EU DATA PROTECTION POLICY

THE PRIVACY FALLACY: ADVERSE EFFECTS OF EUROPE'S DATA PROTECTION POLICY IN AN INFORMATION-DRIVEN ECONOMY[1]

Professor Lucas Bergkamp, Hunton & Williams, Brussels

The European Union has established a comprehensive legislative privacy framework aimed at protecting data pertaining to individuals. The EU is currently in the process of amending and supplementing its data protection legislation to prepare for the information society. In this article, Professor Lucas Bergkamp questions the desirability and necessity of the EU's data protection regime in the information society. He examines the "other side" of data protection law and identifies its paradoxical and adverse effects. Based on a thorough analysis of how privacy law affects markets, he argues that data protection restricts consumer choice and freedom, and results in consumers receiving outdated, lower quality products and services at higher prices. The author proposes possible alternative approaches to data protection in Europe, and identifies the groundwork that needs to be conducted to devise a sensible, balanced privacy framework for the information society.

INTRODUCTION AND SUMMARY

The European Union (EU) has established a comprehensive legislative framework aimed at protecting data pertaining to individuals. This regime applies to a wide range of data held by both public and private entities, imposes serious restrictions on data processing by such entities, grants broad rights to data subjects, and effectively requires government notifications and approvals for many processing operations. To administer this program, new agencies and bureaucracies have been established throughout the EU. The EU is currently in the process of amending and supplementing its data protection legislation to prepare for the information society. The contemplated changes will not address the regime's assumptions and fundamentals, but extend and refine the existing framework for an internet-based and information-driven economy. The EU's data protection programs are generally viewed as necessary and desirable to protect individuals against inappropriate uses of personal data and perceived increasing privacy risks, although empirical data about such risks and the law's effects is lacking. Indeed, there is little or no data on actual harms caused by privacy violations nor on the cost of data protection.

This article questions the presumed desirability and necessity of the EU's data protection regime. It examines the "other side" of data protection law and identifies its paradoxical and adverse effects. Based on a thorough analysis of how privacy law affects markets, it argues that data protection restricts consumer choice and freedom, and results in consumers receiving outdated, lower quality products and services at higher prices. Data protection also prevents consumer empowerment. Unfortunately, the poor are hurt disproportionally and, due to data protection, in some instances cannot obtain goods or services. The EU trumps form over substance by requiring expensive procedures and business process. Further, the EU data protection regime increases risks of fraud and dishonesty. In addition, it restricts competition and raises trade barriers in violation of WTO law. European industry can survive under this regime only because enforcement is extremely lax. Data protection as currently conceived by the EU is a fallacy. It is a shotgun remedy against an incompletely conceptualized problem. It is an emotional, rather than rational reaction to feelings of discomfort with expanding data flows. The EU regime is not supported by any empirical data on privacy risks and demand. Accordingly, a debate on the foundations of EU policy is necessary before the EU proceeds with its data protection programs for the digital economy. This debate should be informed by facts about consumer privacy demand and the cost of data protection and alternative approaches. A future EU privacy program should focus on actual harms and apply targeted remedies.

The first part of this article briefly discusses the use of information in the information-driven, internet-based economy. In the second part, the EU's data protection legislation is briefly reviewed. This part describes the key features of current and proposed privacy laws, and analyzes the EC's approach to privacy and the foundations supporting its current legislation. The third part proceeds to identify and analyze the misunderstandings, misperceptions, and false assumptions underlying the data protection programs. It discusses also common justifications for the EU regime, and shows that they fail. In the fourth part, the paradoxical and unintended adverse consequences of privacy law are discussed in more detail. It outlines the contours of the fundamental issues that need to be addressed before the EU should start working on privacy law for the new economy. The last part proposes possible alternative approaches to data protection in Europe, and identifies the groundwork

ISSN 0267 3649/02/$20.00

that needs to be conducted to devise a sensible, balanced legislative privacy framework for the information society.

THE INFORMATION SOCIETY

The information society is on its way. Globalization and technology are important drivers of the information-based economy. Information is inherently global; it respects no boundaries.[2] Cross-border data flows have become indispensable to transnational enterprise. Technology greatly facilitates the ability to quickly gather and manipulate data relating to customers, prospects, employees, and other people. The information age permits consumers to gain access to more information, more suppliers, and a wider range of products and services in a shorter period of time, thus enhancing competition. Suppliers are able to communicate quicker and better with their customers and prospects. As Macklin observed, "[c]ustomer data will be the currency that drives growth in the business-to-consumer e-commerce over the next five years. It allows websites to tailor goods, services, and content to the consumer and provides advertisers with the most predictive buying patterns of current and potential customers."[3] They can target potential customers with greater accuracy (and thus greater chance of success), and offer personalized service and make personalized offers.[4] In the information society, consumers will receive what they want when they want it.

Likewise, employers manage numerous data concerning their employees. They need this data for various purposes, such as salary administration, evaluation, and to meet legal requirements. Additionally, employers may have an interest in monitoring and having access to data generated by employees, such as email messages.[5] In many multi-national corporations, employee data is transferred across borders and stored centrally on data servers for purposes such as benefits administration and advancement planning. Employees benefit from enhanced services, including increased accessibility, and additional career opportunities.

At the same time, the internet, e-commerce, and the information society have augmented concerns about privacy, personal data, and data flows. Indeed, there is a wide variety of consumer concerns and contexts involved in the privacy debate.[6] On the worldwide web, consumer behaviour can easily be monitored and so-called "digital profiles" can be created. Although there is little or no evidence of any harm or threatened harm, US research suggests that consumers are skeptical about control and security of their data.[7] In our information-driven economy, there are many corporations that specialize in data mining, processing, and management. Data collection, storage, and processing often involve various entities. Not surprisingly, the question has been raised whether we may expect any privacy in the information society. The Chief Executive Officer of a large US-based technology corporation is reported to have said "On the internet, there is no privacy. Get over it!" Privacy advocates, of course, have objected, and raised concerns about the lack of privacy in the digital economy. They call for new rights, including new constitutional rights, and additional legislation.[8] Meanwhile, some corporations have already started to cater to the consumer's demand for privacy.

Information, including personal data, already plays an important role in the day-to-day operations of virtually all businesses. The advancement of the information society, will increase the need for data and data flow.[9] The globalization process and the automation of data processing demand increased centralization and cross-border transfer of personal data.[10] Central data warehousing creates economies of scale, facilitates data enhancement and processing, and makes data management and uses more efficient and effective. Customers, employees, and other data subjects would stand to gain much from these developments.[11] As discussed below, the EU's data protection legislation will not let them benefit fully from these opportunities.

THE EUROPEAN UNION'S DATA PROTECTION LEGISLATION

Current and Proposed Privacy Laws

The European Union (EU) certainly did not get over the asserted absence of privacy in the information society. Instead, it embarked on an ambitious legislative program to protect the privacy of EC residents in the twenty-first century. Initially, privacy protection in Europe was driven by the desire to prevent government use of personal data for purposes of executing malicious policies, as had happened in Nazi Germany and other totalitarian states. The EU Commission started working on data protection legislation in the late 1980's, and has had a significant involvement in privacy issues ever since. In 1995, when several EU Member States had already adopted privacy legislation, the EU enacted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive"),[12] which establishes a broad regime of data protection. The Data Protection Directive is supplemented by Directive 97/66 on the protection of privacy and personal data in the telecommunications sectors,[13] which sets forth specific rules for the telecommunications sector.

The Data Protection Directive prohibits, subject to exhaustively listed exceptions, the collection and processing of personal data. As a consequence, with respect to each and every instance of data processing, the processor bears the burden of proving that the processing is lawful and the risk that he will not be able to meet this burden.[14] Where data collection is permitted, the law imposes serious restrictions on personal data processing, grants individual rights to "data subjects," and sets forth specific procedural obligations, including notification to national authorities. Unlike the selective US legislative approach, EC data protection laws impose an onerous set of requirements on all sectors of industry, from financial institutions to consumer goods companies, and from list brokers to any employer. It applies to personal data processed by conventional or automated means.[15] Personal data is broadly defined to include coded data and some anonymous data. Rather than prohibiting or restricting harmful uses of information and permitting all other uses, the Directive starts from the opposite end and prohibits all data uses, except under certain conditions. Personal data may be processed (e.g. collected, used, or destroyed) only in certain specific situations described in the Directive.[16] Data may be collected only for "specific and legitimate purposes" and may not be "excessive."

The rules with respect to so-called sensitive data (including race, religion and health) are even more stringent. A data subject has a right to be informed about data processing and, in some instances, his prior consent must be obtained (also known as "opt in"[17]). In addition, a data subject has a right of access to the data pertaining to him and to rectify any incorrect data, a right to object to data processing, a right to confidentiality and security, a right not to be subjected to automated individual decisions, and a right to seek a judicial remedy and compensation where his rights are violated. Data processing must be "lawful and fair."[18] Subject to limited exceptions, the Directive prohibits the transfer of personal data to non-EU Member States which are deemed to offer an "inadequate" level of data protection.

The Commission has proposed an overhaul of Directive 97/66/EC to update it and provide for rules that are technology neutral.[19] This proposal favours the "opt-in" approach for direct marketing.[20] The EU has even included the right to data protection in the European Charter of Fundamental Rights.[21] Further, the Data Protection Directive is up for review this year, and the Commission will need to assess what amendments are necessary to meet the ever increasing challenges to privacy posed by the information society.[22] The Commission is to consider whether the Directive should apply also sound and image data. In addition, the Commission is considering whether legal persons should be brought under the Directive's scope.[23] In connection with the presentation of a Commission study on "junk" email, the Commission has indicated also that "the findings will (…) be taken into account (…) when proposing updates to EU data protection legislation," and noted "the potential for technological developments, particularly in terms of data collection, to undermine the strong standards of protection laid down in the Directive."[24] In other words, this one-sided view of technology may well fuel further legislative initiatives.

