions. Adjudication refers to the questions of who should decide whether a company has violated the privacy rules. Whether self-regulation or regulation is in place can be judged according to the handling of these components (see Table 1).

Table 1:

Forms of Power	Self-Regulation	Regulation
Legislation	Industry-drafted rules and regulations (e.g., Bar Association Rules).	National or supra-national legislative act.
Enforcement	Industry-drafted rules and regulations often do not provide for legal enforcement and is instead undertaken by industry organizations.	By governments appointed neutrally policing institution.
Adjudication	Industry organizations can use their involvement credibility to decide over violations.	The courts decide over violations.

Self Regulation

Self-regulation involves the setting of standards by an industry group or certifying agency and the voluntary adherence to the set standards by members or associates. The Better Business Bureau as an example has set standards of ethical business practice and organizations displaying membership seals are, by so doing, expressing their compliance with the agreed upon standards.

There are some advantages to self-regulation in a particular industry. The industry members are intimately familiar with the peculiarities of their work and are in a position to have considerable impact on the behavior of their members. In the legal profession, for instance, the Bar Association has set standards of behavior and the influence of these is pervasive throughout the profession. This example also demonstrates an instance of compliance being voluntary, yet essential for performance within the area. It also demonstrates the ability that self-regulated industries have also developed in some cases to take punitive action with regard to its members.

In the area of marketing, the Direct Marketing Association has taken a strong self-regulatory position. The DMA's self-regulation is an attempt to create a fair social contact by providing customers with knowledge and control (Culnan1995 in Milne 1997).

Government Regulation

The EU Directive on Privacy Protection is a legal description of the treatment of information acceptable to the fifteen European Union member nations (Swire and Litan 1998). The Directive is a set of laws dealing with privacy issues. There are 33 Articles, of

which the most notable for stakeholders outside the EU is Article 25 which prohibits the transfer of information out of the EU to any organization that cannot satisfy the EU demand for protection as described in the Directive. The Directive became effective on October 25, 1998. Many points must be neglected here but those most important for our discussion are summarized below. The directive

- *Imposes obligations on data controllers*. Those who process personal data, such as corporations on customers and employees; hospitals on patients; and book/record clubs on customer preferences. The directive also provides data subjects with certain rights to ensure that data are not misused.

- *Is all encompassing, since "processing" is defined broadly to be any operation performed upon personal data*. This can include, by automatic means or not, the collection, recording, storage, alteration, retrieval, consultation, disclosure by transmission and erasure.

- *Is intended to "approximate" rather than "harmonize" national privacy laws.* It establishes a basic framework of data protection principles and the regulatory mechanisms to ensure those principles are respected. It does not establish a single body of rules enforced by one central authority. EU member states are in principle free to introduce higher standards than those required by the directive, and the enforcement powers and approach of the national supervisory authorities in applying those standards may vary from one country to another.

Basically the Directive provides for a common set of laws governing the exchange of data and the enforcement of regulation within the member nations of European Union in order to provide for the free flow of information within the EU. It also then prohibits (with Article 25) the export of data out of the EU to areas lacking adequate protection. The EU Directive represents a dramatic increase in the reach and importance of data protection laws and a step forward for the development of a unified internal European market. Peter Swire (1998) points out that those interested only in Article 25 (export of data) might miss the point that this type of legislation represents a next logical step in creating a unified internal market, one of the goals of the EU. Data protection issues are handled under the Internal Market and Financial Services Directorate of the EU Commission, an indication that this is intended to foster commerce. (Jerry, if you agree with the changes I made to the table, I think we need more specific talk about its content, e.g., examples for how things are different around the power components…)

The descriptive model of regulation and self-regulation is helpful to understand how privacy protection can be achieved on a systemic level. However, because of this structural focus the descriptive model remains too superficial to help us understand their embedded assumptions about privacy and their intricate implications for marketers and consumers. We must therefore enter a more in-depth analysis about the “philosophy of privacy.”

Philosophies of Privacy: Commodity versus Basic Civil Right

Arthur Miller wrote in 1971, “[T]he challenge of preserving the individual’s right of privacy in an increasingly technocratic society, even one with a democratic heritage as rich as ours, is formidable. But it is one that policy-makers in government, industry and academe simply cannot avoid” (Miller, 1971). Written almost 30 years ago, Miller’s statement rings true today more than ever. It is quite possible that in the digital age privacy in its strict sense (as the conscious and controlled protection of personal information) can not be guaranteed or demanded any longer. But it is precisely at this point that the myth of privacy acquires discursive (rhetoric) meaning. Privacy, however it may be defined, turns into fodder for the "narrative propaganda" (Roesler, 1997) of all parties in the debate. As Dordick (1995, p. 156) states, "[P]ersonal information is becoming increasingly valuable in our market-oriented society and, with today's information technology, relatively easy to gather surreptitiously."

