Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right

DETLEV ZWICK AND NIKHILESH DHOLAKIA

A b s t r a c t

This paper explores the regulatory philosophies underlying the debates on privacy in e-commerce in the European Union and the United States. It offers a framework to grasp these differences and suggests that, in the ultimate, e-commerce players with transatlantic ambitions may need different organizations to deal with the EU and US privacy regimes.

Keywords: e-commerce, electronic markets, privacy, Europe, USA, regulatory philosophy

INTRODUCTION

Models of privacy protection that have evolved on either side of the Atlantic are rooted in very different regulatory philosophies. The European Union has taken the stance that regulation is essential to provide protection for citizens in the marketplace, be it e-commerce or regular commerce. The United States, despite recent initiatives to re-assess its policy approach, has largely refused to pass legislation to regulate privacy and favours self-regulation of e-commerce.

US MODEL OF SELF REGULATION

Self-regulation entails the setting of standards by an industry group or certifying agency and the voluntary adherence to such standards by members or associates. In the US, the Better Business Bureau, for example, sets voluntary standards of ethical business practices in general.

In the area of online marketing, the Direct Marketing Association has taken a strong self-regulatory position. DMA's self-regulation is an attempt to create a fair social contract by providing customers with knowledge and control (Milne 1997). Other efforts in the USA include the TRUSTe initiative, with Microsoft as a major player. The US Federal Trade Commission (FTC) has developed voluntary guidelines for companies to adopt for their websites. Overall, the public and private sector initiatives have favoured voluntary approaches over central regulation.

Recent Developments in the US Position

Recently, US legislators have questioned the effectiveness of the 'self-regulation' approach on the Internet. As evidence mounts of e-commerce sites abusing their power to collect consumer information, the belief is growing that the profit principle governing business practices inherently contradicts consumers' privacy interests (Boyle 1999).

In May 2000 the Federal Trade Commission, reacting to a glaring case of privacy policy violation by *Geocities*, moderated its heretofore-unfettered support for industry self-regulation in regard to consumer privacy. It recommended that Congress enact broad legislation to protect the public's private data on the Internet. The commission's report, however, has been contested even within the organization and whether legislation will eventually be put in place remains to be seen. The Bush presidency would in general steer clear of attempts at government regulation of the Internet. At any rate, at least on the policy level, faith in the ability of the industry to

A u t h o r s

Detlev Zwick (dzwi2898@postoffice.uri.edu) is a Doctoral Candidate in Marketing at the College of Business Administration at the University of Rhode Island, USA. He is currently working on an in-depth study of 'investors as consumers' in the fast-growing electronic stock markets of USA and Europe.

Nikhilesh Dholakia (nik@uri.edu) is Professor of Marketing, E-Commerce and International Business in the College of Business Administration at the University of Rhode Island, USA. His research focuses on Information Age Strategies in the Global Economy and on Global Consumer Culture.

Volume 11 (2): 116–120. www.electronicmarkets.org

regulate itself has been waning and more hybrid solutions to the problem may gain currency.

For example, in summer 2000 the US Department of Commerce and the European Commission formulated the 'safe harbour agreement' that circumscribes the level of protection to be given to European personal information. The arrangement is designed to guarantee the safety of online data transfers between the EU and the US, as stipulated by the EU Data Protection Directive of 1998. In addition, US companies aiming at entering the online markets in Europe will need to achieve 'safe harbour' status.

In short, the Agreement states that consumers must be notified about the purposes for which the company collects and uses information about them. Further, each safe harbour company must give individuals the opportunity to choose whether and how the personal information they provide is used by or disclosed to third parties. Third parties who receive consumer information must provide the same level of privacy protection for that information as the company itself provided. In addition, safe harbour companies must protect information from loss, misuse, unauthorized access, disclosure, alteration or destruction. But they must equally ensure that data is reliable for its intended use, accurate, complete and current. Finally, safe harbour companies must give individuals the right to view, correct, amend or delete information about them held by the company. Firms need to provide mechanisms for ensuring compliance with the privacy principles and the company's privacy policies.

EU MODEL OF GOVERNMENT REGULATION

The EU Directive on Privacy Protection is a legal prescription for national legislators regarding the treatment of information acceptable to the 15 European Union member nations (Swire and Litan 1998). In essence, the EU Directive:

- *Imposes obligations on data controllers.* These include entities that process personal data, such as corporations on customers and employees; hospitals on patients; and book/record clubs on customer preferences. The Directive has provisions to ensure that data are not misused.
- *Is all encompassing.* Processing is defined broadly to be any operation performed upon personal data. This can include – whether by automatic means or otherwise – the collection, recording, storage, alteration, retrieval, consultation, disclosure by transmission and erasure of data.
- *Is intended to 'harmonize' national privacy laws.* EU member states are, however, in principle free to introduce higher standards than those required by the Directive.