The Human Right Foundations of the EU's Privacy Laws

The EU's legislative program raises the question whether the existing privacy laws can simply be amended and supplemented to manage privacy in the information society. Or is a more radical change in EU law and policy required to effectively address privacy in the digital economy? From a thorough analysis of the EU's privacy legislation,[25] one can begin to reconstruct the basic characteristics and foundations on which this legislative structure is built. A sound understanding of these foundations is necessary for purposes of identifying the EU regime's assumptions, assessing its justifications, and analyzing its adverse and paradoxical effects.

The EU considers informational privacy not merely an interest, or a right, but a "fundamental right."[26] The human rights foundations of the right to data protection are the source of many positions of modern privacy advocates and the root cause of much confusion in today's privacy debate. The modern history of the right to privacy starts after the Second World War. In 1950, a fundamental right to "respect for private life" was included in the European Convention for the Protection of Human Rights and Fundamental Freedoms.[27] Although this right is referenced in the context of respect for family life, home and correspondence, the European Court of Human Rights and privacy scholars have interpreted it extensively.[28] The Convention was not intended to have "Drittwirkung," i.e. apply between individuals,[29] but has been interpreted to apply to both vertical (state-individual) and horizontal (citizen-citizen) relations.[30] In ***Niemitz v Germany***, the Court extended the right to respect for *private* life to *professional and business* life, thereby rendering contractual arrangements between employer and employees invalid to the extent they are inconsistent with the newly created right.[31] The modern right to privacy corresponds not only to negative obligations to refrain from doing certain acts (e.g. refrain from collecting "unnecessary" data, and from "inappropriately" monitoring an employee's email and surfing activities), but also to positive obligations to provide resources so that individuals can exercise their rights effectively. European data protection authorities have taken the position that an employee has a right to reasonable personal use of his employer's resources, such as the right to send and receive personal emails.[32] It is clear that Europe's notion of privacy has come a long way since Warren and Brandeis conceived it as "the right to be left alone."[33]

To confirm and reinforce its human rights foundations, data protection has recently been included in the EU Charter of Human Rights, which provides that "everyone has the right to the protection of personal data."[34] The Charter specifies, in unusual detail for a bill of rights, that "[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[35] An unfortunate consequence of including this right among truly fundamental rights, such as the prohibition of torture and slavery and the freedom of expression, is that the notion of fundamental right seriously devaluates, with adverse consequences for the respect for the core human rights.

Privacy Is Priceless

The fundamental character of the right to data protection, in turn, provides a basis for two further principles. This first is that the cost of privacy protection, which, as recent US research suggests,[36] is substantial, does not matter because privacy is fundamental and therefore must be protected in any event. The EU privacy legislation does not provide for exceptions where the costs of privacy protection are high or excessive. It accommodates other interests only to a limited extent and mostly in connection with state powers such as public security and national defence. Privacy is priceless. It is beyond cost, and accordingly data on the cost of the EU data protection regime is not necessary.

However, this proposition is false even if one accepts that privacy is a fundamental right. Like any other good, privacy protection is in competition with other rights for resources and is subject to the law of diminishing marginal returns. Once the most serious threats to privacy have been addressed, further investments in privacy protection may well exceed the value of any added protection, if any. It is unclear whether EU consumers are willing to pay a possibly significant price for the level of privacy set by the EU, and the EU does little to

find out.[37] Again, the philosophy seems to be that the facts do not matter because privacy is a fundamental right.

Privacy Is Inalienable

The second principle flowing from the "fundamental right" thesis is that privacy, because it is so fundamental, should be inalienable and non-waivable. In other words, even if an individual wants to give up some or all of his privacy rights (e.g. to obtain a lower price for a product or service), EU law will not let him do so.[38] The EU privacy rights cannot be waived in any manner. Consequently, any agreement pursuant to which a data subject waives some or all of his rights under the Data Protection Directive is void and unenforceable, even if the agreement otherwise meets all validity requirements and is in the data subject's interest. To protect data subjects anywhere in the world, the directive, through a complicated transfer regime, applies extra-territorially to any person that receives personal data from the EU. Although the directive permits transfers to non-EU jurisdictions if the data subject has given his consent, European data protection authorities have narrowed this exception by requiring that consent must be informed and truly free, thus declaring consent from certain groups, such as employees, legally invalid or doubtful.[39]

The conventional justification for making individual rights inalienable is that unsophisticated people would be lured or pressured into giving up their rights without understanding the consequences. These people need to be protected, the reasoning goes, and therefore privacy rights must be inalienable. But privacy rights have ended up being inalienable for all individuals, including those that need no protection whatsoever, and they are inalienable under any and all circumstances, including all situations where a waiver is in the data subject's interest.

Governmental Discretion and Ad Hoc Decision Making

Because privacy is deemed to be both fundamental and fluid, the EU has not defined it with any precision and granted broad discretion to government agencies to block or permit specific data processing operations. Under the EU's approach, privacy in Europe is like pornography in the US: the government will know a privacy violation when it sees one. If, in a particular case, data processing is not fair or not justified by the controller's legitimate interests, it violates the law.[40] Because data controllers will not be able to tell whether these vague principles are met, they will have to turn to the data protection authorities and request their blessing. In addition, data processing operations must be notified to the authorities, who have the power to investigate if the notification raises questions in their minds. Processing operations "likely to present specific risks" must be examined prior to he start thereof.[41] Social justice in privacy administration is deemed to require case-by-case balancing of interests and *ad-hoc* decision making in individual cases. Thus, the fundamental nature of the right to privacy legitimizes not only paternalism but also broad governmental discretion.

The risks of a discretion-heavy legal regime are evident. It reduces the coordination of behaviour, since we cannot tell what the law requires. Discretion thus creates inefficiencies, and limits our liberty since we are under a constant threat that our activities will be deemed non-compliant and we have to call on experts for help. Discretion further increases our dependency on government since we have to please them to receive the benefits. In the privacy area, these effects are clearly visible. But the government's privacy agencies, which have limited staffs and resources, have great trouble administering the system of government-approved exceptions to a broad privacy protection regime. Without any guidance from the legislature, they are called on to interpret vague principles in a consistent, coherent, and justifiable way. That is a daunting task, which many of the agencies are unable to meet.

FALSE ASSUMPTIONS AND FAILING JUSTIFICATIONS

This analysis of the Directive's basic characteristics allows us to identify and examine the underlying assumptions, perceptions, and beliefs, and to assess common justifications for the EU regime. In devising its laws and policies, the EU appears to have been guided by some implicit assumptions and perceptions about the value of information in the information society, and the nature of business process. To assess whether these often unspoken perceptions and implicit assumptions are accurate and appropriate for privacy policy in the information society, each is examined in turn below. This section then analyzes three common justifications for the EU regime, i.e. preventing harm, promoting individual autonomy, and preventing government abuse of private sector data.

The Value of Information Use

The EU's views on the value of information in the information society and its balancing of the various interests involved do not reflect economic reality. Information is at the core of a market-based economy, which depends critically on the accessibility of data. Information is multi-dimensional. On the one hand, the free flow of information has increased productivity and the efficiency of production.[42] Intelligent, creative use of personal data facilitates targeted direct marketing, thus reducing waste, increasing efficiency, and reducing the consumer's search and information cost. The consumer receives better, faster, and cheaper service.[43] The benefits of information have been empirically confirmed for consumer credit[44] and financial services,[45] and the mail order business.[46]

On the other hand, consumers have security, control, and economic interests in their data, but value such interests differently, and are willing to trade-off privacy for economic value (e.g. accept less privacy in return for a lower price). Consumer privacy preferences not only differ widely, but also evolve over time and with the introduction of new products, services, and technology. Corporations have an interest in protecting their information, which represents its intellectual capital. Information sustains not only business decisions, but also political and social decisions. Privacy thus is a dynamic, multi-dimensional issue. Accordingly, privacy legislation should carefully balance the various dimensions and interests involved.[47] Specifically, there is critical need for balancing

legitimate privacy interests with the responsible, productive use of personal information.[48]

In the EU's view, however, information is regarded as valuable not to consumers but only to for-profit corporations that will make intense use of personal data to sell their products or services, expand market share, or sell customer lists, thus creating privacy risks. The Directive's recitals do not even once refer to the benefits of data use to data subjects. References to "fundamental rights and freedoms," "risks" and "protection" are plentiful, however.[49] Apparently, the EU sees only half of the picture. The other half are the customers and web-surfers that benefit from business use of data in several ways. They receive more targeted and relevant information, they benefit from a larger range of products and services that are offered to them, they benefit from lower prices, et cetera.[50] The technology that makes this possible is not necessarily a threat to privacy, as is often assumed.[51] Although technological developments have aggravated privacy concerns, technology is able to provide solutions to many privacy problems.

Information, including personal data, is also undervalued in relation to the freedom of press and expression. Data is absolutely critical to the press, media, political, social and academic debate, et cetera. In the US, the tension between privacy protection and the freedom to disclose, disseminate, and receive information, which is protected by the First Amendment of the US Constitution, is widely recognized. Securing one person's privacy may infringe on another person's freedom of expression and information. The US privacy legislation is incomplete, maybe even incoherent, because the US has often given priority to the freedom of expression and information.[52] This would appear to be different in Europe. The EU's data protection regime clearly restricts the freedom of speech and expression and the freedom of information. It gives national governments the authority to provide for "necessary" exemptions for data processing for "journalistic" and "literary" purposes.[53] This would seem to be a risky arrangement; national government could decide not to provide any such exemptions, but, if they do, they have to define what the terms "journalistic" and "artistic" mean. The freedom of ordinary, i.e. non-journalistic and non-artistic, or commercial expression is not in any way accommodated by the Directive.[54] The fundamental question is whether the EU has any business regulating the possession and exchange of lawfully obtained and truthful information. Since the EU has no constitution, this issue does not get the same scrutiny as it gets in the US. However, by not providing for clear and broad exemptions, the EU underplays the significance of the freedom of expression and information, and of the restrictions imposed thereon by the Data Protection Directive.