Consumers feel insecure about data protection on the Internet, especially when engaging in commercial transactions with another party. The perceived threat comes from several different directions. There is the possibility that the other party collects personal information without notifying the consumer. There is the consumer's fear that a third person could intercept and abuse any type of personal information (e.g., name, credit card number, mailing address, email address, etc.). There is the consumer's fear that the business partner might commit privacy violations such as selling personal customer information to a third party without permission. It would not be difficult to demonstrate with ample examples that these concerns are justified (e.g., Süddeutsche, 1999; Weichert, 1998; Frankfurter Allgemeine, 1999). Thus, consumer anxiety about data protection and privacy in the digital age poses a viable threat for the global growth of electronic business. Therefore, national governments, business organizations and consumer groups have an equal interest in putting the privacy issue on top of their list. However, while the problem seems clear, the possible solution remains cause for heated debate and finding a broad consensus will be difficult.

On the surface, the conflict seems to be one of public policy where what is at stake is the age-old question of government regulation of the economic sphere versus self-regulated marketplace.[18] We think however, that under the surface of this political debate, a much more important struggle is taking place over the power to control the meaning of privacy. We argue that the self-regulation model based on the assumption that privacy in the digital age be defined as human property as only such a definition allows for total commodification, and thus marketability, of personal information. The private property approach implies individual ownership of privacy in form of personal information. The ownership status permits the consumer, who is conceived as the rational decision maker of neo-classical economic, to treat personal information as a commodity, which he is free to exchange in a decentralized marketplace. The marketer in this scenario is a legitimate business partner.

The regulation model, on the other hand, adheres to the traditional notion of privacy as basic civil right—as being integral part of being a citizen-- that cannot be violated by the economic sphere. Defined as a civil right, privacy escapes commodification and cannot be owned by anyone in an economic sense, only in a political. Thus understood, privacy cannot be traded in the marketplace but must be protected by the state or any other legislative system in charge of protecting the rights of its citizens against violation.[19] Thereby, protection of privacy is centralized and its commodification is prevented. The marketer here is conceived

as a potential threat to the citizens' rights (see Figure 3). We take a brief look at both models before we discuss the implications for marketing.

Figure 3

Ontological Beliefs Based on Model

	Regulation Model	Self-Regulation Model
Consumer	Citizen to be Protected	Homo Economicus Maximizing Benefits
Marketer	Threat	Exchange Partner Maximizing Benefits

Privacy as Property or Commodity

The idea of personal information as property is not a new one. It has a long history in legal as well as sociological thought. Westin says "personal information, thought of as the right of decision over one's private personality, should be defined as a property right" (cited in Miller, p. 211). Edward Shils is even more encompassing, when he says that "the social space around an individual, the recollection of his past, the conversation, his body and its image, all *belong* to him" (cited in Miller, p. 212). The intention of such definition was to provide the carrier of personal information with the right to sue when there was information abuse (Miller, 1971, p. 212).

This perspective, however, overlooked the much more substantive consequence of the privacy-property nexus, as already anticipated by Marx (1978). He said that property (unlike capital) had its source in man himself, in form of his body and the incontestable possession of his body strength. Marx, of course, at the heights of the industrial age, talks here about "labor-power." In the post-industrial age, however, not labor-power is at the center of capitalist production but the accumulation and exchange of information (Poster, 1990b; Toffler, 1990). In fact, not production but consumption is at the heart of late capitalism (Jameson, 1984) and therefore not the worker's labor-power but the consumer's personal information now carries value. Yet, in order for it to attain a knowable value, an exchange value to be more exact, the consumer's personal information must become commodified. As a commodity, personal information can be traded in the market where it yields a price.

We can then understand the real implications for marketers and consumers of the property discourse propelled by the US government (represented by the FTC, FCC, and US Commission for Privacy) and the business groups. Personal information defined as commodity means that the individual consumer holds the right for commercial exchange of his or her own privacy in the marketplace. Businesses interested in data acquisition can then offer a price to the consumer, thus copying, albeit in inverted roles, a regular commercial transaction. At this moment, privacy is unhinged from its constitutional location, commodified via the concept of personal information, and re-located in the economic field (Habermas, 1990). Such an act of re-position opens up a new landscape for marketers, which will be discussed below. In contrast, the European Union's approach, to which we will turn now, is quite different.

