jrc
Journal of Research for Consumers

Issue: 1, 2001

Privacy and Consumer Agency in the Information Age: Between Prying Profilers and Preening Webcams

AUTHOR(S): Nikhilesh Dholakia, Detlev Zwick

ABSTRACT

This article is about the ability of the consumer to control his or her destiny in the new electronic marketspace. Two seemingly opposite phenomena – the need for privacy and the desire for exhibitionism and voyeurism – are vying for attention on the media landscape. We believe the simultaneous occurrence of privacy concerns and ultraexhibitionism is not coincidental. Indeed, exhibitionism and voyeurism seem to offer new tools for consumer resistance against the electronic surveillance systems in networked markets and are inextricably linked to consumers' desire for control over their intimate personal information.

ARTICLE

As the Internet becomes increasingly commercialized and globalized, it spawns exciting opportunities as well as insidious challenges for consumers. Industry alliances, government agencies, and consumer groups are jostling to set standards for best online business practices and to influence legislation (Johnston, 2000). In the burgeoning field of e-commerce, efforts are under way to (Dekleva, 2000):

1) Build trust for consumers.
2) Establish ground rules for the digital marketplace.
3) Enhance the infrastructure for conducting business electronically.
4) Maximize the benefits for all market participants.

We will focus on the first of these larger topic areas, particularly on the questions of privacy protection, confidentiality, and consumer autonomy.

The networked society of the Information Age is a mixed blessing for consumers. While some of the rhapsodies about perfect market information and consumer empowerment in the electronic marketspace are justified, such celebratory accounts do not tell the whole story from a consumer perspective. If one side of the e-commerce coin is imprinted with consumer benefits like instant price comparisons, increased choice, and added convenience, the other side is inscribed with threats to consumers' security, privacy, and autonomy (Bennett, 1996; Hoffman, Novak and Peralta, 1999; Kling and Allen, 1996). Like other momentous technological innovations of the past, the Internet produces a double discourse of progress: one bright and promising, the other dark and foreboding (Virilio, 1997).[1]

While the positive effects of electronic commerce are extolled at length, the downside for consumers is either underplayed or receives cursory, sensationalistic treatments. In this article, we explore critically what it means for the consumer to become implicated in an increasingly networked and digitized marketspace. By looking at two central technologies of electronic markets - consumer profiling[2] and electronic databases - we point to the danger that consumers face when they deliberately or inadvertently cede the power to control how personal information is externalized and distributed.

A struggle over personal information is ultimately a struggle over who controls the formation of the *consumer self* and *consumer agency* in the market. In other words, whose man or woman is the e-consumer? As the engine of electronic commerce gains momentum, these are issues too important to be left unexplored.

We should also point out what this article is not about. Legal concerns over privacy, security, and consumer protection have drawn the attention of national and international agencies seeking ways of facilitating global electronic commerce. Their objective is to find acceptable standards - legislatively or self-imposed - for the collection and exchange of consumer information (Dekleva, 2000). These are very important efforts to bring the dream of global electronic commerce to fruition. Our discussion is not at the manifest level of the legalities of Internet-oriented privacy. Instead, we focus on the structural and phenomenological logic of electronic commerce and its immediate implications for the consumer's ability to control his or her "digital self" (Nakamura, 1995; Turkle, 1995).

Many of the issues touched on in this paper are not unique to the Internet - they have arisen in the context of other media. Because of its massiveness and prodigal rate of change, however, the Internet has added poignancy and urgency to every issue of

consumer security, privacy, and autonomy. In its commercial form, the Internet brings into play whole new dimensions of data production, collection, storage, dissection, and exchange. More than anything, the Internet allows the marketer to get ever closer to the consumer, in *real-time and interactively*.

Such a dramatic change in the relationship between market participants is bringing tectonic shifts in market interactions and market power. In particular, technologies of profiling and datamining allow the marketer to take an ever-greater control of the representation of the consumer. In a metaphorical sense, the consumer's soul is being captured in a matrix of data while his/her body and mind are being pampered by technologies of seemingly obsequious personalization. If we are right, this new brave world of electronic commerce poses a threat to consumers that goes mostly unnoticed but nonetheless imperils the consumer's self and agency (autonomy) in the marketspace by stripping it of its most intimate information. Ultimately, then, this article is not about privacy but about the ability of the consumer to control his or her destiny in the new electronic marketspace.

Two Contradictory Tendencies

Before we can enter our discussion on profiling, databases, and consumer privacy, we need to acknowledge the recent emergence of voyeurism and exhibitionism as among the most striking social and cultural developments in the Western world. We deem such a discussion necessary for two reasons. First, it has been argued that people's desire to expose themselves on the Internet documents their complete disinterest in privacy and control over personal information, making the whole debate a moot one. But giving in to this argument means relinquishing consumers' rights of self-expression. In contrast to this view, we assert that voyeurism and exhibitionism demonstrate people's deep concern with issues of privacy and the externalization of personal information. Second, voyeurism and exhibitionism could be seen as sociocultural practices that are wholly unrelated to consumers' concerns about privacy and personal information. In contrast to this view, we propose that discourses of exhibitionism and privacy are inextricably linked and that separating them would prevent us from grasping the link between the ubiquity of the global media complex and consumer behavior.