The Nature of Business

In devising and implementing its legislative programs for the information society, the EU seems to concentrate disproportionately on private enterprise, partly, maybe, as result of the fact that government lags behind in moving its affairs onto the internet. There is much attention for privacy issues associated with personalized advertising and direct marketing. Despite the lack of any evidence of actual harm caused by privacy violations, private enterprise is thought to pose serious privacy risks, because the drive to make ever more profit is believed to cause corporations to completely disregard privacy if they have to.[55] In fact, however, business use of personal data in activities such as direct marketing is self-limiting. Government itself, much more so than private enterprise, poses privacy risks.[56]

The significant attention for private enterprise reflects a misunderstanding of the nature of business process. Unlike governments in some situations, private enterprise has nothing to gain by positively harming people. In market economies, business use, unlike government use, of personal data would appear to be self-limiting and self-correcting as a result of the market mechanism and the lack of externalities. If data use does not result in increased transactions, which are by definition consensual and thus agreed by data subjects, it will cease. If consumers want more privacy and are willing to pay for it, business will offer more privacy. The reality is that businesses are interested in having adequate means to service customers and develop the market at reasonable costs, *and* meet consumers' diverging privacy expectations. The government has no such incentives when it comes to dealing with is "enemies."[57]

Relatedly, the EU portrays the privacy issue in terms of consumers versus business. In doing so, it mis-characterizes business's role and the role of information in the economy. The real tension in the current privacy debate, as the Information Law and Commerce Institute has emphasized, is not between consumers and businesses, but rather between consumers' desire for greater privacy and their desire for the many benefits that flow from readily available personal information.[58] In other words, privacy is a conflict between "me and myself." By missing this critical point, the EU started off the wrong track.

Harms and Risks

Legislation involves the state's coercive powers and restricts the liberty of the persons that are subject to its obligations and requirements. Coercion and thus legislation is an evil, but it is sometimes justified. If legislation, by restricting the conduct of some persons, prevents a greater harm to other persons, it may be justified. The Data Protection Directive is aimed at protecting individual privacy and reducing the risks to privacy arising from data processing. In doing so, it seeks to ensure a "high level of protection."[59] Remarkably, the EU failed to identify against *what* exactly the directive protects, other than some vague references to "risks." What, then, is the threatened harm against which the EU data protection regime protects us?

This question reveals the Data Protection Directive's conceptual and empirical weakness. There are virtually no indications of actual harm caused by private sector privacy violations. The examples that are typically proffered are either trivial harms (e.g. receiving an undesired mailing), or completely hypothetical (e.g. information about food purchases being transferred by the supermarket's computer to the consumer's health insurer so that insurance premiums can be adjusted in function of health risks arising from eating habits). All known real harms have been caused by the state's invasion of privacy and abuse of information, from the Holocaust, to the "Schnüffelstaat" incident in Switzerland, to the Stasi-files that turned up after Germany's reunification. Even if companies were involved in some of these scandals, the wrongdoing was

directly related to the state's objectives, rather than to any market mechanism. In line with these historical data, the US citizens organization "Citizens Against Government Waste" found that today the private sector does a better job than the government in protecting personal information.[60] The Data Protection Directive, however, applies not only to public bodies but also to private persons and businesses.

Autonomy and Fraud

But what about autonomy, one might ask. Is not that the main objective of data protection? Indeed, privacy protection is often characterized as aimed not only at protecting data security and preventing harmful use, but also at promoting individual autonomy. Privacy protection allows an individual to define himself, i.e. determine "what face he wants to present to other people." Accordingly, the EU data protection policy is said to be based on the concept of "informational self-determination."[61] As noted above, EU privacy policy does not fully accept autonomy and provides a mechanism to correct individual decisions where they are believed to result in unfair or undesirable outcomes.

More importantly, by allowing people to determine the face they want to present to the world, we allow them to deprive others of a competitive or economic advantage, or to improve their own position otherwise at the expense of others. In particular, privacy protection restricts the ability to learn about the less attractive side of individuals and to communicate that information to others, and, hence, increases the risk that people misrepresent themselves and defraud other people.[62] [63] Privacy, Cate explains: "facilitates the dissemination of false information, such as when a job applicant lies about his previous employment, by making discovery of that falsity more difficult or impossible. Privacy similarly protects the withholding of relevant true information, such as when an airline pilot fails to disclose a medical condition that might affect job performance."[64] While possibly enhancing the autonomy of some, privacy law thus restricts the freedom to protect oneself against cheats. It also increases losses due to identity theft. As Cate and Staten explain, "[p]ersonal information is one of the most effective tools for stemming losses due to fraud and identity theft. Many consumers report that the first warning they receive about credit card fraud comes not from law enforcement authorities, but from a retailer or other business that detected an odd pattern of charging activity. Personal information is also essential to preventing, detecting, and solving other crimes and improving the public welfare, for example, by locating and contacting missing family members, heirs to estates, pension fund beneficiaries, witnesses in criminal and civil maters, tax evaders, and parents who are delinquent in child support payments."[65] The EU data protection regime deprives us of many of these benefits. Similarly, by granting employees a privacy right to use their employer's resources (computer, internet, email, telephone) for personal purposes[66] and denying employers a right to monitor employees' activities,[67] data protection law has further exacerbated the asymmetry of power in the employer-employee relationship, which has worked to the advantage of dishonest, recalcitrant, and under-performing employees. These adverse consequences should be weighed carefully against any benefits, if any, the right to define oneself might produce.

Data protection's autonomy rationale is invoked also to justify moves towards an opt-in system, pursuant to which data may be processed only after the data subject's unambiguous consent has been obtained. Opt-in, which is the functional equivalent of a property rights regime, indeed greatly enhances the autonomy of data subjects. But it does so at the expense of data controllers' autonomy. In addition, as discussed below, opt-in enhanced autonomy provides disincentives for creating valuable assets.

Government Abuse of Private Sector Data

The historical grounds for restricting data processing in the private sector are no longer persuasive. Historically, the harm addressed by data protection law was the possible use of personal data by governments to deprive people of fundamental rights, life and liberty. In totalitarian states, such as Nazi Germany and communist countries, both public and private sector data had been used for such purposes.[68] Hence, the historic justification for private sector restrictions was the potential for government abuse of personal data. If the private sector does not collect and store personal data, the government cannot misuse it. In other words, the best way to protect against government misuse was believed to be to not have data anywhere to misuse. Although it is odd, it may sound like a noble cause.

However, the policy of the government restricting the collection of data to assure that the government itself will not have access to information to misuse it, is not only odd, it is also morally questionable, and probably ineffective and inefficient. From an ethical viewpoint, does the government's own potential malice justify the government imposing restrictions on the individual liberty to collect data? Is it acceptable that the government invokes its own inclination to murder to restrict our freedom? This logic, of course, could be applied to a virtually endless range of activities and would have very undesirable consequences. If there are no guns, the government cannot wage wars, but we also could not protect our lives and property. If there is no nuclear expertise, the government cannot make atom bombs, but we also could not have nuclear energy. If there is no biotechnology, the government cannot convert us into obedient slaves, but we would not have biotech food and pharmaceuticals. If we accept this logic, we would gradually loose all of our freedom (or become extinct: if there are no people, the government cannot violate human rights). The fundamental misconception is that government failure requires additional government intervention to remedy such failure.[69] However, the solution to government failure is not more government; it is better, and often less, more limited government.

The policy of restricting private sector data to prevent government abuse is ineffective. It is ineffective not only because the EU privacy law does not apply to many government activities and grants broad exceptions for data use "in the public interest,"[70] i.e. by government, but also because it is unlikely that a malicious government would be prevented from executing its plans by any pre-existing data protection laws. It would abolish or work around those laws. But even if private sector restrictions delay the implementation of malicious governments' plans or make their lives more difficult, these favourable effects should be weighed against the cost of the restrictions. In short, to the extent possible future government

misuse of private sector data is an issue, it should be addressed by limiting government, rather than imposing onerous restrictions on the pirvate sector. If we are concerned that "big brother is watching us," we should impose appropriate restrictions on big brother himself.

PRIVACY LAW'S PARADOXES AND ADVERSE EFFECTS

In the past, when data was used mostly for only a single purpose, the cost of the EU regime's restrictions may have been relatively low. However in in the new economy, data is used for multiple purposes and much more intensely and effectively than ever before. In other words, the cost of the restrictions has gone up dramatically, because we now lose much more benefit than in the past. Even if private sector restructions were cost-justified in the past, they are probably no longer cost-effective.

As the discussion in previous sections has demonstrated, the foundations on which the EU's privacy law is built are unsound. The underlying assumptions, perceptions, and beliefs are erroneous. The EU's data protection regime has been conceived as a linear, single issue scheme. At bottom, it is premised on the assumption that citizens and consumers care little about anything but protection of the data pertaining to them. This assumption is doubtful, and the justifications for the EU regime fail. Consequently, the EU data protection regime is paradoxical and has many unintended adverse effects. The information society is global, while the EU's privacy legislation is isolationist and idiosyncratic. The internet and information society empower the consumer, while the EU applies the old economy's consumer protection-oriented model. The information society is radically decentralized, while the EU approach is based on strong centralization.[71] The information age encourages innovation and competition, while EU privacy law generates disincentives for innovation and restricts competition. Globalization and economic progress demand free trade, but the EU regime restricts trade. Privacy over-regulation will produce under-regulation, because overly stringent requirements will not be enforced. It imposes expensive business process, but fails to deliver value. It hurts the poor disproportionally and has regressive income effects. Privacy legislation seeks to protect privacy, but increases privacy risks by expanding the quantity of identifiable data.[72] As discussed above, privacy protection allows people to define themselves, buit increases the risk of fraud and other crimes, including terrorism. Privacy legislation hence is paradoxical and counter-productive. In this section, some of these paradoxes and adverse effects of the EU regime are analyzed in more detail.

Limiting Choice and Harming Consumers

First and foremost, government-dictated privacy preferences restrict consumer choice in at least two ways. First, they restrict choice by not permitting consumers to contract on the basis of their own privacy preferences. Second, they restrict consumer choice indirectly because they burden the introduction and marketing of new products and services (e.g. by increasing the price thereof and, in some instances, effectively banning the marketing). The privacy law that is intended to promote choice thus achieves the opposite result. It seeks to promote choice, but ends up restricting consumer choice by disregarding privacy preferences and adversely affecting supply. In the name of freedom, it reduces our freedom.