Privacy as Civil Right

With the issuing of a *Directive for Data Protection*, the European Union has taken a strong initiative toward a top-down approach regarding consumer privacy protection online. A general argument of the directive is that the reliance on the recognition of a property right of personal information would have the undesirable consequence of placing responsibility on each individual to protect his own interest. Without an external authority imposing and enforcing regulations on business organization, the individual consumer's interest for protection and the businesses' interest for data accumulation are in direct conflict, with the business organizations having a superior position in the unequal bargaining procedure (Miller, 1971).

Unlike the Americans, the Europeans are not willing to put the protection of privacy under the rule of competition (Samuel, 1999). The EU politics surrounding the Directive is fueled by the established view of privacy as a human rights issue. As Deborah Hurley states (1998, italics added), "In Europe, privacy and personal data protection is regarded as an *inalienable right* because it is so important to [their] dignity and sense of autonomy." Under such a position privacy is not understood as a property of the individual, which he or she owns and is free to sell in the marketplace. As an inalienable right, like human or civil rights, privacy in modern societies is provided to the individual as a sphere of freedom and autonomy. In fact, in the first modern constitutions, the section listing basic rights provided in image of the liberal model of the public-private divide, in which society is guaranteed to its citizens as a sphere of private autonomy (Habermas, 1990). By abiding to this traditional understanding of privacy, personal information is not to be owned as much as protected, and the authority stewarding privacy is, of course, the government.[20]

The EU Directive for Data Protection in its operative provisions, expressly states that the right to privacy is a fundamental right and freedom of natural persons (Rosenoer, 1995). Once privacy is (re)asserted as part of the constitutional sphere of fundamental basic rights, only sweeping legislative regulations can safeguard it. Privacy, therefore, is irreducible to the individual property principle and personal information cannot be commodified. It becomes clear now, that the European position on the online privacy issue is diametrically opposed to that of the US administration and business groups. Obviously, both models, the regulative model proposed by the European Union and the Self-regulative model proposed by the United States and the industries, imply two totally different marketing strategies, which we outline next.

Business in the Digital Age: Privacy Models and the Role of Marketing

Because it is easier to establish trust relationships among commercial sellers and buyers (Kalwani & Narayandas, 1995), electronic commerce has been growing fastest in the business-to-business market (see Aspen, 1998). For it to gain an equally central role in the consumer marketplace, consumers must feel safe and secure online. In other words, they need to have confidence and trust in the electronic infrastructure. While technological fixes will help to solve practical problems they cannot by themselves create trust and consumer confidence. Those are characteristics of social relationships, which need to be established between two parties (Grönroos, 1995).

The self-regulation model implies that the responsibility to build a trust relationship lies with the businesses. By setting high industry standards for privacy protection and holding all industry members accountable, consumer confidence will result. The regulation model suggests that trust ensue from consumers' reliance on a neutral authority strictly enforcing their rights. Thus, the government sets high privacy protection standards and is also responsible for exacting compliance (see Swire & Litan, 1998). Which model leads to a higher degree of consumer confidence and trust is an interesting empirical question that cannot be addressed here.[21] We want to focus instead on the two forms of privacy these models suggest as their operating principle—commodity versus civil right—and their immediate implications for marketers and consumers.

Both models are normatively similar and their systemic difference is mainly to be found on the operational level, i.e. the acts of implementation and enforcement. Marketing, the operating principle of business organization in regard to the consumer, is placed at the center of this difference. Critically, underlying any marketing operation is the basic distinction between privacy as basic civil right versus privacy as individual property (commodity). Because of this distinction, marketing's role in the self-regulated model is very different from that in the regulated model.