Thus, we are entering an era where two seemingly contradictory phenomena of the Information Age are co-evolving. On one hand, growing concerns about the possibility of electronic surveillance have stirred fierce debates over privacy protection. On the other hand, we are witnessing the growing confluence of what CNN

correspondent Greg Lefevre (1998) terms the phenomenon of "voyeur meets exhibitionist." Webcams and other technologies have unleashed the repressed, atavistic exhibitionist and voyeur in us. Since the theater of the new media is global, we are building up to a worldwide tsunami of ultraexhibitionism.

The facts are instructive. In 1997 about 300,000 webcams were sold. In 1999 the number was up to 2.5 million. For 2003 the projected number is 36 million. The tiny webcam will become part of the standard computing package just like the keyboard is today. Over a quarter million webcam sites are now up and running. These webcams "show everyone and everything from naked mole rats to New York City taxi drivers, all live and unedited" (Taylor, 2000, p. 60). But exhibitionism is not limited to the Internet. In fact, the biggest "movement" toward total exposure of oneself is produced on TV. Beginning in the early 1990s with the show *Real World* on Music Television (MTV), in the US there is now a whole array of reality/voyeuristic shows on TV. Leading exemplars are *Survivor* (CBS), the *1900 House* (PBS), *Making the Band* and *The Mole* (ABC), and *Big Brother* (CBS). What is even more stunning, the new generation of reality/voyeuristic television was devised in Europe, where privacy concerns ignited by the Internet are noticeably more pronounced than rest of the world (Samuel, 1999).

But exhibitionism needs a voyeuristic audience to succeed. The original *Big Brother* show in the Netherlands led to the highest ratings in that country's recent television history. In Germany, *Big Brother* was not only televised but also available online. All cameras in the house were linked to the Internet in real-time, allowing the web user to choose the preferred camera angle. The Web broadcast was "on" 24 hours a day and, unlike television, unedited. For the two weeks the show was on television, the site had as many hits as blockbuster sites like Yahoo and AOL.

Earthcam.com is a site where everyone who is "webcaming" his or her daily activities can broadcast the pictures directly into cyberspace, thus allowing viewers to participate in one's life. Earthcam.com has about two million hits a day from people who come to peek into the life of someone they have never met. Thus, acamgirl.com shows Aimee, a woman in her late twenties, as she wanders around the house. The pictures are of bad quality, slowly updated, and boring. Yet, Aimee's site is often mentioned among the 100 top sites on the Web (Taylor, 2000, p. 60).

The next wave, predictably, is the blending of the staged exhibitionism of television with the raw exhibitionism of the webcam. In *Runner*, a show being produced by Disney's ABC network and the Internet firm LivePlanet, a man in the U.S. is to be

selected "the Runner". This person has to elude capture in the continental U.S. for 30 days while accomplishing 15 tasks. The tasks include things such as visiting a McDonald's in New Mexico during a set 48-hour period. Television and Web audiences track the Runner and try to find him, in the real world. If anyone catches the Runner, that person gets the prize money that has accumulated to date. The Runner will carry a hidden camera (and hidden cameras will follow him) as he, for instance, moves from a Caesar's Palace buffet in Las Vegas to a Miller brewery tour in Milwaukee to a rock concert in Atlanta.

What are we to make of these two seemingly opposite phenomena - the need for privacy and the desire for exhibitionism and voyeurism - vying for attention on the social and cultural landscape of Europe and the USA? If we ignore this question, then we might as well side with those who suggest that privacy is an outdated concept. We reject this position. We believe the simultaneous occurrence of privacy concerns and ultraexhibitionism is neither coincidental nor that they are fundamentally opposed. Indeed, exhibitionism and voyeurism seem to offer new tools for consumer resistance against the electronic surveillance systems in networked markets and are inextricably interwoven with consumers' desire for control over their information.

Privacy and the Digital Consumer Self

The transformation of the Internet into commercial space is occurring at a blistering pace. Coupled with the unique cultural and psychological aspects of electronic venues of interaction (Hoffman, Novak and Peralta, 1999; Turkle, 1995), the e-commerce revolution has created unprecedented challenges for regulators, the legal system, technology developers, cyberspace marketers, and ultimately consumers (see, for example, Pitofsky, 1996; Varney, 1995). Privacy has become a major focus in the debate about the organization of the Internet (Bridis, 1998). But what does privacy of/for the consumer mean in the context of electronic commerce?

Benn (1971, p. 8) recommends that a general principle of privacy might best be grounded in the more comprehensive principle of *respect for a person*. By tying private affairs directly to the concept of "person," Benn suggests that privacy is having control over the *externalization of one's personal information*. Personal information, in this sense, *belongs* to the person, or in a commercial setting, to the consumer. In Western consumer cultures, where a person's possessions are regarded as an extension of himself or herself (Belk, 1988), personal *consumer* information has at least two important components: 1) demographics and psychographics (i.e., lifestyle information) and 2) personal consumption practices

(Solomon and Englis, 1997). Legalities notwithstanding, there is some form of privacy invasion when information on these two components is collected, stored, and distributed without the consumer's consent.

But the Information Age is the age of digital communication. It has transformed our understanding of producing, storing, accessing, and sharing information. A consumer who goes shopping at a downtown mall could hitherto choose to remain relatively anonymous and *private*. The faceless crowd provides a veneer of protection. But in a digital mall this is no longer so. 'Being digital' means first and foremost the transformation of physical matter into electronically generated bits (Negroponte, 1995). The consumer is no longer a physical body that roams the mall but a set of data points - a *digital representation* of his or her movement and behavior (Turkle, 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. At the level of the code, a vast variety of different information types are reduced to indistinguishable binary bitstreams. All such information can be stored, accessed, and exchanged by digital equipment. Digital matter (e.g., in form of consumer information) becomes free flowing and free-floating, in technical as well as symbolic terms. These binary '0s' and '1s' are the basic elements of an intricate language system that, as philosophers of language and media have made clear, not simply represents but actively *constructs* the reality we perceive (Plant, 1997). Thus, whoever controls this language controls the production of reality, at least in digital spaces.