Consumers indeed are harmed positively where they are required to purchase, included in the price of goods and services they acquire, a privacy protection regime that they do not want. Privacy protection raises additional barriers to the introduction of new products, increases the cost of marketing products and servicing customers, and delays innovation. As a result, consumers suffer harm because they receive outdated, lower quality products and services at higher prices. In addition, privacy law raises serious distributional issues.

Paradoxically, while there is no sound research on harm resulting from privacy violations, there is a growing body of research on the cost of privacy and the harm to consumers caused by restrictive privacy laws.

Preventing Consumer Empowerment

The EU's legislative program is driven by an unspoken supposition that unrestrained, ruthless capitalism poses severe privacy threats and will inflict serious harm on consumers. Only the government is able to protect consumers against these threatened harms. EU policy thus is driven by paternalistic motives; individuals need to be protected and be given inalienable but vague fundamental rights, the scope of which government officials define *ex post* in specific cases.

In fact, however, the information age promises to reduce the need for consumer protection because it enables consumers to gain access to more information, more suppliers, and a wider range of options, including privacy policies, in a shorter period of time, thus enabling them to protect themselves.[73] In addition, technological advances, such as consumer privacy preferences procedures and blocking and filtering software, will reduce privacy concerns, since individuals will have easy access to most of the tools they need to obtain the level of privacy protection they desire. Unfortunately, the EU data protection regime undermines the development and application of this technology.

The Necessity of Lax Enforcement

In the past, business could survive under European privacy legislation only because enforcement was extremely lax and the government could grant ad-hoc privileges in any event. Even in member states that have had data protection laws on the books for more than a decade, the number of sanctions imposed for violations of the legal standards is very small.[74] Monitoring or verifying compliance with data protection rules, of course, requires thorough and laborious audits of a data controller's data collection, use, and management practices. The government agencies responsible for data protection have only limited powers and resources, and enforcement tends not to be their first priority.[75] As a result, regulated entities do not have appropriate incentives to comply with the law.[76] But governments are not inclined to rectify these shortcomings because they know what vigorous enforcement of privacy laws would do. As long as the public believes that there is a reasonably adequate protection regime in place, they have no incentives to take action.

Now that privacy law enforcement has become a matter of concern to the EU, 'neutralizing' the adverse consequences of privacy legislation through non-enforcement may no longer be an option. The Commission has the responsibility to ensure that member states adequately implement the Data Protection Directive, which requires not only that they transpose the directive correctly but also that they administer and enforce it.[77] The Commission may not be as easily manipulated into tolerating a lax enforcement regime, but its authority over enforcement is limited.[78] On the other hand, thus far, the Data Protection Directive does not seem to have much impact on practice. An internet privacy study conducted by Consumers International found that: "[d]espite tight EU regulation, sites within the EU are no better at telling users how they use their data than sites in the US." To the contrary: "[t]he most popular US sites were more likely than the EU ones to give users a choice about being on the company's mailing list or having their name passed on, despite the existence of legislation which obliges EU-based sites to provide users with a choice."[79] It remains to be seen, however, whether the EU will be able to get away with this hypocrisy,[80] now that the Commission has started to insist that data protection regimes abroad must be effectively enforced for data transfers to be permissible.[81] Once enforced, paternalistic, broad and relatively vague legislation that does not permit variation by contract, raises cost significantly, has perverse effects, and consequently does not even protect the consumer.

Form over Substance

Law requires form to implement and effectuate its substantive provisions. More so than the average law, privacy law requires form and procedures. The EU data regime, implicitly or explicitly, requires a significant number of forms and procedures. Data controllers must submit notifications to national data protection authorities for both data processing operations and data transfers. To be able to apply the law as the government wants it to be applied, they need to obtain opinions from the data protection authorities on a regular basis. They must provide notice to data subjects. Obviously, they have to be in a position to prove that they have done so and are required to develop notice forms,[82] document notice, obtain acknowledgements, et cetera. In some cases, the privacy law requires the data subject's consent, and controllers must develop consent forms, obtain the data subject's signature, and manage the documentation. The law gives data subjects a right of access, and data controllers must develop and implement often complicated access procedures, document access, et cetera. The law imposes a more onerous regime for sensitive data, which requires that data controllers separate sensitive data, establish separate management procedures, et cetera. To ensure extra-territorial application of the EU's comprehensive protection regime, transfers to non-EU jurisdictions are permitted only under a complicated and bureaucratic cross-border regime that imposes many formalities. Under this regime, controllers need to establish and document the necessary transfer procedures (enter into an adequate agreement, sign up for the Safe Harbor arrangement, obtain consents, apply for authorization from the data protection authorities), develop and implement appropriate compliance tools, et cetera. Specific procedures and contracts are necessary for onward transfers and data processing by third parties. Data controllers need assessment tools, employee training, dispute resolution procedures, and much more. The number of procedures and the amount of documentation are vast.

There is nothing inherently wrong with procedures, process, and documentation. It is inherent to law as an instrument of social control. And many data controllers are not unfamiliar with forms and procedures. But there should be a balance between form and substance. In the privacy context, the forms and procedures should help to achieve the law's objectives, and deliver value to data subjects. The onus of the law's process should be proportional to the value it delivers. Does the EU data protection regime meet this proportionality test? Is there a reasonable balance between form and substance? Although reliable data is lacking, the sheer volume of procedures and documents necessary to meet the EU data protection regime's requirements suggest an imbalance and disproportionality. Real world experience suggests that data subjects do not understand the forms and procedures and do not want to invest time and effort in learning about the controller's data management practices. It suggests that the Data Protection Directive requires a whole lot of expensive business process to deliver little or no value to data subjects.

Regressive Income Effects

The benefits and burdens of privacy protection are not distributed equally over rich and poor. Privacy protection is a superior (or luxury) good, which implies that the demand for it is not only a negative function of price but also a positive function of income and wealth.[83] The rich want more privacy protection than the poor. Consequently, privacy law has a regressive income effect and hurts the poor who are required to cross-subsidize the needs of a rich privacy elite.

The poor suffer disproportionately also where they already have less choice and pay higher prices than the rich. Take, for instance, consumer credit and lending. Due to privacy law's adverse effects on the free circulation of consumer credit information, loans or credit may no longer be available to the poor or only at substantially higher interest rates; the rich, on the other hand, may not be significantly affected by the restricted flow of their credit data.[84] Privacy protection thus indirectly causes economic and social exclusion. Similarly, a move from opt-out to opt-in in the catalog apparel sector would increase prices by up to 11% and those increases would disproportionally affect rural customers and those in less affluent city neighbourhoods.[85] Unfortunately, these effects are not recognized, denied or at best downplayed by the various participants in the privacy debate.

Disincentives to Create Valuable Assets

The EU data protection regime is moving towards opt-in, which requires explicit, informed, and unambiguous consent before data may be collected and processed. As noted above, an opt-in regime imposes substantial cost. Opt-in is so expensive because it establishes individual property rights in personal data. Property rights can be transferred only by consent. That is what makes property, and thus opt-in, regimes so expensive.[86] Precisely for that reason we should use opt-in only if the benefits it provides outweigh its significant cost. As

Cate and Staten put it: "'opt-in' is an exceptional tool that imposes high cost and harmful unintended consequences, and should therefore be reserved for exceptional situations where the risk of those costs and consequences is justified."[87] Opt-in, as a general rule, would thus have significant adverse consequences.[88]

Granting data subjects property rights in all data pertaining to them fails to recognize that the person that collects the data makes investments in collecting and manipulating the data, thus creating economic value. Sophisticated data controllers use the data that they collect to generate new data, including purchasing predictions. Consumer and customer databases are valuable corporate assets. "[T]he consumer information that firms acquire in the course of doing business," Litan has observed, "can be one of the most valuable assets on their balance sheets, which some may closely guard while others may sell or share with third parties."[89]

We have answered the question "whose data is it" too quickly. There is no reason to grant a data subject a property right in data merely because the data pertains to him. The person that collects and manipulates the data has made the investments to create a valuable resource; the data subject has not in any significant way contributed to that value creation. Corporations will have a disincentive to make these investments and create economic value if they do not obtain full intellectual property rights in these assets. Opt-in regimes limit a corporation's intellectual property rights and thus provide disincentives for worthwhile economic activity that generates the assets we need to make our lives better. An opt-in rule, or any data subject property right, therefore is undesirable from a public interest perspective.

Anti-Competitive Effects and Trade Barriers

The EU privacy laws restrict competition directly and indirectly. Direct restrictions are caused by the law eliminating privacy protection as an element of competition between suppliers in a market. EU law, offering a "high level of protection," prescribes the "privacy product" that corporations must offer, and no deviations are permitted. As a result, all corporations offer the same level of privacy protection and any competition as to privacy protection is excluded. In addition, privacy regulation directly reduces competition in markets for direct marketing services by burdening the sale or licensing of many products and services involving customer data.

Relatedly, privacy law indirectly restricts competition in other markets by restricting the availability of customer data in the market. New entrants and small companies are often put in a competitive disadvantage by privacy regulation. As Litan has observed, switching from opt-out to opt-in would: "raise barriers to entry by smaller, and often more innovative, firms and organizations." Litan explains that under an opt-in regime: "organizations would have to painstakingly build solicitation lists from scratch, a task that would be prohibitively expensive for all but the very largest commercial entities."[90] Indeed, open access to third party information (and the use of that information for targeted marketing) is essential to leveling the playing field for new market entrants. Information-sharing hence promotes competition by facilitating the entry of new competitors into established markets, reduces the advantage that large, incumbent firms have over smaller startups, and encourages the creation of businesses specialized in satisfying specific customer needs.[91] Because the EU has misconceived the role of data flows in the economy, the anti-competitive effects of privacy law have been overlooked.