Marketing under the Self-Regulated Model

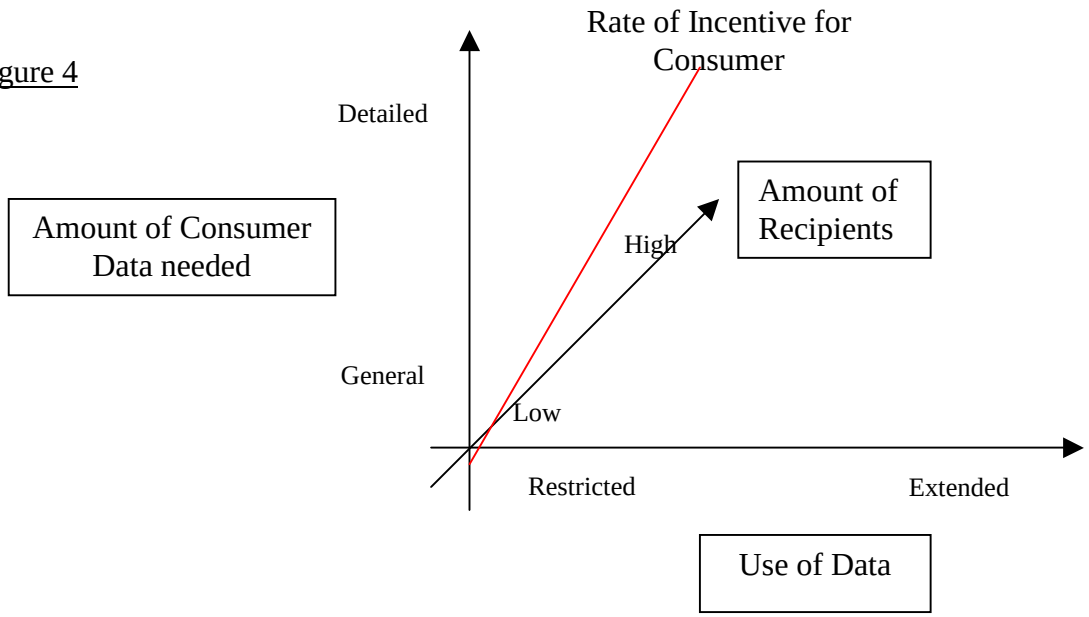
The combination of self-regulation and privacy as individual property allows for a range of marketing action that otherwise would not exist. In this scenario, privacy becomes an exchangeable property and the possessor of property presumably makes rational choices as to how, when, with whom, and for what price he or she wants to trade it. Companies on the other hand can and must decide how much personal information it needs for its business purpose, what quality is required, and how much the company has to pay for it. When companies begin to purchase personal information, marketing strategies are useful to help the company manage their information needs.

Consequently, the nature and normative function of the five core principles suggested by the FTC must be reconsidered in marketing terms. We focus particularly on principle 1 and 2 (Notice/Awareness and Choice/Consent) of the FTC Report to Congress, because principles 3-5 (Access/Participation, Integrity/Security, and Enforcement/Redress) do not seem to lend themselves to marketing mix strategies without potentially imperiling legal or moral rights. Notice and Awareness requires companies to notify the consumer about the entity's information practices before collecting personal data. Furthermore, the company has to identify a) the uses to which the data will be put, b) any potential recipients of the data, c) the nature of the data collected, d) whether the provision of the requested data is voluntary or required, and e) steps taken by the company to ensure confidentiality, integrity, and quality of the data.

In the self-regulation model proposed here, consumer notification would remain central to the marketer's task. However, point a-c offers immediate marketing possibilities in the marketer's dealing with the consumer. The consumer can be offered several 'levels of uses' to which the data can be put ranging from restricted internal use for customer service to inner-departmental to networked inner-corporate uses. Depending on the (re)use of the personal information, different incentives can be offered to entice the consumer to share personal information. In addition, point b) suggests that incentives for personal data can be ranked according to the 'amount of recipients' with which the company wishes to share the consumer's personal information. This may vary from one to a potentially infinite (or open)

number of recipients. Furthermore, point c) opens up a third dimension for marketers to take into consideration for the company's information marketing management. The 'nature of data shared' by the consumer can range from very general demographic or psychographic information to a much more detailed set of information including values, attitudes, and interests. The limits to more data can only be imagined to be set by the amount of incentives (i.e., the costs of the data) marketers have to offer to compensate consumers and consumers' willingness to share information (see figure 2).

Figure 4



The model proposed by the self-regulative system requires the company to inform the consumer about possible uses the data is put to, the possible number of recipients that might access the data, and the amount of personal data demanded. On the other hand, after obtaining all the information and evaluating all possibilities, the consumer makes a rational decision as to what "amount" of privacy he or she is willing to give up for a specific "Rate of Incentive."

By doing so, the self-regulative system automatically incorporates the second FTC principle, consumer choice or consent, into the model. It demands from companies to offer an opt-in and opt-out function for consumers. However, the FTC report expressly states, that companies should consider going beyond the binary yes/no option and possibly creating "in-between" choices for consumers. In a self-regulative system in which privacy is traded as a commodity, the second FTC principle becomes a built-in function as consumers have a virtually infinite amount of "in-between" options.

In conclusion, the self-regulative system allows for complex decision making as to how the marketer should negotiate his or her need for consumer information and the consumer's desire to exchange personal information. Because privacy is defined as a commodity, it can be treated according to the economic laws of the marketplace and without direct normative interference from other authorities. As a result, marketers face a difficult but rich task in managing personal consumer information.