The Directive provides a common platform for laws governing the exchange of data and the enforcement of regulation within the EU member nations. The overall intent is to facilitate the free flow of information within the EU. The Directive prohibits the export of data out of the EU to areas lacking adequate protection (including, at present, the United States).

Despite some emerging interest in the United States to legislate about privacy on the Internet, it is clear that the US self-regulation and EU regulation still represent starkly different approaches to consumer privacy. But perhaps more important than the discussions on the level of public policy are the underlying assumptions that drive privacy initiatives on both sides of the Atlantic. We therefore need to move beyond legislative questions and explore the regulatory philosophies of privacy. An understanding of key differences in regulatory philosophies will help firms seeking to participate in the transatlantic online market spaces.

REGULATORY PHILOSOPHIES OF PRIVACY: COMMODITY VERSUS BASIC CIVIL RIGHT

Miller (1971) wrote that 'the 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'. Perhaps in the digital age privacy in its strict sense – as the conscious and controlled protection of personal information – cannot 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: 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. This consumer anxiety about data protection and privacy in the digital age poses a threat to global e-commerce. Therefore, national governments, business organizations and consumer advocates – all with interest in privacy issues – need to come together as a group of 'privacy peacemakers' (Belgum 1999). While the problem seems clear, the possible solutions remain controversial. Finding a broad consensus seems difficult.

On the surface, the issue revolves around the age-old question of government regulation of the economic sphere versus a self-regulated marketplace. Under the surface of this political debate, a more basic struggle is occurring over the meaning of privacy based on the distinction between *possession* and *ownership*. Markets are a means by which agents exchange *ownership of expected value*. Possession is a physical circumstance, *while ownership is socially constructed* (i.e., property right). If a legitimizing authority does not confer ownership to one's possessions, then one still possesses but does not own. *Only ownership bestows the right to exchange in the marketplace.* Is privacy or personal information a possession or an owned resource?

While every consumer has *possession* of personal information, the critical question is who is the owner: the state, a datamining corporation, or the consumer? The answer to this question decides whether consumers are reduced to passive objects of protection from market forces or motivated to be active and entrepreneurial in the emerging digital marketplace.

The self-regulation model following traditional libertarian ideals of property right in market economies – is based on the assumption that privacy in the digital age be defined as personal property of the data subject (Boyle 1999). This view of market opportunism (Belgum 1999) (which, it should be pointed out, is currently not easily compatible with constitutional concerns in the US, most notably the First Amendment) abets the commodification, and thus marketability, of personal information. Such an approach implies *individual ownership of privacy* in the form of personal information. Ownership then permits the consumer, as a rational economic decision-maker, to trade personal information as a commodity in a decentralized marketplace (Murphy 1996). The marketer in this scenario is a legitimate transaction partner.

The regulation model, on the other hand, adheres to the traditional notion of privacy as a basic civil right – an integral part of being a citizen. Such a right cannot be appropriated or violated by the economic sphere. Defined as a civil right, privacy escapes commodification, but not the notion of possession. It is important to note that the EU directive endows the data subject with a form of possession right over his or her personal information that the data subject in the US does not enjoy under current law. Indeed, the EU privacy directive only makes sense if the data subject – and not anyone who has collected and stored personal information as is the case in the US – is the inalienable possessor of his or her own personal information. Unlike the property right that the data subject enjoys in the self-regulated model of market opportunism, however, this form of possession is non-economic and must be protected from third party appropriation (e.g., businesses). Thus, possession in the regulatory model is not like ownership because personal information cannot be owned by anyone in an economic sense. Only political solutions to privacy threats are allowable.

Table 1. Philosophical Assumptions of the Two Privacy Models

	Regulation Model	*Self-regulation Model*
Consumer	Citizen (To be protected)	Homo Economicus (Maximizer of benefits)
Marketer	Potential violator of rights (To be regulated)	Exchange Partner (Maximizer of benefits)

Thus understood, privacy cannot be traded by economic agents in the marketplace. It must be protected by the state or other legislative system in charge of safeguarding the rights of its citizens (including the citizen *qua* consumer). The marketer here is conceived as a potential threat to the citizens' rights (see Table 1). We look at both models briefly before discussing the implications for e-commerce.