There is strong empirical evidence for the competition-distorting effect of privacy regulation in the financial services industry. A study by Kichenman established that: "[e]fforts to open the [EU] financial services industry — to foster the development of competition, better serve customers, lower prices, and compete more effectively with US institutions — have largely failed because of restrictive privacy laws."[92] Restrictive privacy laws act as a competition barrier by giving the dominant incumbent firm a monopoly over the customer information it possesses while denying new market entrants the information needed to offer and market financial services. As a result, Kitchenman concludes, consumer lending is not common and where it exists, it is concentrated among a few major banks in each country, each of which has its own large database.[93] The EU data protection regime has thus had the effect of protecting the EU market from foreign competition in the wake of financial modernization.

By creating new barriers to entry and augmenting existing ones, the EU data protection regime also adversely affects international trade.[94] The more data-intensive the sector of industry, the stronger this effect. Accordingly, the data protection regime raises huge barriers to direct marketing services and consumer credit services. Even if the effect is not as strong with respect to other products and services, non-EU traders are disadvantaged in entering the EU market because they do not have access to the consumer data they need to engage in targeted marketing. The EU regime affects US traders disproportionally. The trade-restrictive effects are much stronger for US business than for EU and other non-EU businesses because US businesses are more advanced in the use of information.[95] This suggests that the EU Data Protection Directive may have been driven also by protectionist motives.

Indeed, the EU data protection regime may be in violation of WTO law, which extends also to e-commerce.[96] This may be so not only with respect to services under the General Agreement on Trade in Services (GATS),[97] but also with respect to products under the General Agreement on Tariffs and Trade (GATT). The EU privacy laws may not discriminate on their face, but, as noted, they target specifically a clear competitive advantage of US business, i.e. data management and customer relations management. The evidence of an exclusionary intent and disguised trade restriction is strengthened further by the disparate levels of enforcement of the privacy rules; enforcement under the Safe Harbor arrangement and the model contracts is more stringent than enforcement of the Directive within the EU.[98] With respect to services covered by the GATS, this disparity would seem to violate also the requirements that US service providers be treated as favorable as EU providers,[99] and that regulation must be applied in a "reasonable" manner.[100] In any event, if the EU effectively bans data flows to the US, but not to other countries with "inadequate" protection regimes, it would most likely violate the GATS most favoured nation clause.[101] The EU data protection regime would probably not be saved by the exception for trade restrictions aimed at protecting "the privacy of individuals,"[102]

because these restrictions will likely not be deemed "necessary" to secure compliance with the EU data protection regime as less trade-restrictive are available. This is so, for instance, because the Directive's data transfer rules, by their terms, require merely "adequate" foreign privacy protection, not "equivalent" or "identical" protection, while the Safe Harbor regime and model transfer contract impose equivalent protection. The EU's data transfer regime is also unnecessary because it fails to reflect the effect of superior US enforcement mechanisms and the *de facto* better compliance records. Once the adverse effects of the EU regime are more widely recognized, political and media pressure would no longer exercise undue influence on the WTO's adjudicating system, and the EU may be forced to change its practices.[103]

Research on Privacy and the Cost of Protecting IT

Empirical data on privacy have long been completely nonexistent. In the last several years, sound research is beginning to appear. Indeed, throughout this article, references have been made to studies on privacy, privacy protection, and the cost thereof. Virtually all sound research on the cost of privacy has been done in the US. Paradoxically, the EU has adopted a far more elaborate privacy protection regime than the US, but no research on the cost or benefits of privacy law has been conducted in the EU.

Although it has been widely recognized that information and information technology have been driving economic growth, no research has been done on the information's effect on productivity, because no sound methodology has yet been developed. The research that has been carried out focuses on what happens when data is removed from business process.[104] From a theoretical perspective, one can predict that restricting data flows will interfere with the market, and impose cost on businesses, consumers, and the economy as a whole. A growing body of research has confirmed these theoretical projections. It demonstrates in specific and practical terms that restrictive privacy laws intended to protect consumers impose real costs on consumers, in the form of higher prices, worse products and services, greater burdens and inconvenience, and less opportunity. More generally, it shows that privacy laws cause a serious drain on the economy as a whole.[105]

The EU, as noted, has not conducted any empirical research on critical issues such as harms caused by privacy violations, consumer attitudes towards privacy and privacy protection, and the cost of privacy protection. The lack of empirical data on these issues is a major and fatal deficiency. While there is no research on the cost of privacy, the EU has commissioned a study on the cost of unsolicited commercial communications.[106] When this study was released, the headline of the Commission's press release read as follows: "Commission study: 'junk' email costs internet users euro 10 billion a year worldwide."[107] The next line of the press statement refers to "an estimated euro 10 billion a year." Many newspapers and magazines have reported this finding and the euro 10 billion number without questioning it. There would appear to be no reason to question the number as it constitutes empirical research and is reported by a reputable government institution, which presumably would not dare to report junk research results. However, the study to which the Commission refers does not contain any research data on the cost of 'junk' email.[108] Instead, it appears that the euro 10 billion number is based entirely on dubious assumptions, speculation, and flawed methodology. Specifically, the study assumes that "sooner or later every email marketer will acquire the technical capacity to transmit 100 million emails daily."[109] The study does not cite any support for this assumption. Moreover, the "sooner or later" is highly relevant; the later that situation will arise, the less relevant the issue is now. The researchers, apparently by way of example, then state that "200 senders with that sort of capacity could mean 20 billion commercial emails being sent every day."[110] Thus, "[e]very websurfer[111] would receive an average of over 60 emails a day, representing a download time of approximately one hour with current technology." The assumption that technology does not evolve is dubious; with the advance of broadband, download time will decrease dramatically in the course of a few years. Based on some further cost estimates, which are again not supported by any references, the researchers arrive at a "conservative" estimate of euro 10 billion in total cost.

Although the flaws in this research are dramatic, the most telling error may be the total absence of any consideration of benefit arising from these commercial communications. Many unsolicited emails are not "junk," but meet a real consumer need. We know from research that people do respond to unsolicited communications and appreciate such messages.[113] The Commission shows to be totally ignorant of this and even went so far as to label all of these communications as "junk" email. This not only introduces a further wholly unsupportable assumption (namely, that all "unsolicited" email is "junk" email), it also sounds like a modern form of censorship. We do not need the government to decide for us what is junk and what is not. Some advertising and advocacy by the government for its own programs is unavoidable, but ideological propaganda is a different thing.

As noted, this research is intended to support a move towards "opt-in," a least with respect to electronic commercial messages. The implicit assumption in the Commission study is that an "opt-in" rule would be observed by the senders of these messages. However, for a number of reasons, that assumption is erroneous. A distinction should be made between what is referred to as "spam" and legitimate commercial messages that meet a real need. Many of the "spammers" (who sell dubious and sometimes outright unlawful services and products) are already in violation of the law and they will not care about violating an additional rule. It will be easy for these companies to move their marketing operations to outside the EC. The marketers that would comply with an "opt-in" rule are those that offer legitimate products and services that meet a real need. These companies are also the ones that do typically not employ the "shotgun" approach that characterizes "spamming," but they utilize targeted direct marketing techniques. Thus, the "spamming" problem would not be solved, but we would be deprived of the targeted direct marketing messages that are so valuable to us. (By restricting targeted marketing, the law unfortunately creates an increased risk of spamming, yet another paradox of privacy law.) The solution to the spamming problem will come from technological innovation, such as filtering techniques, not from government intervention.[114]

ALTERNATIVE APPROACHES

Under the current data protection regime, corporations either have to live with substantial legal uncertainty or with the delays and risks involved with *ad-hoc* decision making by the bureaucracy. As discussed above, consumers must purchase products and services with a government-dictated 'one fits all' privacy policy attached to them, as a result of which diversification and consumer choice are eliminated. Privacy law's marketing rules impede and delay the introduction of new products, as a result of which consumers receive old products, at higher prices, and with worse service. The law imposes expensive business process but fails to deliver value to data subjects, and the poor are hurt disproportionately. It creates disincentives for value creation, restricts competition, and raises trade barriers.

Is that the kind of law we need to protect privacy in the information society? Given its paradoxes and adverse effects, the answer obviously is no. Indeed, it is remarkable that governments have been able to adopt and implement such onerous, expensive, and paradoxical data protection regimes without any plausible evidence of harm or threatened harm, entirely based on some vague notion of a "fundamental right" and hypothetical risks.[115] In its rhetoric, the EU has misled the public to believe that its data protection regime was merely implementation of pre-existing fundamental rights. But the EU privacy protection laws are the emperor's new clothes, and the little boy who observes that the emperor is naked is ridiculed. The EU has never tried to define and analyze the right to privacy with the precision required for legislative programs. Once the paradoxes and adverse effects of the current privacy regimes are understood, it will become clear that government regulation of data flows is not the way to go. And once the promises of the information-driven economy are understood, it will become clear that the current legislative framework imposes even higher cost in the information-driven society. Government policy makers do what they can to maintain and improve the existing privacy structure. However, it is doubtful whether that will be enough to save it from collapse once the information society kicks into full gear. The EU therefore urgently needs to start studying alternatives to the current data protection regime.

Both consumers and business want workable law, legal certainty, and freedom of contract.[116] Regulation should be compared to alternative, less interventionist approaches. On the internet, reasonable contractual safeguards and a fair privacy policy agreed between the parties involved are not only the most effective way to enhance privacy, they are also the only way to meet consumers' diverging demands for privacy protection. Private privacy initiatives should therefore be strongly encouraged by the government. A market-based approach will result in a better balance between privacy and other interests in the information age.[117]

A Fundamental Choice

The privacy issue presents a classical choice of political philosophy: do we rely on the market or on the government to produce and deliver privacy? Who do we trust to resolve our privacy issues: technology companies or governments? Or do we need both to act? This indeed is a fundamental choice. Markets are flexible and accommodate diverging demands, law imposes a "one- fits-all" solution, creates "forced riders," and focuses on form rather than substance.