At this juncture, the "electronic marketspace" becomes dramatically different from the "physical marketplace" (Rayport and Sviokla, 1994). Marketers can now survey and analyze consumer behavior in cyberspace in such a detailed way that they achieve what has been unachievable heretofore: turning the consumer's interior inside out (Levy, 1998). The consumer's electronic trail now renders her fully transparent, allowing deep access into her nature, albeit a nature coded in algorithmic language. Tracking software is now able to monitor every minute detail of online consumers (Locke, 2000). Besides the obligatory and already somewhat antiquated clickstream analysis and cookies, computers can now capture where consumers go with their mouse and how long they linger at a site. What is more, software can capture whether a consumer who was exposed to company X's banner advertising when visiting website Y, actually visits company X's website even if he does so three days later (Allard, et al., 1999). With such information at hand, stored in massive databases yet accessed and analyzed with lightning speed if needed, software packages produce a consumer description in

real-time that can be matched against one of hundreds of pre-configured profiles or, as in collaborative filtering, against other consumers with similar preferences. Electronic databases thus play a central role in the struggle for the consumer self. Therefore, we need to take a closer look at the logic of the database.

The Database and the Constructing of the Consumer

The number of databases, their reach, and volume are increasing constantly. It is by now fair to assume that the combined data possessed by the largest credit companies in the United States allow them to profile virtually every U.S. citizen.[3] The immense circulation of information has generated databases that constitute what Mark Poster (1990, p. 93) calls the "Superpanopticon, a system of surveillance without walls, windows, towers or guards." We have social security cards, credit cards, library cards, driver's licenses, frequent flyer cards, and the like and "the individual must apply for them, have them ready at all times, use them continuously" (Poster, 1990, p. 93). In addition, the Internet collects data sometimes surreptitiously as when clickstreams are monitored and cookies placed, or openly as when consumers fill out personal profiles and credit card information. Consumers have grown used to the fact that almost anywhere they go and whatever they do, they provide information about themselves leaving an electronic trace, which will eventually end up in some database. In other words, consumers have been disciplined to participate in the process of recording, encoding, and adding information to databases.

Viewed from this position, the database is nothing but a tool, a handy technological support for marketers, that perfectly reproduces the spoken and written information derived from the individual (i.e., reality). Such a belief, however, entirely ignores the productive role of language in shaping meaning and practice (Foucault, 1972). Only further interrogation into the quality of the database as a language, which is bound, governed, and truly limited by a definite structure of grammar and syntax, can reveal its power.

Digital encoding of information inevitably eliminates ambiguity, limits and statistically filters out "noise," and thus *restricts meaning*. As Poster points out, "the electronic information gathering that constitutes databases, for all its speed, accuracy and computational power, incurs a tremendous loss of data" (1990, p. 94). The limiting syntax of the database only legitimizes those entries that conform to the rigidly defined categories and fields. Each field is limited in space and form (e.g., when only dates or numbers are allowed). Thus, a database could have the following fields: first name, last name, social security number, zip code, street address, city, state,

phone number, age, sex, race, unpaid credit card bills, time when credit card was used, merchandise bought at a concert, subscriptions to magazines, and season ticket holder. Once this data is collected and digitally encoded, the resulting information constitutes a representation of the consumer that is determined by the language employed in the database.

But this language is ultimately an impoverished, limited language. It functions only by assembling bits and pieces of information that make no sense outside of the database. Consumer data can be pieced together in myriad ways, depending on the preferences of the marketer or the consumer, creating innumerable representations of consumers and markets. Hence - and this is the essence of our discussion on privacy and the consumer self - databases become responsible for "the multiplication of the consumer, the constitution of an *additional self*, one that may be acted upon *to the detriment of the 'real' self without the 'real' self ever being aware of what is happening*" (Poster, 1990, pp. 97-98, italics added).

There is constant interplay between the externalization of consumer information, virtually inevitable in the electronic marketspace, and the simultaneous loss of the consumer's representational control. It is now entirely in the hands of marketers, or worse, software programs, to define the nature of the consumer self - a "self" that is rendered real by algorithmic computation. In addition to the loss of control over the representation of one's self, the digital version can now be diffused throughout an electronic network at the speed of light, chaining the consumer to this virtual consumer self with every entry into another database. What is the value of garden-variety privacy when a virtual consumer self has been formulated, stored, and exchanged well outside the sovereignty of the physical consumer?[4] And more importantly, what happens to the ability of the consumer to choose what to see in the electronic marketspace, which advertising to consider, and even which products to buy at what price, when the entire virtual market environment can be manipulated in real-time via a pre-determined or adaptive profile matching program? The recent publication of Amazon.com's (in the scale of things quite innocuous) practice to present different prices to different consumers depending on their profile shows only the tip of the iceberg of possible manipulation. But it is clear that where databases and profiling intersect, the *agency* of consumers to freely express their will in the market is threatened.

Dataveillance: Consumer Agency at Risk

Marketers and others are gathering, exchanging, and analyzing data in huge quantities in ways never before possible. Information

technology has made it possible for companies to obtain information easily and turn it into a composite picture of an individual's life. Therefore, 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 eavesdropping devices. The convergence of new information technologies and new communications media has created a novel, incorporeal form of consumer surveillance. Roger Clarke (1994) 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.