Privacy as Property and Commodity

The idea of personal information as property is not new. It has a long legal and social history. 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 1971: 211). Edward Shils is even more encompassing. He claims 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 1971: 212). The intention of such definitions was to provide the carrier of personal information with the right to sue when there was information abuse.

This perspective, however, overlooked the much more substantive consequence of the privacy–property nexus. Karl Marx (1978) posited 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 height of the industrial age, was referring to raw 'labour power'. In the post-industrial age, however, the centre of capitalist production in not labour-power but the accumulation and exchange of information (Poster 1990). In fact, not production but consumption is at the heart of late capitalism (Jameson 1984). It is not the worker's labour-power but the consumer's personal information that now carries value. Yet, in order for it to attain an exchange value, 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 consumers of the property discourse endorsed implicitly by the US government (represented by the FTC, FCC, and US Commission for Privacy) and propelled explicitly by US 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 (Murphy 1996; Tapscott 1995; Varian 1997). Businesses interested in data acquisition can then offer a price to the consumer, thus mimicking – in inverted roles – a regular commercial transaction. At this moment, privacy becomes unhinged from its constitutional location, commodified as personal information, and relocated in the economic field (Habermas 1990). The marketization of privacy can be discerned in the language used by some commentators as they state that 'disclosure of privacy policies by

data gatherers is designed to stimulate market resolution of privacy concerns' (Clinton and Gore 1997). This relocation opens up a new exchange landscape for consumers, which we discuss later. In contrast, the European Union's approach, to which we turn now, is quite different.

Privacy as Civil Right

A general argument underlying the EU directive is that treating personal information as property would have the undesirable consequence of placing responsibility on individuals to protect their own interests. While in the age of mechanical production of information (photographs and print media) the individual's *control* over his or her personal information was still considerable, in the digital age this is no longer the case. With control largely lost, responsibility for privacy protection has moved ever more urgently into the focus of legislation. Without an external authority imposing and enforcing regulations on business organizations, the individual consumer's interest for protection and the business's interest for data accumulation are in direct conflict. Businesses have a superior position in the ensuing unequal bargaining procedure (Miller 1971).

Unlike the Americans, Europeans are unwilling to put the protection of privacy under the rule of competition (Samuel 1999). The EU politics surrounding the Directive are fuelled by the established view of privacy as a human rights issue. As Hurley (1998, italics added) states, 'In Europe, privacy and personal data protection is regarded as an *inalienable right* because it is so important to [the consumer's] dignity and sense of autonomy.' Under such a position privacy is not understood as a tradable property of the individual consumer. Privacy is an inalienable right, like human or civil rights. Privacy is accorded to the individual as a type of freedom and autonomy and as such is a possession. Ownership of the data can only be a socially constructed circumstance as in this case via the authority of the state. In fact, in the first modern constitutions, basic rights provided an image of the liberal model of the public–private divide. In this liberal model, 'society' is guaranteed to its citizens as a sphere of private autonomy (Habermas 1990). Under this traditional understanding of privacy, personal information is not to be 'owned' as much as protected – against repressive state power as well as greedy business practices (Poster 1995). The authority stewarding privacy is, of course, the government.

In its operative provisions, the EU Directive 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 could safeguard it. Privacy, therefore, is irreducible to the individual property principle and personal information cannot be commodified.

IMPLICATIONS

In terms of implied philosophical assumptions, then, the European position on the online privacy of consumers is diametrically opposed to that of the US administration and business groups. The two models imply very different business and consumer strategies.

In the self-regulative model built on libertarian market principles and property rights, the firm is required 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. After obtaining all such information and evaluating all possibilities, the consumer makes a rational decision as to what 'amount' of privacy s/he is willing to give up for a specific 'Rate of Incentive.'

As a result, the self-regulatory market model does not focus on the importance of privacy or the role it plays in the lives of individuals or society. Instead, it focuses on describing the theoretical benefits and limitations of free and active markets in private information, identifying obstacles to creation of such markets, and proposing policy measures designed to foster development of such efficient markets. The goal is to let consumers share in the value of their own personal information (Belgum 1999).

One can envision individual consumers entering into transactions online with individual websites. The marketer requests information and thus prompts the consumer to demand a *quid pro quo* in the form of money, credit or discount for online goods and services. Another possibility would be that groups of consumers use information brokers to package their aggregated information and market it to commercial buyers. The data subject would share in the profits the information package would generate in the marketplace. Laudon (1997) even foresees a kind of stock market, the National Information Exchange, where individuals would have the right to sell their information to the highest bidder. In the last instance, the self-regulation model proffered by scholars such as Varian and Laudon entails a dramatic role reversal – the marketer transforms from a seller of goods and services to a buyer of consumer information.