Marketing under the Regulated System

The regulation model sets up a trust infrastructure that exists fully outside the parties involved in the trust relationship. In other words, the regulation model *imposes* trust, as a rational act in Weber's sense, onto the exchanging parties. According to Weber, an act is rational when a) it is oriented toward a clearly formulated unambiguous goal, or to a set of values which are clearly formulated; b) the means chosen are, according to the best available knowledge, adapted to the realization of the goal (Parsons, 1947). The self-regulation model strives for a similar rationality but has to face the difficulty that it must be established from "within." Every time a consumer and a marketer meet, the two parties must find an agreement on the goal (degree of personal information protected or given up), the values, and the means to reach the goal, which leads to a multitude of qualitatively different trust relationships. In such a situation, the marketer has more control over the nature of the trust relationship by, for instance, creating a brand name, sport a particular trust or security badge from a reliable source (like the Better Business Bureau) on the web site, or create customer chat rooms or suggestion boxes. When, as in the case of the regulation model, the goals, values, and ends are already provided by an external authority, trust relations are freed from differences in the parties' strategies, values, and goals. The role of the marketer, then, is limited to compliance of these regulations and the possibility to communicate a successful conformity (Swire & Litan, 1998).

As demonstrated above, personal information under the regulation model is not treated as a commodity but conceived instead as the fundamental component of privacy. Personal consumer information, as a result, cannot be exchanged in the marketplace but must be protected from exploitation. The consequence for marketing is that data collection possibilities are clearly delimited and room for interpretation is small. For consumers it means that their ability to leverage on their personal information in order to negotiate exchange value with the marketer is limited to a minimum.

Conclusion

Privacy protection has played and will continue to play an important role in the development of the new information technologies. Consumer concerns over privacy violations have prompted reactions from all stakeholders, national and regional governments, businesses, and consumer groups. Two models have emerged from the debates so far, the self-regulation model proffered by the United States and the regulation model, already actualized by the European Union. Both models operate with quite different concepts of privacy. The self-regulation model sees privacy, composed of personal information, as the consumer's individual property. The consumer has free choice in exchanging personal information in the market, thereby making a rational decision about the degree to which he or she wishes to protect his or her privacy. In contrast, the regulation model treats privacy as an inalienable civic right that cannot be commodified in the marketplace.

The implications for marketers are important. If the self-regulation model is accepted, a marketer enjoys a tremendous freedom of information management, maybe much more than is obvious on first sight. On the other hand, the consumer is empowered and forced to make responsible decisions as to how much personal information should be exchanged for what in return. If the regulation model is accepted, marketers as well as consumers have only little freedom to interact on the matter of privacy. Both parties underlie a strict normative framework that rather tightly controls their actions.

References

Agre, P. E. (1994a). Surveillance and Capture: Two Models of Privacy. *The Information Society, 10*(2), 101-127.

Agre, P. E. (1994b). Understanding the Digital Individual. *The Information Society, 10*(2), 73-76.

Andrews, W. (1996). Surveillance in cyberspace. *American Journal Review, 18*(2), 13.

Arendt, H. (1998). *The Human Condition*. Chicago and London: University of Chicago Press.

Aspen, R. (1998). *The Global Advance of Electronic Commerce: Reinventing Markets, Management, and National Security* (A report of the sixth Annual Aspen Institute Roundtable on Information Technology). Washington, DC.: Aspen Institute.

Belk, R. W. (1988). Possessions and the Extended Self. *Journal of Consumer Research, 15*(September), 139-168.

Benn, S. I. (1971). Privacy, Freedom, and Respect for Persons. In R. J. Pennock & J. W. Chapman (Eds.), *Privacy* (pp. 1-26). New York: Atherton Press.

Bennett, C. J. (1996). The Public Surveillance of Personal Data: A Cross-National Analysis. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 237-259). Minneapolis: University of Minnesota Press.

Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge ; New York: Cambridge University Press.

Bondebjerg, I. (1996). Public Discourse/Private Fascination: Hybridization in 'True-Life-Story' Genres. *Media, Culture, And Society, 18*(1), 27-45.

Cavoukian, A., & Tapscott, D. (1997). *Who Knows : Safeguarding Your Privacy In A Networked World*. New York: McGraw-Hill.

Clarke, R. (1991). Information Technology and Dataveillance. In C. Dunlop & R. Kling (Eds.), *Computerization and Controversy: Value Conflict and Social Choice* . Boston: Academic Press.

Clarke, R. (1994). The Digital Persona and its Application to Data Surveillance. *The Information Society, 10*(2), 77-92.