If there is asymmetry of information and a market failure, government intervention may be justified. But the key questions are where the market fails, in what way it fails, and what intervention could correct the failure without causing other adverse effects. Not every market failure calls for government intervention; the remedy may be worse than the disease. Why and for what groups would we need minimum privacy standards? Asymmetry of information would appear to call for no more than disclosure obligations, unless consumers are unable to decide for themselves. If consumers are currently not able to protect themselves, what tools would enable them to do so? Assuming consumers are able to decide, are there externalities that require government measures? These are the kinds of questions that should be at the roots of the privacy debate. If they are ignored, both private enterprise and consumers will pay the price.

A Debate About Fundamentals Based on Facts

The EU should be interested in these fundamental questions. Before moving ahead on the basis of a set of questionable assumptions, an informed and thorough debate should take place. The empirical basis for the EU's vast and expensive data protection regime is unbearably and irresponsibly thin. The coming debate should be informed by facts, not hypothetical "privacy risks" and rhetoric about "fundamental rights." We need facts about consumers' understanding of business use of information and their perception of the benefits of free data flow and data protection. We need facts about actual harms resulting from privacy violations, what consumers want (who demands how much privacy protection), how much privacy costs, and whether consumers are willing to pay the price for the privacy they claim. We need to understand better whether, and, if so, why the market fails to deliver the desired privacy protection, and whether there are any externalities that the government can effectively address. We need to identify and analyze the unintended adverse consequences of alternative data protection rules. On the basis of these facts, the debate should revisit the objectives of the EU's privacy policy.

Privacy and Its Constituent Parts

As noted, the EU has not attempted to define privacy, which is the conceptual basis for its Data Protection Directive.[118] The EU is not to blame for this failure; no adequate definition of privacy has ever been produced. It is a common feature of any privacy analysis to start with a disclaimer about the inherent difficulty or impossibility of defining exactly what "privacy" is, or of dissecting the concept into its various components.[119] This, in itself, raises a question about the wisdom of privacy legislation. The Data Protection Directive regulates the processing of personal data, rather than privacy itself, but that does not remedy the absence of a sound conceptual basis. In functional terms, it is entirely unclear what problem the EU data protection regime is trying to solve. The Data Protection Directive does not shed any light on this issue. It may be a solution, but what is the problem?

Even if the term "privacy" may serve a purpose in social discussions, it is probably not suitable as a concept for

government intervention. The reason is not only that privacy is vague and undefined, but also (and relatedly) that it means different things to different people. Flaherty, for instance, uses a very broad privacy concept that includes: "privacy in terms of architecture and town planning, family and community life, religious practices, social legislation, and law enforcement."[120] There are many other definitions, which all differ, include fewer or more elements, and emphasize different aspects. Despite this fluidity, privacy may still be a useful concept for informal discourse. However, it should not be used in formal discussions, let alone in legislative debates. Instead, specific elements that often are often deemed to be part of the privacy concept should be examined to determine whether and, if so, how they could provide a solid basis for building legal structures. Along these lines, Abrams has suggested that privacy should be disaggregated into its constituent parts, including consumer security, autonomy (i.e. "a sense that matters are under control"), and value (i.e. "all the benefits of a digital age in the form they want it when they want it").[121] Noting that the growth of privacy law has taken chaotic forms, Epstein has concluded that protecting certain forms of privacy (such as that against eavesdropping) works to the long-term advantage of all individuals, while other claims for privacy (such as shielding medical records from employers and insurers) should not be protected by law.[122] Once the privacy concept has been taken apart, one can begin to deal with its constituent parts in a targeted, more useful, and less harmful fashion.

Targeted Approaches to Preventing Harm

Based on the analysis set forth in this article, the EU data protection regime appears to be misconceived and misfocused. It is not merely over-inclusive and overbroad, but is built on foundations that are not able to support the data protection structure. The focus has erroneously been on data as such, instead of harm arising from data uses. "Restrictions on the flow of information in a more information-oriented age," Kitchenman explains, "may be the equivalent at the dawn of this new century to tariffs between nations at the dawn of the last."[123] We have been able to get rid of tariffs, but it took us quite some time. Hopefully, we will be able to eliminate restrictive privacy laws in a shorter time span. Indeed, if the EU data protection regime were abolished *in toto* tomorrow, very few citizens and consumers would be any worse off, and many would benefit significantly.

The EU regime misconceives the role of information in the economy. As all other information, personal data (to be sure, exactly the same data) can be used or misused. The EU restricts data collection and processing to prevent perceived misuses, but at the same time seriously limits valuable uses. Proper and valuable uses are much more common than improper, harmful uses. The EU regime regulates at the wrong level and fails to balance competing interests properly. It regulates the collection and processing of data upstream, while it should regulate specific harmful uses downstream.[124] The foundations of the EU regime therefore should be reexamined. Once the foundations are clearly understood, two questions should be addressed. First, what default data protection regime (if any) should be created by the legislature? Second, is there a core of privacy that should be inalienable and protected by law? These questions will refocus the debate on the concepts of harm and remedies. Although law cannot and should not address all harms, it should seek to prevent and provide adequate remedies against some harms and threatened harms, possibly including privacy-related harms.

Where law is an appropriate and effective instrument, we need to identify the harm with precision so that we can craft a precise and targeted solution that does not cause "collateral damage." An increasing number of privacy scholars reaches a similar conclusion. Litan, for instance, favors a balancing framework that weighs the benefits of the free flow of information against the possible threats to privacy on a *case-by-case* basis. Using this balancing approach, Litan advocates narrowly targeted legislation aimed at enhancing protections of sensitive medical and financial information.[125] In other words, harmful use of data requires a "surgical" remedy targeted solely at that specific harmful use, rather than a "shotgun" remedy aimed at a wide range of imaginary and unidentified potentially harmful uses. The core of privacy that law protects should be clearly defined in terms of harmful uses and remedies. Imaginary harms must be addressed by communication and education, not by legislation and regulation.[126] Once people understand business use of information, the benefits of free flow, and the cost of privacy, their privacy preferences may well appear to be not what we believe them to be. While the research and debate proceed, a moratorium on any further legislation would be appropriate, and enforcement should be based on Commissioner Bolkestein's suggestion of "fair application."[127]

Professor Lucas Bergkamp, Hunton & Williams, Brussels

FOOTNOTES

[1] I presented a short version of this paper at a seminar hosted by FEDMA and the Center for Information Policy Leadership @ Hunton & Williams (*Data Flows and Individual Autonomy: The Benefits of Free Flow and the Cost of Privacy*, Brussels, May 22, 2001). I am grateful for comments received from participants at that seminar, including Ulf Brühann, Commission of the EC, and Paul de Hert, Catholic University Brabant (KUB). In addition, Marty Abrams, Professor Fred Cate, Oscar Marquis, and Jan Dhont, all of the law firm of Hunton & Williams, and Professor Corien Prins, Catholic University Brabant (KUB), made helpful comments and suggestions. My thinking on this subject has been shaped by discussions in the context of the *Global Solutions Project of the Center for Information Policy Leadership @ Hunton & Williams.*

[2] Cate F. Global Information Policymaking and Domestic Law *Indiana Journal of Global Legal Studies 1994*, p467-487.

[3] Macklin BW. E-Commerce at What Price? Privacy Protection in the

Information Economy. Australian National University, 08/04/99.

[4] Amazon.com's Vice President for Global Public Policy has testified that Amazon.com: "uses personally identifiable customer information to personalize the shopping experience at our store. Rather than present an identical store front to all visitors, our longstanding objective is to provide a unique store to every one of our customers." Misener P. Prepared Witness Testimony. How Do Businesses Use Customer Information: Is the Customer's Privacy Protected? House of Representatives. The Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection. July 26, 2001

[5] Personal data regarding employees raises two sets of issues. First, it raises issues under the European Community's (EC) legislation on the protection of personal data. Second, if employers screen or monitor employees and the data that they generate, privacy and confidentiality arise under human rights, constitutional, privacy protection, and labour laws. For a fuller discussion of these issues see Bergkamp L, Dhont J. Managing Workplace Privacy. *World Data Protection Report*, July 2001, pp. 22-25.

[6] Cate FH. The Privacy Commission: An Examination of Privacy Protection. Subcommittee on Government Management, Information and Technology, Committee on Government Reform, US House of Representatives, April 12, 2000.

[7] Harris & Associates, Westin AF. *Privacy Concerns and Consumer Choice*. Washington DC: Independent Survey, 1998. Harris & Associates, Westin AF. *E-Commerce and Privacy: What Net Users Want*. Washington DC: Independent Survey, 1998. A recent survey by Harris Interactive revealed that a trust gap exists between consumers and businesses about information exchange. Privacy Leadership Initiative. New Survey Reveals Trust Gap Exists Between Consumers and Businesses About Information Exchange. New York, April 2, 2001. <www.understandingprivacy.org>.

[8] A commission in The Netherlands, for instance, has proposed new constitutional rights for the information society.

[9] Cate has argued that the: "fact that we are in the midst of rapid, significant change — not just in technologies but also in the new services, markets, and activities that those technologies are facilitating — argues against legislative action." Cate FH. Privacy In Electronic Communications. Prepared Statement before the Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, US House of Representatives, March 26, 1998.

[10] Branscomb has said that: "[t]ransborder data flow has become indispensable to the very existence of transnational enterprise and to the currently flourishing global marketplace (…) Information is the lifeblood that sustains political, social, and business decisions." Cited in: Cate F. Global Information Policymaking and Domestic Law. *1 Indiana Journal of Global Legal Studies 1994*, pp. 467-487.

[11] As Cate has argued, electronic information networks offer extraordinary advantages to business, government, and individuals in terms of power, capacity, speed, accessibility and cost. Cate FH. *Privacy in the Information Age*. New York: Brookings Press, 1997.

[12] OJ L 281/31 (23.11.95). For a commentary on the Data Protection Directive, see Damman U, Simitis S. *EG-Datenschutzrichtlinie*. Baden-Baden: Nomos, 1997.

[13] O.J. L 24/1 (30.01.98).