Today, in "the age of [digital] marketing" (Firat and Venkatesh, 1993), a new breed of *information entrepreneur* feeds marketers with data for such tasks as market segmentation, profiling, personality projections, and database matching (Clarke, 1991). Digital technologies exacerbate the privacy concerns associated with such marketplace activities. To cite a few examples:

· In 1991, Lotus Development Corporation marketed a CD-ROM database of households called MarketPlace:Household which allowed easy access to the personal data of more than 120 million Americans (Kling and Allen, 1996).

· Microsoft's attempt to incorporate a built-in mechanism in Windows 95 operating system that automatically accumulates data about users' hardware as they registered their software brought sharp criticism from computer users.

· Privacy advocates also attacked Intel's Pentium chips that embedded a code number that could be communicated back to computer makers.

· Amazon.com started analyzing the book-buying behavior of certain identifiable groups and reporting which books were the most popular among employees at selected companies such as Microsoft, IBM, and Dell. Even though no individual consumer was identified, such data disclosure created a media stir and brought forth protests from privacy groups.

· In November 1999, the RealNetwork's widely used software RealJukebox for playing musical tracks on the computer was found to have snooping capabilities. The program surreptitiously monitored the listening habits and certain other activities of people who used the program and continuously reported that information - and the user's identity - to RealNetworks when they were connected to the Internet (Robinson, 1999).

· DoubleClick, the biggest Internet-based advertising service, came

under fire because it was attaching real names to behavioral profiles that were supposed to be only illustrative and anonymous.

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 and 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; Shapiro and Varian, 1999).

Of course, there is nothing essentially new about the superpanopticon. Marketers have always collected market information in order to define segments and categorize consumers (Miller and Rose, 1997). But what makes the markets of electronic commerce radically different is that they are interactive and can be manipulated as easily by the marketer as they can be surfed by the consumer. This characteristic of the marketspace endows technologies of datamining and profiling with an entirely new clout; indeed, a clout so strong, it threatens the agency of the consumer. Such a line of thought, as we will see below, bestows consumer-friendly concepts like "customization" and "personalization" with the dark aura of totalitarian control (Kling, 2000; Levine, 2000).

Perhaps the most defining characteristic of the electronic commerce marketspace is, according to its proponents, its ability to be interactive. Unlike ordinary television, a non-interactive mass medium, the Internet allows for a two-way communication stream. In addition, the Internet allows personalized (one-on-one) communication between individuals or companies. These features of the Internet quickly led to its blissful installation as the final piece of the one-on-one marketing puzzle, the end-game of relationship marketing, and the ultimate birth of mass personalization (Godin, 1999; Newell, 1997; Peppers and Rogers, 1997). What has been overlooked is the fact that personalization of messages means something quite different from the personalization of a mountain bike after a long and personal conversation with the bike's builder (even a virtual one) (Levine, 2000). The interactive aspect of the Internet allows the marketer to "personalize" the marketing message according *to whatever the marketer believes to be the appropriate message in a particular case*. In other words, everything, from banner ads, to product offerings, to prices, and the mechanics of the checkout process can and will be personalized for each individual shopper. What the consumer sees or is offered will be based on his or her purchasing or customer support history,

what sites were visited previously, and more traditional parameters like demographics and psychographics, among others. These ultra-discriminatory marketing practices could make some of the racial discriminatory practices of Apartheid South Africa or the segregated American South look like kindergarten tactics.

E-commerce champions argue that such dark, Orwellian imagery is unwarranted. In a positive sense, such manipulation of the shopping environment to presumably make it fit to the specific needs and wants of the consumer could be seen as providing additional customer value (e.g., by reducing search costs, offering discounts to loyal customers, etc.). Of course, the other side of the coin is that such a practice *is not based on the direct input from the consumer, what we call consumer agency, but is the result of arbitrary interpretations, assumptions, and interests of the marketer*. This means that the *real* consumer self, his or her desires, needs, and wants are (over)determined by the data-generated *virtual* consumer profile stored in the computers of the web business.

As Krishnamurthy (2000) points out, profile-building technology has never been stronger. Phenomenally powerful systems lurk in the shadows of cyberspace, building profiles. These systems know everything worth knowing about the consumer. Where the system fails, it makes up by asking the consumer directly. But as Krishnamurthy states, such technologies have many problems. First, they assume stable consumer preferences, otherwise past preferences could not be used as predictors for future purchases. Marketing scholars however know that for at least two prevalent forms of consumer behavior - variety seeking and impulse shopping - past behavior is a poor predictor of future preferences. Another widely explored consumer type, the hedonic, would also seem to reject the assumption of behavioral consistency (Allen and McGoun, forthcoming; Arnould and Price, 1993).