Cowhey, P. (1995). Building the Global Information Highway: Toll Booths, Construction Contracts, and Rules of the Road. In W. J. Drake (Ed.), *The Information Infrastructure* (pp. 175-204). New York: The Twentieth Century Fund Press.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.

Dordick, H. S. (1995). The Social Consequences of Liberalization and Corporate Control in Telecommunications. In W. J. Drake (Ed.), *The Information Infrastructure* (pp. 155-172). New York: The Twentieth Century Fund Press.

Durkheim, E. (1984). *The Division of Labor in Society* (Halls, W D, Trans.). New York: The Free Press.

Firat, F. A., & Venkatesh, A. (1993). Postmodernity: The Age of Marketing. *International Journal of Research in Marketing, 10*(3), 227-249.

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison* (Sheridan, A, Trans.). New York: Vintage Books.

Frankfurter Allgemeine Zeitung (1999, August 25). Im Datenwald, pp. 45

Gandy, O. H. J. (1996). Coming to Terms with the Panoptic Sort. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 132-155). Minneapolis: University of Minnesota Press.

Ger, G., & Belk, R. W. (1996). I'd Like to Buy the World A Coke: Consumptionscapes of the "Less Affluent World". *Journal of Consumer Policy, 19*, 271-304.

Gibson, W. (1984). *Neuromancer*. New York: Ace Science Fiction Books.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, N.Y: Doubleday.

Grönroos, C. (1995). Relationship Marketing: The Strategy Continuum. *Journal of the Academy of Marketing Science, 23*(4), 252-254.

Habermas, J. (1981). *Theorie des kommunikative Handelns, Band 1*. Frankfurt am Main: Suhrkamp.

Habermas, J. (1990). *Strukturwandel der Offentlichkeit : Untersuchungen zu einer Kategorie der burgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp.

Habermas, J. (1991). The Public Sphere. In C. Mukerji & M. Schudson (Eds.), *Rethinking Popular Culture: Contemporary Perspectives in Cultural Studies* (pp. 398-404). Berkeley: University of California Press.

Harris, L., & Westin, A. F. (1991). *Harris-Equifax Consumer Privacy Survey*. Atlanta, GA: Equifax.

Hurley, D. (1998,). Privacy in Play. *Think Leadership Magazine*.

Jameson, F. (1984). Postmodernism or, The Cultural Logic of Late Capitalism. *New Left Review, 146*(July-August), 55-75.

Jones, S. (1997). Kommunikation, das Internet und Elektromagnetismus. In S. Munker & A. Roesler (Eds.), *Mythos Internet* (pp. 131-146). Frankfurt a. M.: Suhrkamp.

Kalwani, M., & Narayandas, N. (1995). Long-Term Manufacturer-Supplier Relationships: Do They Pay off for Supplier Firms? *Journal of Marketing, 59*(January), 1-16.

Kling, R., & Allen, J. P. (1996). How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy. In D. Lyon & E. Zureik (Eds.), *Computers, Surveillance, and Privacy* (pp. 104-131). Minneapolis: University of Minnesota Press.

Kotler, P., & Armstrong, P. (1996). *Principles in Marketing*. Englewood Cliffs, NJ: Prentice Hall, Inc.

Kroker, A., & Kroker, M. (1996). *Hacking the Future*. New York: St. Martin's Press.

Lefebvre, H. (1991). *The Production of Space*. Oxford, England: Blackwell.

Levy, H. (1997). *Collective Intelligence: Mankind's Emerging World in Cyberspace*. New York : Plenum Trade