[14] This reversal of the burden of proof restricts liberty to a much greater extent than a regime that requires that the government prove that the data processor has violated the law. As a result of the asymmetry of proof, it is much easier to prove positively that an activity results in specific harm to specific individuals than to prove negatively that it will not cause any harm to any individual. See Jasay A de. Justice. In: Newman P (editor). The New Palgrave Dictionary of Economics and the Law. Volume 1. London: Macmillan, 1998, pp. 400-409.

[15] Recital 4 states that: "the progress made in information technology is making the processing and exchange of such data considerably easier." Recital 4, Data Protection Directive. Recital 27 stipulates that: "the protection of individuals must apply as much to automatic processing of data as to manual processing." Recital 27, Data Protection Directive.

[16] Member states may adopt exemptions to safeguard public interests such as public security, the investigation of crimes, important economic or financial interests, and certain regulatory functions. Articles 8(4), 8(5), and 13, Data Protection Directive.

[17] Opt-in for direct marketing is currently required in Austria, Denmark, Finland, Italy, and Germany. Cate and Staten have persuasively argued that "'opt-in' provides no greater privacy protection than 'opt-out' but imposes significantly higher costs with dramatically different legal and economic implications. Specifically: "'opt-in' is an exceptional tool that imposes high cost and harmful unintended consequences, and should therefore be reserved for exceptional situations where the risk of those costs and consequences is justified." Cate FH, Staten ME. *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In" (2001)*.

[18] Article 5, Data Protection Directive.

[19] Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, COM (2000) 385 final, 2000/0189 (COD).

[20] The Commission claims that the proposed opt-in model is supported by a Commission study, which allegedly found that: "from the point of view of industry, 'permission base marketing' is providing a more effective and viable method of data collection." Commission of the EC. Commission study: "Junk" email costs internet users euro 10 billion a year worldwide. Press release, 2 February 2001. However, the study itself does not support this statement. It asserts merely that permission-based marketing is on the rise, will become: "the standard for commercial communication on the internet," and "changes the parameters of the privacy protection issue without offering a completely satisfactory solution." There are no comparative data regarding various marketing methods in terms of effectiveness and viability from industry's viewpoint. Gauthronet S, Drouard E. Commission of the European Communities. *Unsolicited Commercial Communications and Data Protection*. ETD/99/B5-3000/E/96. January, 2001. Nothing indicates that the study was peer-reviewed.

[21] Article 8, Charter of Fundamental Rights of the EU. OJ C 364/1 (18.12.2000).

[22] Article 33, Data Protection Directive provides that: "the Commission shall report to the Council and the European Parliament at regular intervals (…) on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments."

[23] See Korff D. *Commission Study on the protection of the rights and interests of legal persons with regard to the processing of personal data relating to such persons*. ETD/97/B5-9500/78. Cambridge, October 1998.

[24] Commission of the EC. Commission study: "Junk" email costs internet users euro 10 billion a year worldwide. Press release, 2 February 2001.

[25] Bergkamp L, Dhont J. Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web. 7 *EDI Law Review 2000*, pp. 71-

114. Bergkamp L, Dhont J. Applying Europe's Data Protection to the Internet: More Questions than Answers. *World Data Protection Review 2001*, Part 1, April 2001, pp. 25-28, Part 2, May 2001, pp. 19-21.

[26] The object clause of the Directive provides that: "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." Article 1, Data Protection Directive.

[27] Article 8, European Convention for the Protection of Human Rights and Fundamental Rights, as amended by Protocol No. 11, Rome, 4.XI.1950, <http://conventions.coe.int>.

[28] For an overview, see De Hert P. *Artikel 8 EVRM en het Belgisch Recht: De bescherming van privacy, gezin, woonst en communicatie*. Gent: Mys & Breesch, 1998.

[29] Van Dijk and van Hoof comment that: "the problem of *Drittwirkung* (third party effect, LB) was not taken into account when the Convention was drafted, if it played any part at all in the discussions. One can infer from the formulation of various provisions that they were not written with a view to relations between individuals." Van Dijk, van Hoof. *Theory and Practice of the European Convention on Human Rights. Second Edition*. Deventer: Kluwer, 1990, p. 17.

[30] Verhey LFM. *Horizontale werking van grondrechten, in het bijzonder van het recht van privacy*. Zwolle: WEJ Tjeenk Willink. 1992.

[31] **Niemitz v Germany**, ECHR, 23 November 1992, Series A No. 251/B, para. 29. The Court held that: "[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings," and there is no reason why this understanding of the notion of private life "should be taken to exclude activities of a professional or business nature, since it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world."

[32] Registratiekamer. Goed Werken in Netwerken: Regels voor controle op email en internetgebruik van werknemers. http://www.registratiekamer.nl. It is not clear whether the employer may require that the employee reimburse the cost; at best, the employer may hope to be able to recover the direct out-of-pocket expense.

[33] Warren SD, Brandeis LD. The Right to Privacy. 4 *Harvard law Review 1890*, pp. 193-220.

[34] Article 8 (1), Charter of Fundamental Rights of the EU. OJ C 364/1 (18.12.2000).

[35] Article 8 (2), Charter of Fundamental Rights of the EU. OJ C 364/1 (18.12.2000). The Data Protection Directive, which limits the right of access and rectification, would appear to be in conflict with these provisions. The Charter, however, is not binding.

[36] For reasons that are unclear, the third section of Article 8 provides that: "[c]ompliance with these rules shall be subject to control by an independent authority."

[37] See, for instance, the studies published by the Privacy Leadership Initiative, www.understandingprivacy.org. Many of these studies are referenced in this article. A study by Hahn estimates the costs of various aspects of proposed online privacy legislation. Using "fairly conservative" assumptions, Hahn finds that these costs easily could be in the billions, if not tens of billions of dollars (the estimated range is USD 9 to 36 billion). This fact alone, Hahn concludes, suggests that proposed regulations that would flow from these laws could have a substantial economic impact on consumers and businesses. Hahn argues that online privacy regulation is premature because the costs could be substantial, no good quantitative estimates of the benefits of such regulation exist, and the market is reacting to and addressing consumer concerns. Hahn RW. An *Assessment of the Costs of Proposed Online Privacy Legislation* (May 7, 2001).

[38] No empirical data are available on these issues. The economic studies that were undertaken at the request of the Commission are very scanty. See, for instance, for a study that claims to estimate the cost of spamming in Europe, Gauthronet S, Drouard E. Commission of the European Communities. Unsolicited Commercial Communications and Data Protection. ETD/99/B5-3000/E/96. January, 2001.

[39] The Data Protection Directive establishes a public law regime that cannot be varied by a private law contract.

[40] Article 29 Data Protection Working Party. Opinion 8/2001 on the processing of personal data in the employment context. Brussels, 13 September 2001, 5062/01/EN/Final, WP 48.

[41] Cf. Articles 6(1)(a) and 7(f), Data Protection Directive.

[42] Article 20(1), Data Protection Directive.

[43] "The responsible use of personal information enhances the speed of credit, insurance, and many other financial services decisions; reduces the cost of virtually all financial services; gives consumers real choices; facilitates consumer mobility; and 'democratizes' opportunities." Cate FH. The Privacy Commission: *An Examination of Privacy Protection. Subcommittee on Government Management, Information and Technology,* Committee on Government Reform, US House of Representatives, April 12, 2000.

[44] Cate notes that in 1997: "82% of auto loan applicants in the US received a decision within an hour, 48% within 30 minutes. Many retailers open new charge accounts at the point of sale — in less than two minutes. This is unheard of in countries where restrictive laws prevent business from routinely collecting the information on consumer activities that is necessary to support rapid, accurate credit decisions." Cate FH. *Privacy in Perspective.* The AEI Press, June 5, 2001.

[45] Barron JM, Staten M. The Value of Comprehensive Credit Reports: Lessons from the US Experience (2000). These researchers applied Australian laws over US historic experience using credit scoring. They found that 19% of the American public that should get credit would not have gotten it under the Australian rules. The reason is that the US credit reporting system uses full positive and negative information (negative indicates who failed in the past and positive and negative combined predict future behaviour); privacy laws do not permit that these tools be developed and used and, as a result, lenders are more restrictive. Abrams M. *US Research on the Cost of More Restrictive Privacy Laws.* In: FEDMA/Center for Information Policy Leadership. *Data Flows and Individual Autonomy: The Benefits of Free Flow and the Cost of Privacy*. Brussels, May 22, 2001. The Barron-Staten study suggests that consumer credit will be less available and more expensive in countries that restrict the reporting of credit information by type of information or by parties with whom the information can be shared. Consumer credit in restricted-reporting countries is more expensive both in terms of finance charges, and in other features of the loan, including down payment, convenience of access, credit limits and fees. Long-term effects of credit reporting restrictions include impairing the growth of consumer spending and growth in consumer durable industries. Cf. *Information Law and Commerce Institute. The Cost of Privacy* (2001).

[46] Glassman CA. Customer Benefits from Current Information Sharing by Financial Services Companies (December 2000). This US

study found that information sharing saves the customer of 90 financial services institutions (accounting for 30% of industry revenues) USD 17 billion per year (USD 195 per average household) an 320 million person hours annually (4 hours per average customer household). This figure does not include savings resulting from the use of information to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards, and automated teller machines nationwide. It also does not include the lost benefits of future innovative services and products developed on the basis of an understanding of consumer needs. Cf. *Information Law and Commerce Institute. The Cost of Privacy (2001)*. See also Kitchenman WF. *US Credit Reporting: Perceived Benefits Outweigh Privacy Concerns (1999)* (because of accurate data, financial institutions avoid making bad loans and the consolidation of loans based on similar risk scores creates securitized investments and secondary markets).