Even the best computer language and algorithms underestimate the non-linearity of the shopping experience. In the words of philosopher Walter Ong (1982, p. 7), computer languages are "forever totally unlike human languages in that they do not grow out of the unconscious [like the human language] but directly out of the consciousness [of the marketer-software programmer]. Computer language rules ['grammar'] are stated first and thereafter used." Because artificial systems of profiling and clustering require a priori formulation, they must assume a deterministic nature of consumer behavior, otherwise they would imply their own uselessness. Consider what Lynne Harvey, senior consultant with the Patricia Seybold group, considers the role of technology (2000,

italics added): "We are … starting to see some progress made toward deep personalization using integrated rule bases, reasoning systems, inferencing engines, and referral systems to deliver a *consistent* personalized environment on a Web site." If the best these systems can do is create consistency, how can they personalize anything for the fickle, complex, and nimble consumer of the electronic consumer markets, the postmodern consumptionscape par excellence (Firat and Dholakia, 1998; Firat, Sherry and Venkatesh, 1994)? Some Internet consultants have recognized this dilemma, consciously or not. Thus, beyond personalization, they now see profiling systems as the avenue for "proactive personalization" (Allard, et al., 1999), "deep personalization" (Harvey, 2000), or - openly demystifying their intentions - "empowered marketing" (Allard, et al., 1999). In other words, as personalization systems cannot (at this point) really personalize the interaction with the consumer, the consumer must be personalized to fit the system. As Krishnamurthy (2000) puts it poignantly, many personalization systems focus on adding value to the marketer and not to the consumer.

Proactive personalization is the crux and the pinnacle of current dreams of consumer profiling. Data collection application providers, data warehouses and managers, datamining programs, and database infrastructure all converge on this ideal of consumer control. The objective is no longer to react to the consumer's actions but to actively anticipate the consumer preferences and fashion the interactive environment accordingly.

As a result, instead of letting the real consumer choose from an unspecified and untargeted assortment of messages and products (i.e. giving the consumer autonomy over the environment akin to the physical marketplace), his or her choice environment is (over)determined *not* because the consumer demanded it so but because of the marketer's strategic orientation. The exclusionary aspects of target marketing were not a significant public policy issue in the past but pinpointed database marketing opens a new, controversial chapter. Personalization and customization of that kind has nothing in common with providing support for the consumer's desire to *actively* and *consciously* participate in the process of need fulfillment.

In sum, instead of promoting consumer agency in the market, something "honest" programs of mass customization and personalization try to do, real-time customization of interactive messages can actually limit the ability of the consumer to shape his or her ideas of market prices, product variability, and quality, among other things. In such a scenario - of which we can see the

first signs in the electronic marketspace - real-time interactivity does not enable consumer choice and informed decision-making, but delimits consumer freedom and unrestrained agency in the market.

The Cry for a Voice

Our discussion leads us now back to our earlier observation that in a culture obsessed with privacy and the protection of personal information, individuals are increasingly prone to feature exhibitionist tendencies and voyeuristic indulgence. Pessimistic thinkers have argued that these new forms of exhibitionism should be interpreted as the ultimate uselessness and historical death of the idea of privacy. Privacy has finally succumbed to the power of electronic gaze. Instead of being appalled by the prospect of permanent surveillance, sometimes humans actually enjoy - in a perverse way - their own exposure and observation (Baudrillard, 1985; Virilio, 1998).

Based on our preceding discussion on the loss of the consumer self and the threats for consumer agency in the age of electronic commerce, we suggest that while a few humans may enjoy exhibitionist exposure, people in general have not succumbed to the surveillance of the networked powers. Quite the contrary is true. Ultraexhibitionism, we argue, is not a negation of privacy but an attempt to *reclaim some control over the externalization of information*. As such, ultraexhibitionism is to be understood as an act of resistance against the surreptitious modes of profiling, categorization, and identity definition that are being performed *by others* on the consumer whenever he or she enters the electronic "consumptionscape" (Ger and Belk, 1996). In other words, since the externalization of personal information cannot be prevented, the individual might as well take charge and be proactive in doing the externalization. That way, at least some power remains with the consumer to form his or her own vision/version of one's Self.

In addition, in the webcam scenario, the production of the consumer self is not negotiated against some virtual algorithm of the marketing system, but against the "real" feedback of "real" people. Not only does the exhibitionist know *that* someone is watching him or her but *who* is watching and what they think. Being a webcam exhibitionist is closely linked to the experience of being a fully autonomous receiver and sender, something that has been lost in the commercial electronic environment.

The phenomenon of opening the raincoat on a global stage should then be understood as evidence that consumers care deeply about their privacy, the control over the mode of representation, and the reclaiming of agency in the world of electronic communication.

These aspects of a consumer's existence are precious and should be protected and respected. In the final section of the paper, we want to point out some practical ways in which consumers can deal with their privacy concerns in electronic markets and how they might be able to maintain as much control as possible over their life as virtual consumers.

Manifestly Private: Life in the Web Menagerie

Data about consumers is traded every day in huge volumes. This is generally done without the consumers' consent or even knowledge. In addition, it is usually very difficult if not impossible to trace and check the database entries and change false information once it has been gathered and stored. The low costs of data entry, now virtually down to zero when recorded as Internet-generated data, makes it economical for even small companies to engage in the business of collecting and interchanging consumer data.

Renting, sharing, or selling names are the common form of data trading. For a little more, companies will sell along with it far more information than just the consumer's name and address. Information can be bought regarding consumers' age, income, ethnicity, lifestyle, the names and ages of children or co-residents, what was bought and when using which credit card and even who it was bought for. Besides entailing sometimes annoying direct marketing activities, being captured in massive databases can become a life-threatening reality as the example of Beverly Dennis proves:

Metromail (now part of Experian) held "more than 900 tidbits of Ms. Dennis's life going back to 1987. Laid out on 25 closely printed pages of spreadsheets were not only her income, marital status, hobbies and ailments, but whether she had dentures, the brands of antacid tablets she had taken, how often she had used room deodorizers, sleeping aids and hemorrhoid remedies" (Bernstein, 1997, p. A30). An inmate serving seven years in a Texas prison for breaking into a woman's house and raping her after threatening to kill her children sent Beverly Dennis a 12-page letter. The letter referred to magazines she reads, her interest in physical fitness, the fact that she was divorced, her income, and her birthday. It included elaborate sexual fantasies involving a specific brand of hand lotion and other personal care products that she uses. Hal Parfait, the prison inmate who wrote the letter, obtained the information about Beverly Dennis for 25 cents (Wallace, 1998).