In the regulation model, however, the marketer–consumer relationships are freed from the specifics of the transacting parties' strategies, values and goals. The role of the marketer, then, is limited to compliance with privacy regulations and to communicate a successful conformity (Swire and Litan 1998). The role of the consumer is a passive one as the ownership of privacy or personal information has not been transferred to the individual. Exchange value for privacy cannot be established nor, of course, exchange of privacy for incentives.

CONCLUSIONS

Privacy protection has played and will continue to play an important role in

the development of e-commerce. Two models have emerged from the debates so far, the self-regulation model, in some variations popular in the US, and the regulation model, preferred by the EU. Both models operate with quite different concepts of privacy.

The implications of the two models for businesses and consumers are important. If the self-regulation model is accepted in conjunction with market rules and property rights, consumers enjoy a tremendous freedom of personal information management but at the potential cost of 'information overload' in terms of negotiating privacy-related affairs. Businesses, correspondingly, have to evolve a whole range of strategies to build and sustain a myriad of trust and market relationships.

If the regulation model is accepted, consumers possess the right to privacy but cannot use personal information as a tradable commodity. Businesses are obligated to protect consumers' personal data within a well-defined legal framework. Strategic flexibility exists only in terms of how well businesses communicate their conformity to privacy regulations.

As e-commerce develops greater transatlantic links, these two positions on privacy will continue to tangle. While periodic accommodations will be reached to allow mutual e-commerce, in the longer run many businesses will be forced to create separate transatlantic organizations to deal with the two distinct privacy concepts.

References

Belgum, K.D. (1999) 'Who Leads at Half-time? Three Conflicting Visions of Internet Privacy Policy', *Richmond Journal of Law and Technology* 6 (Symposium 1999)(1), http://www.richmond.edu/jolt/v6i1/belgum.html

Boyle, J. (1999) Chapter from *Net Total: Law, Politics and Property in Cyberspace*, [online] http://www.law.yale.edu/censor/boyle.htm [accessed 15 December 2000].

Clinton, W.J. and Gore, A. (1997, 1 July). *A Framework for Global Electronic Commerce*, [online] http://www.iitf.nist.gov/eleccomm/ecomm.html [accessed 13 December 2000].

Dordick, H.S. (1995) 'The Social Consequences of Liberalization and Corporate Control in Telecommunications', in Drake, W.J. (ed.), *The Information Infrastructure* (pp. 155–72), New York: The Twentieth Century Fund Press.

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

Hurley, D. (1998) 'Privacy in Play', *Think Leadership Magazine* (March), [online] http://www.ibm.com/ibm/ThinkMag/articles/privacy/text.html

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

Laudon, K.C. (1997) 'Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information', in *Privacy and Self-Regulation in the Information Age*, US Department of Commerce, [online] http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm [accessed 13 December 2000].

Marx, K. (1978) *Capital, Vol. 1*, New York: W.W. Norton & Company.

Miller, A.R. (1971) *The Assault on Privacy*, Ann Arbor: The University of Michigan.

Milne, G.R. (1997) 'Consumer Participation in Mailing Lists: A Field Experiment', *Journal of Public Policy and Marketing*, 16(2), 298–309.

Murphy, R.S. (1996) 'Property Rights in Personal Information: An Economic Defence of Privacy', *Georgetown Law Journal* 84, 2381–418.

Poster, M. (1990) *The Mode of Information*, Chicago: The University of Chicago Press.

Poster, M. (1995) *The Second Media Age*, Cambridge: Polity Press.

Roesler, A. (1997) 'Bequeme Einmischung. Internet und Offentlichkeit', in Munker, S. and Roesler, A. (eds), *Mythos Internet* (pp. 171–92), Frankfurt am Main: Suhrkamp.

Rosenoer, J. (1995, August) 'The Privacy Directive', *CyberLaw*, [online] http://www.CyberLaw.com/cylw0895.html

Samuel, A. (1999, Ma) 'German Shepherds', *Business 2.0*, [online] http://www.business2.com/content/magazine/ideas/1999/05/01/19652

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

Tapscott, D. (1995) *The Digital Economy*, New York: McGraw-Hill.

Varian, H.R. (1997) 'Economic Aspects of Personal Privacy', in *Privacy and Self-Regulation in the Information Age*, US Department of Commerce, [online] http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm [accessed 13 December 2000].