Lievrouw, L. A. (1998). Our Own Devices: Heterotopic Communication, Discourse, and Culture in the Information Society. *The Information Society, 14*(2), 83-96.
Luhmann, N. (1984). *Soziale Systeme*. Frankfurt/Main: Suhrkamp.
Luhmann, N. (1997). Selbstorganisation and Mikrodiversitat: Zur Wissenssoziologie des neuzeitlichen Individualismus. *Soziale Systeme, 3*(1), 23-32.
Luke, T. L. (1999). Simulated Sovereignty, Telematic Territoriality: The political economy of cyberspace. In M. Featherstone & S. Lash (Eds.), *Spaces of Culture* (pp. 27-48). London: Sage.
Lunefeld, P. (1999). *The Digital Dialectic*. Cambridge, MA: MIT Press.
Lyon, D., & Zureik, E. (1996). *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press.
Marx, G. T. (1999). What's in a Name? Some Reflections on the Sociology of Anonymity. *The Information Society, 15*, 99-112.
Marx, K. (1978). *Capital, Vol. 1*. New York: W. W. Norton & Company.
Meyrowitz, J. (1985). *No Sense of Place: The Impact of Electronic Media on Social Behavior*. New York: Oxford University Press.
Miller, A. R. (1971). *The Assault on Privacy*. Ann Arbor: The University of Michigan.
Mitchel, W. J. (1999). Replacing Place. In P. Lunefeld (Ed.), *The Digital Dialectic* (pp. 113-128). Cambridge, MA: MIT Press.
Negroponte, N. (1995). *Being Digital*. New York: Knopf.
Ong, W. (1987). *Oralitat und Schriftlichkeit*. Opladen: Westdeutscher Verlag.
Paquin, J., Zwick, D., & Dholakia, N. (1998). Anonymity and Recognizability in Cyberspace: Ethical and Legal Issues. *Paper presented at the 23rd Annual Macro-Marketing Conference, University of Rhode Island*.
Parsons, T. (1947). Introduction. In T. Parsons (Ed.), *The Theory of Social and Economic Organization*. Glencoe, Ill.: The Free Press.
Poster, M. (1990a). Foucault and Databases. *Discourse, 12*(2), 110-127.
Poster, M. (1990b). *The Mode of Information*. Chicago: The University of Chicago Press.
Reidenberg, J. R. (1995). Information Flows and the Global *Infobahn:* Toward New U.S. Policies. In W. J. Drake (Ed.), *The Information Infrastructure* (pp. 251-268). New York: The Twentieth Century Fund Press.
Roberts, J. M., & Gregor, T. (1971). Privacy: A Cultural View. In R. J. Pennock & J. W. Chapman (Eds.), *Privacy* (pp. 199-225). New York: Atherton Press.
Robins, K. (1999). New Media and Knowledge. *New Media & Society, 1*(1), 18-24.
Roesler, A. (1997). Bequeme Einmischung. Internet und Offentlichkeit. In S. Munker & A. Roesler (Eds.), *Mythos Internet* (pp. 171-192). Frankfurt a. M.: Suhrkamp.
Rosenoer, J. (1995, August). The Privacy Directive. *CyberLaw*.
Rotzer, F. (1995). *Die Telepolis - Urbanitat im digitalen Zeitalter*. Mannheim: Bollmann.
Samuel, A. (1999, May). German Shepherds. *Business 2.0*.
Sassen, S. (1996). *Losing control?: Sovereignty in an Age of Globalization*. New York: Columbia University Press.
Sassen, S. (1999). Digital Networks and Power. In M. Featherstone & S. Lash (Eds.), *Spaces of Culture* (pp. 48-63). London: Sage.
Simmel, A. (1971). Privacy is Not an Isolated Freedom. In R. J. Pennock & J. W. Chapman (Eds.), *Privacy* (pp. 71-87). New York: Atherton Press.

Solomon, M. R., & Englis, B. G. (1997). Breaking Out of the Box - Is Lifestyle a Construct or a Construction? In S. Brown & D. Turley (Eds.), *Consumer Research: Postcards from the edge* (pp. 322-349). London: Routledge.

Süddeutsche Zeitung (1999, 10. Juli). Datenschutz auf Amerikanisch, p. 24.

Swire, P. P., & Litan, R. E. (1998). *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive*. Washington, D.C.: Brookings Institution Press.

The Economist (1997, August 23rd). Hi Ho, Hi Ho, Down the Data Mine 344, 47-48, and We Go.

Toffler, A. (1990). *The Powershift*. New York: Bantam Books.

Turkle, S. (1995). *Life on the Screen*. New York, NY: Touchstone.

Weber, M. (1947). *The Theory of Social and Economic Organization* (Henderson, A M Parsons, T, Trans.). Glencoe, Ill.: The Free Press.

Weichert, T. (1998, October 24). Der europaeische "Sonderweg". *taz, die tageszeitung*, pp. 12.

---

[1] For the remainder of the document, both terms are used interchangeably.

[2] Just think of the ominous 'cookies,' small electronic programs that are sent to the consumer's hard drive. These programs allow the website to gather a host of valuable, yet personal, information about the consumer.

3 Attorney Janlori Goldman, cited in (DeCew, 1997, p. 47), has noted:

> National polls document a growing demand for privacy protection. A Trends and Forecasts survey released in May, 1989 found that 7 out of 10 consumers feel that personal privacy is very important to them, with many expressing the fear that their privacy is in jeopardy.

4 In our lives on the screen of cyberspace (Turkle, 1995), we are quite removed from the classic ideal of face-to-face relations as in the Greek agora or the discussion clubs of the Enlightenment era.