Here is the bad news. We believe it is impossible to return to what consumers in the pre-information age would have considered a reasonable level of privacy. The interconnectivity of databases, the ease of storing and exchanging data, the ability of collecting

consumer data, especially on the Internet, have led to a situation where total control over the externalization of personal information is unrealizable. There are, however, some practical ways for consumers to reduce privacy dispossession and to reclaim some control over their representation in the marketplace. We offer behavioral and technical solutions - a somewhat artificial division as both are increasingly intertwined.

Behavioral Solutions:

· In case consumers know which companies are selling their information to others, they can have their name removed from the company's list.
· Consumers who want to receive messages from particular companies and have given permission to use their personal information for direct marketing purposes should be proactive by telling these companies not to rent or share this information with others.
· Consumers can contact the Direct Marketing Association (in the United States) to have their personal information removed from hundreds of databases.
· Whether in the physical or the virtual marketspace, consumers could use cash or anonymous smart cards and stored-value cards whenever possible. As soon as a credit card or check is used, the transaction enters the data stream and will be stored somewhere for marketing purposes. On the Internet, the popularization of anonymous electronic payment will open up ways of reducing the information externalized due to purchases.
· If prompted to enter personal information when it is not critical for the delivery of service, consumers could use a fake identity.
· In Internet-based forms, care should be exercised to report only the "required" items and to check (or uncheck, as the case may be) the boxes that prevent the information collector from sharing or selling the information.
· Consumers should read privacy statements carefully.

Technical Solutions:

As consumers browse the Web, data is collected about the stores they visit, the topics they search for, the purchases they make, and the newspapers they read. Every mouseclick can potentially be monitored and cookies, little electronic files, are stored on the consumer's hard drive to create a history of the consumer's browsing activity. The controllers of this data may match this data with physical addresses and real persons, which would create the most seamless picture of the consumer. DoubleClick, a leading Internet advertising company in the U.S. wanted to do just this, but was sued and prevented from matching IP addresses collected from online consumers with their physical addresses (Rodger, 2000).[5]

MatchLogic, another ad company, sponsors several different give-aways that ask for personal information for participants. The company's privacy policy describes how they combine some of the data gathered from sweepstakes registration with consumers' surfing behavior. The possibilities for substantial privacy invasion exist in such cases and are difficult to guard against as a consumer. Technical solutions can help to fend off much of the danger emanating from being monitored by advertising agencies or other parties online. Some of the technological options for the consumers are the following:

· Various software packages are available to consumers to protect their identity online. For example Junkbusters (www.JunkBusters.com) and Guidescope (Guidescope.com) offer protection against attempts of advertising companies to follow consumers around on the Internet. Such software also blocks out ads and cookies.

· Anonymizer.com offers the possibility for consumers to browse the web using its website as the portal. By doing so, Anonymizer functions as a proxy server and prevents anyone from monitoring a consumer's surfing behavior.

· Consumers could switch off the "Accept cookies" option on their browsers. Unfortunately, this also prevents the use of many personalized services on the web.

· Of all places, Microsoft (http://profiles.msn.com/) offers a web page where everyone can set up his or her individual public (preference) profile. Others are Yahoo, Kingdomality, or special shopping communities like wineaccess.com. A public profile posted on the Internet may sound paradoxical in regard to a consumer's active attempt to safeguard personal information. In line with our theory on ultraexhibitionism, however, a public profile offers a strategy to reclaim one's identity from the murky depths of the cyber matrix.

· Some companies offer digital certificates and digital signature systems as ways to unequivocally establish your identity and to communicate such identify electronically to others. Some firms that offer such services include the Digital Signature Trust Co. and VeriSign.

Sometimes, leakage of personal information takes place outside the control of the consumer because it is embedded in the technology they use. For instance, information that users entered into certain financial calculators at Intuit's Quicken website had been seeping out to advertisers, due to a hole in the HTML coding problem[6] (Junnarkar, 2000). The same problem was found at Travelocity.com and Buy.com. These are just other incidents demonstrating that absolute control over even the most intimate consumer information is virtually impossible to achieve.

The information age has changed the marketplace in formidable ways. No doubt, consumer empowerment has increased because of market transparencies and efficiencies. By the same token, consumers' control over their personal information has never been so precarious. For the consumer, perfect security is impossible to attain. The goal must be to acquire the tools and knowledge needed to maintain as much consumer agency as possible in this fast moving and evolving marketspace of the Internet. With privacy dispossession, the consumer most significantly loses the power over his or her *representation* as consumer in the market. Someone else's image of what the consumer *might be* takes on a *real* existence. These synthesized representations of the consumer "self" are being distributed through information entrepreneurs to the databases of the world. Some possible strategies for consumers have been mentioned, but many more are and will become available as the desire for online privacy will not vanish.

Finally, we are not arguing that consumer profiling by marketers is inherently bad and should be banned from the electronic commerce landscape. As Doc Searls and David Weinberger put it in the *Cluetrain Manifesto* (2000, p. 113), "Marketing is not going away. Nor should it. But it needs to evolve." Instead of controlling consumers, marketers need to engage into conversations with them, hear them, and listen to them. Communities are a way for marketers to engage in honest and *really* personal conversations with the market. Then, personalization and other bilaterally empowering aspects of the networked market can be implemented without compromising consumers' agency and autonomy.

Companies such as Amazon.com offer high additional value to their clients based on the use of modern information systems and many customers like the personalized recommendations they receive as a result of the stored personal information. Western Digital, for example, allows users of their hard disk drives to pose questions on their website. In the open, users are actually eager to share their information with the company, be it "only" user information and questions. Usually within hours, a company worker will post a response. The result is open exchange of preferences, knowledge, and information. Both sides benefit as a real community is created through such a conversation. If personalization (the consumer's desire) and consumer data (the marketer's desire) coincide so perfectly, marketing has succeeded. These, however, are exceptions.

In all such exchange of information, systemic value creation must remain under the control of the consumer and should not become a totalizing property of the networked marketspace. The power

balance has shifted to the marketers, who are now able to "turn the consumer inside out" (Levy, 1998). It is critical for consumers to be aware of the threats that accompany the ascendance of these new technologies into every aspect of their existence. This is a difficult task and this article only provides a first step into creating such awareness. Much more remains to be done especially since the electronic "arms race" of the networked marketspace will hardly slow down.

Notes

1. Many examples of such a double discourse on technological progress come to mind. The assembly line ushered in productivity increases **and** workers' alienation. The arrival of the train in 19th century USA led to greater mobility (for wealthy whites) **and** expedited the conquering of Indian land and the extinction of the Buffalo. Atomic fission has produced inexpensive energy **and** disasters like Hiroshima and Chernobyl.

2. Under this term we include popular techniques and data mining tools such as collaborative filtering, clustering, and artificial intelligence (AI). For a detailed discussion of these personalization tools see Allard, Graves, Gluck, May and McAteer (1999).

3. The decision to use "citizen" instead of the more logical choice "customer" was a deliberate one as credit card companies as well as mail catalogue companies and others have long understood the fact that it is as valuable to have information on customers as on non-customers. Also, as we realized by talking to a high-level German executive who moved to New York for a 3-year assignment, his non-citizen status excluded him from such databases, making it very difficult for him to obtain credit in the U.S.

4. Companies that build systems for such databases understand this all too well. That is why Scott McNealy, CEO of Sun Microsystems, reportedly made the blasé statement: "You have zero privacy… Get over it!"

5. The practice, known as profiling, gives marketers the ability to know the household, and in many cases the precise identity, of the person visiting any one of the 11,500 sites that use DoubleClick's ad-tracking "cookies."

6. The coding problem, according to Brooks Fisher, Intuit's vice president, occurs when the GET command--which allows users to input data into Web forms--is used, because it builds a URL, or a specific page on the Net. It also includes information from the previous page in the Web address.

Acknowledgment
The authors wish to acknowledge support from the Research Institute for Telecommunications and Information Marketing (RITIM) at the University of Rhode Island, USA and from the Department of Computer Science at Aalborg University, Denmark. Comments from the editor and reviewers for *The Journal of Research for Consumers* are also gratefully acknowledged.

References

References

Allard, K., Graves, L., Gluck, M., May, M. and McAteer, S. (1999), "Proactive Personalization*", ericaclark.com*, (http://www.ericaclark.com/article4.html).
Allen, D. E. and McGoun, E. G. (forthcoming), "Hedonic Investment," in Hoch, S. J. and Myer, R. (eds.), *Advances in Consumer Research*, Provo, UT: Association of Consumer Research.
Arnould, E. J. and Price, L. L. (1993), "River Magic: Extraordinary Experience and the Extended Service Encounter," *Journal of Consumer Research*, 20, (June), 24-45.
Baudrillard, J. (1985), " The Masses: The Implosion of the Social in the Media," *New Literature History*, 16, (3), 577-589.
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 Pennock, R. J. and Chapman, J. W. (ed.), *Privacy* (pp. 1-26). New York: Atherton Press.
Bennett, C. J. (1996), "The Public Surveillance of Personal Data: A Cross-National Analysis," in Lyon, D. and Zureik, E. (eds.), *Computers, Surveillance, and Privacy* (pp. 237-259). Minneapolis: University of Minnesota Press.
Bernstein, N. (1997), "Personal Files Via Computer Offer Money and Pose Threat," *New York Times*, (Jun. 12), A30.
Bridis, T. (1998), "Judge: Trans Union Can't Sell Credit Details to Marketers," *Marketing News*, 32, 20, p. 18.
Clarke, R. (1991), "Information Technology and Dataveillance," In Dunlop, C. and Kling, R. (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.
Dekleva, S. (2000), "Electronic Commerce a Half-Empty Glass?" *Communication of AIS*, 4, (Article 18).
Firat, A. and Dholakia, N. (1998), *Consuming People: From Political Economy to Theatres of Consumption*. London: Routledge.
Firat, F. A. and Venkatesh, A. (1993), "Postmodernity: The Age of Marketing," *International Journal of Research in Marketing*, 10, (3), 227-249.