5 It is true that marketing textbooks increasingly incorporate information about the possibilities that new technologies offer to identify potential customers more efficiently, improve market segmentation and product positioning. As Kling and Allen (1996, p. 116) state it rather gravely, " [O]verall, business schools teach their students to be clever and opportunistic information entrepreneurs, without paying much attention to the way that routine businesses practices can create problems in public life. Such as by intruding personal privacy."

6 Obvious examples of matter turned into digital codes are print language and photographs. However, considering the staggering advances made in the realm of computer simulation, most everything from cars, to buildings to hi-tech medical equipment to medical patients, can now be encoded into digital structures. Finally, electronic codes have been used to accumulate massive databases of individuals, which are re-produced with simulated subjectivities according to the composer's motives.

7 Turkle refers to the two ontological states described by computer users as Real Life (RL) and Virtual Life (VL). For many of her informants, VL offered the more invigorating and spirited life world. For a visionary and highly stimulating literary account on this subject see Gibson's cyberpunk novel Neuromancer (1984), in which the protagonist's pathetic existence in real world is dramatically juxtaposed to his powerful and potent position in cyberspace.

8 Of course, in the light of ongoing debates about the postmodern, especially in regard to the new communication technologies, the use of terms such as 'complete consumer subject' and 'modern' must be qualified. We speak of a complete subject to acknowledge its factual and concrete existence in cyberspace regardless of its other existences in the "real world." Subjects in cyberspace create (or have) complex

identities and use at times elaborate rituals to present a coherent self to others (see Turkle, 1995). We do not reject the thesis that new communication technologies create a fragmented subject (as advanced by Turkle and others). But we wish to point out that the idea of the fragmented subject carries the possibility of incompleteness in it, as if every fragment is less than the whole, which we reject at least in the context presented here.

9 As many other technological advancements, the Net project was pushed by the U.S. military as well as the Universities. However, it is now also well known that computer hacker joined in to design software that strengthened the original design of the Net. The idea was to create an open and totally decentralized net(work) available at no cost (Sassen, 1999).

10 The Internet, in contrast to EDI and DDI, is an open, decentralized, and real-time network. It allows spontaneous but constant connectivity for a potentially "infinite" number of business partners and consumers. In addition, the Internet is inexpensive. Therefore, it is a "distinct improvement over so-called VAN's, or value-added networks, which are private communication networks that connect a number of trading partners together (using EDI, for example)" (Aspen, 1998, p. 4).

11 Email, for instance, is generally considered a private form of communication as the outrage over companies monitoring their employee's electronic correspondence proves. Chat rooms can be considered public forms of communication. Internet service providers such as America On Line (AOL) have recognized users' need to chose between private and public communication. Chat room visitors engaged in public discussions can instantly engage in private communication by contacting a chat room member using AOL's "instant message" option. An instant message can only be read by the party it was addressed to.

12 Obviously, we all know about his contempt form private property.

13 Of course, there might be reasons to observe an individual without his or her permission as in the prison. In such situations, social norms promoting general security and protection against violence and crime might override the individual's right to privacy 9and obviously freedom).

14 As Jones (1997) points out, just think of the vital market of personal planners and organizers.

[15] For instance, to participate in "restricted" forums or discussion groups, or to increase chances for a loan application to be successful.

[16] Of course, consumers apply the same strategies in the "real" world as well but because of the nature of the virtual space, these strategies seem much more prominent here. Furthermore, Marx's types of identity knowledge (legal name, locatability, pseudonyms, pattern knowledge, social categorization, symbols of eligibility) are based on the "reality" of the virtual.

17 Infinite because pseudonymity allows for the ongoing invention of new personae for which new personal information has to be imagined.

18 This dilemma is closely linked with the emergence of modern capitalism and the increasing complexity of modern societies. While during the age of antiquity and the Christian middle ages the economic sphere remained subordinated to politics and theology respectively, Emile Durkheim (1984) proclaimed that modern societies underlie a process of differentiation that spreads to all social spheres such as work, home, leisure, or religion. As a result, the social system becomes an aggregate of equal sub-systems, the economic sphere being one of them, which establish their own normative rules and reproduce autonomously (Luhmann, 1984). At this point in history, not a hierarchy but a dualism was established between the economics and politics, which made state intervention into economic affairs a site of contestation (Habermas, 1981). "General interest", the standard for society's action in the 18th and 19th century was to be attained through the dealings of private persons in the marketplace liberated from social forces.

19 Increasingly, nation states relinquish legislative, financial, and political power to supra-national, so-called "institutional" power centers (Sassen, 1996).

20 Increasingly, nation states relinquish legislative, financial, and political power to supra-national, so-called "institutional" power centers (Sassen, 1996).

21 Except, we believe that it could be highly culturally dependent.