Firat, F. A., Sherry, J. F. and Venkatesh, A. (1994), "Postmodernism, Marketing and the Consumer,". *International Journal of Research in Marketing*, 11, (4), 311-316.
Foucault, M. (1972), *The Archaeology of Knowledge: A Discourse on Language*. New York: Pantheon Books.
Gandy, O. H. J. (1996), "Coming to Terms with the Panoptic Sort," in Lyon, D. and Zureik, E. (eds.), *Computers, Surveillance, and Privacy* (pp. 132-155). Minneapolis: University of Minnesota Press.
Ger, G. and Belk, R. W. (1996), "I'd like to buy the world a Coke: Consumptionscapes of the 'Less Affluent World', *Journal of Consumer Policy*, 19, (3), 271-304.
Godin, S. (1999), *Permission Marketing: Turning Strangers into Friends, and Friends into Customers*. New York: Simon & Schuster.
Harvey, L. (2000), "It's All About Me and You: How Personalization Can Build Better Customer Relationships," *personalization.com*, (http://www.personalization.com/soapbox/contributions/harvey.asp).
Hoffman, D. L., Novak, T. P. and Peralta, M. A. (1999), "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *The Information Society*, 15, (2), 129-139.
Johnston, M. (2000), "Privacy Debate: Is Orwell Online?" *PCWorld.com* (April 26), (http://www.pcworld.com/resource/printable/article.asp?aid=16503).
Junnarkar, S. (2000), "Intuit Plugs Leaks to DoubleClick," *CNET News.com* (March 2), (http://news.cnet.com/news/0-1007-200-1562341.html).
Kling, A. (2000), "Impersonalization," *personalization.com*, (http://www.personalization.com/soapbox/contributions/kling2.asp).
Kling, R. and Allen, J. P. (1996), "How the Marriage of Management and Computing Intensifies the Struggle for Personal Privacy," in Lyon, D. and Zureik, E. (eds.), *Computers, Surveillance, and Privacy* (pp. 104-131). Minneapolis: University of Minnesota Press.
Kotler, P. and Armstrong, P. (1996), *Principles in Marketing*. Englewood Cliffs, NJ: Prentice Hall.
Krishnamurthy, S. (2000), "The Problem with Personalization," *personalization.com*, http://www.personalization.com/soapbox/contributions/Krishnamurthy.asp).
Levine, R. (2000), *The Cluetrain Manifesto: The End of Business as Usual*. Cambridge, Mass.: Perseus Books.
Levy, P. (1998), *Becoming Virtual: Reality in the Digital Age*. New York and London: Plenum Trade.
Locke, C. (2000), "Personalization and Privacy: The Race is on," *personalization.com*, (http://www.personalization.com/soapbox/).
Lunefeld, P. (1999), *The Digital Dialectic*. Cambridge, MA: MIT

Press.
Miller, P. and Rose, N. (1997), *Mobilizing the Consumer. Theory, Culture, and Society*, 14, (1), 1-36.
Nakamura, L. (1995), "Race in/for Cyberspace: Identity Tourism and Racial Passing on the Internet," *Works and Day* 25/26, 13, (1&2), 181-193.
Negroponte, N. (1995), *Being Digital*. New York: Knopf.
Newell, F. (1997, *The New Rules of Marketing: How to Use One-To-One Relationship Marketing to be the Leader in Your Industry*. New York: McGraw-Hill.
Ong, W. J. (1982), *Orality and Literacy: The Technologizing of the Word*. London and New York: Methuen.
Peppers, D. and Rogers, M. (1997), *Enterprise One-To-One: Tools for Competing in the Interactive Age*. New York: Currency Doubleday.
Pitofsky, R. (1996), "FTC to Media: Screen Ads Better," *Advertising Age*, 67 (April 29), p. 30.
Plant, S. (1997), *Zeros + Ones: Digital Women + The New Technoculture*. New York: Doubleday.
Poster, M. (1990), *The Mode of Information*. Chicago: The University of Chicago Press.
Rayport, J. F. and Sviokla, J. J. (1994), "Managing in the Marketspace," *Harvard Business Review*, 72, (6), 141-150.
Robinson, S. (1999), "CD Software Said to Gather Data on Users," *The New York Times* (November 1), C1, C10.
Rodger, W. (2000), "Activists Charge DoubleClick Double Cross," *USAToday.com* (January 25), (http://www.usatoday.com/life/cyber/tech/cth211.htm).
Samuel, A. (1999), "German Shepherds," *Business 2.0* (May), (http://www.business2.com/content/magazine/ideas/1999/05/01/11766).
Shapiro, C. and Varian, H. R. (1999), *Information Rules: A Strategic Guide to the Network Economy*. Boston, Mass.: Harvard Business School Press.
Solomon, M. R. and Englis, B. G. (1997), "Breaking Out of the Box - Is Lifestyle a Construct or a Construction?" in Brown, S. and Turley, D. (eds.), *Consumer Research: Postcards From the Edge* (pp. 322-349). London: Routledge.
Taylor, C. (June 26, 2000), "Looking Online," *Time*, 155, (26), 56-62.
Turkle, S. (1995), *Life on the Screen*. New York, NY: Touchstone.
Varney, C. (1998), "You Call This Self-Regulation?" *Wired*, 6, 6, p. 107.
Virilio, P. (1997),*Open Sky*. London and New York: Verso.
Virilio, P. (1998), "Le Règne de la Délation Optique," *Le Monde Diplomatique*, August, 20, p. 20, (http://www.monde-diplomatique.fr/1998/08/VIRILIO/10812.html).

Wallace, C. (1998), "Inmates Inc. - How Your Personal Info Ends Up in Convicts' Hands," *ABCNews.com* (Feb. 18), (http://more.abcnews.go.com/onair/ptl/html_files/transcripts/ptl0218a.html).