[47] Turner M. *The Impact of Data Restrictions on Consumers Who Buy Apparel from Catalogs and the Internet (December 2000)*. This study assessed the cost of moving from an opt-out regime to an opt-in regime. The cost would be more than USD 1 billion in the catalog apparel industry alone. Prices would increase by up to 11%. Price increases would disproportionally affect rural customers and those in less affluent city neighborhoods. Abrams explains that catalogers use data to (i) match their files and improve their addresses to assure delivery of catalogues most cost effectively, (ii) enhance their files to understand current customers and chose who to mail to, and (iii) find new customers similar to successful customers. He points out that lifting response from 1.5% to 3% is a doubling of performance. Abrams M. US Research on the Cost of More Restrictive Privacy Laws. In: FEDMA/Center for Information Policy Leadership. *Data Flows and Individual Autonomy: The Benefits of Free Flow and the Cost of Privacy*. Brussels, May 22, 2001.

[48] According to Cate and Staten: "privacy is [not] unimportant or unprotected, but (…) it must be balanced — as consumers do in their choices every day — with the benefits that they enjoy because of the responsible use of personal information." Cate FH, Staten ME. *Putting People First: Consumer Benefits Of Information-Sharing (December 12, 2000)*.

[49] Cate FH. The Privacy Commission: *An Examination of Privacy Protection*. Subcommittee on Government Management, Information and Technology, Committee on Government Reform, US House of Representatives, April 12, 2000.

[50] See, for instance, Recitals 2, 10, 18, 23-27, 46, 53, 54, and 59, Data Protection Directive.

[51] Cate and Staten have identified six sets of benefits of data flows: identify and meet individual needs, increase efficiency and lower prices, enhance consumer convenience, inform customers of new opportunities, expand access to services and products, and detect and prevent fraud and other crimes. Cate FH, Staten ME. Putting People First: *Consumer Benefits Of Information-Sharing*. December 12, 2000.

[52] The EU over-emphasizes potential privacy risks arising from technology, and under-estimates its benefits to individuals.

[53] Maxeiner JR. Freedom of Information and the EU Data Protection Directive. <www.law.indiana.edu/fclj/pubs/v48/no1/maxeiner.html>.

[54] Article 9 of the Data Protection Directive stipulates that the member states must provide for exemptions for the processing of personal data: "carried out solely for the journalistic purposes or the purpose of artistic or literary expressions only if they are necessary to reconcile the right to privacy with the rules governing the freedom of expression."

[55] There is a general exception for "purely personal" data processing. Article 3(2), Data Protection Directive.

[56] The Commission's handbook on cost-effective compliance with the Data Protection Directive states that personal data can give the data controller "power" over the data subject, and "experience has shown that this power can be abused." No further explanation is provided. European Commission. *Handbook on cost-effective compliance with Directive 95/46/EC.* Luxembourg: Office of Official Publications of the EC, 1998, p.1.

[57] For a brief overview, see Kuitenbrouwer F. Privacy: een historisch vergelijkend overzicht. In: Prins JEJ, Berkvens JMA (red.). Privacyregulering in theorie en praktijk. Tweede druk. Deventer: Kluwer, 2000, pp. 33-56.

[58] For instance, secret service agencies in several countries have compiled extensive data bases on political opponents and other "*personae non gratae*," and applied subversive techniques in violation of law to render such individuals "harmless" to the government.

[59] *Information Law and Commerce Institute. The Cost of Privacy (2001).*

[60] Recital 10, Data Protection Directive.

[61] *Citizens Against Government Waste. Keeping Big Brother from Watching You*. <www.cagw.org> (28 August 2001). The CAGW cites numerous examples of government abuse of information, and concludes that: "there is ample evidence that the federal government is incapable of sufficiently protecting the sensitive data it collects."

[62] This concept was first articulated by the German Federal Administrative Court (Bundesverfassungsgericht). BverfG., EUGRZ, 1983, p. 588.

[63] Posner R. *Overcoming Law*. Cambridge: Harvard University Press, 1995, Chapter 25.

[64] A proposed Dutch statute on video monitoring of employees would prohibit the secret use of a camera to detect fraud, except by the police. This prohibition would effectively make it impermissible for a shop-keeper who suspects that an employee steals, to install a hidden camera; he would have to request that the police do so, which means that it would likely not be done, and the fraud would continue. Thierry DM. *Het gebruik van camera's ter opsporing van strafbare feiten op de werkvloer*. Bb 24 juni 2001, nr. 12, pp. 132-134.

[65] Cate FH. *Privacy In Electronic Communications*. Prepared Statement before the Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, US House of Representatives, March 26, 1998.

[66] Cate FH, Staten ME. *Putting People First: Consumer Benefits Of Information-Sharing. December 12, 2000*.

[67] In practice, employers often grant employees a limited and conditional privilege to use the employer's resources for personal purposes. But, because personal use is not a right, employers may deny this privilege if they feel the company's interest so requires.

[68] See, for instance, **Nikon France v Onos, Cass. Soc.**, Arret No. 41-6410/2/01. This case involved an engineer who had been discharged by his employer because he violated a non-competition agreement. The employer suspected that the engineer was working for competitors and examined the employee's personal computer files. The French Supreme Court held that in doing so the employer violated the employee's privacy right. Even if the employer prohibits the use of resources for personal purposes, he would not have a right to monitor for personal use.

[69] See, for instance, Black E. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Crown, 2001.

[70] For a fuller discussion see Bergkamp L. *Liability and Environment: Private and Public Law Aspects of Environmental Harm in an International Context*. Kluwer Law International: The Hague, 2001.

[71] Articles 3(2), 8(4) and (5), and 13, Data Protection Directive.

[72] One may query whether the EU data protection legislation meets the requirements imposed by the subsidiarity principle set forth in Article 5 (ex 3b) of the EC Treaty.

[73] It does so by requiring that previously anonymous and coded data are personalized. Through an over-broad definition of personal data, the Data Protection Directive imposes notice and consent requirements *vis-a-vis* unknown data subjects.

[74] A US survey conducted by Harris Interactive for the Privacy Leadership Initiative showed that: "Americans accept personal responsibility for protecting their privacy, and that they are prepared to exercise that responsibility when given the tools to do so." Privacy Leadership Initiative. *Americans Accept Responsibility for Privacy Protection*. New York, July 10, 2001.

[75] Kitchenman has noted that there is little evidence that consent requirements are being observed in Europe. Kitchenman WF. Will the Emerging EU and US Privacy Regime Derail the CRM Carousel? (September 1999). Kitchenman WF. *Update on the European Union Directive on Privacy and the Creation of Safe Harbors in the United States (April 2000).*

[76] The Dutch Data Protection Authority has stated explicitly that in 2001 it will not focus on enforcement, but on education, awareness, and norm development. Registratiekamer. Jaarverslag 2000. <www.cbpweb.nl>.

[77] Polls on consumer privacy concerns conducted by Harris & Associates in the US and Europe show virtually identical results. This suggests also that the much more stringent European laws do not increase consumer confidence, which may well be correlated to lack of enforcement.

[78] Internal Market Commissioner Bolkestein appears to be more realistic where he states that: "the Commission has the responsibility to ensure that the Data Protection Directives are *fairly applied* (emphasis added) across the union." Commission of the EC. Commission study: "Junk" email costs internet users euro 10 billion a year worldwide. Press release, 2 February 2001.

[79] The national governments, rather than the EU institutions, have jurisdiction over enforcement. However, EC law imposes limits on national enforcement discretion by requiring adequate implementation.

[80] Consumers International. Privacy@net. An international comparative study of consumer privacy on the internet (January 2001). The quotes are from a press release "Consumer Privacy Threatened on the Net," dated 25 January 2001. This study suggests also that privacy self-regulation (US) is not necessarily inferior to privacy legislation (EU).

[81] The Preamble to the Charter of Fundamental Rights adopted at the Nice Summit, which follows a Solemn Proclamation signed by all EU institutions, provides that the EU is based on "the rule of law." It seems that this charter should not be taken literally.

[82] The Commission requires effective enforcement in connection with the Safe Harbor arrangement and the model data transfer contract.

[83] US research has shown that few consumers actually read privacy notices, partly because they do not have enough time, and they also view them as too long or providing too much detail. Harris Interactive. *Consumer Privacy Attitudes and Behaviors Survey. Wave II*. July 11, 2001.

[84] This explains also why privacy demand in developing economies is much lower than in the rich West.

[85] Barron JM, Staten M. *The Value of Comprehensive Credit Reports: Lessons from the US Experience (2000).* This study found that 19% of the American public that should get credit would not have gotten it under the Australian rules. The impact is especially great on those consumers who are more vulnerable, such as consumers who are young, have short time on the job or at their residence, or lower incomes. Cf. Information Law and Commerce Institute. *The Cost of Privacy (2001).*

[86] Turner M. *The Impact of Data Restrictions on Consumers Who Buy Apparel from Catalogs and the Internet (December 2000).*

[87] Cate notes that opt-in is often tantamount to outright prohibition because of the cost of obtaining consent. Cate FH. *Privacy in Perspective*. The AEI Press, June 5, 2001.

[88] Cate FH, Staten ME. *Protecting Privacy in the New Millennium: The Fallacy of "Opt-In" (2001).*

[89] "Consent requirements often impose a considerable burden on consumers in the form of increased contacts from institutions seeking consent, services delayed or denied because of the difficulties of obtaining consent, and higher prices to cover the cost of seeking consent." Cate FH. *Privacy in Perspective.* The AEI Press, June 5, 2001.

[90] Litan RE. *Balancing Costs and Benefits of New Privacy Mandates*. AEI-Brookings Joint Center for Regulatory Studies. Working Paper 99-3, April 1999.

[91] Litan RE. *Balancing Costs and Benefits of New Privacy Mandates*. AEI-Brookings Joint Center for Regulatory Studies. Working Paper 99-3, April 1999. Cate and Staten found also that privacy regulation "imposes an especially heavy burden on small companies, which cannot afford mass market advertising and lack the customer lists of their well-established competitors." Cate FH, Staten ME. *The Value of Information-Sharing (July 28, 2000).*

[92] Cate FH, Staten ME. *The Value of Information-Sharing (July 28, 2000).*

[93] ILCI. *Summary of Tower Group Studies Related to European Systems of Opt-In (2001).*

[94] Kitchenman WF. *Will the Emerging EU and US Privacy Regime Derail the CRM Carousel (September 1999).*

[95] For a discussion of the issue of extra-territoriality of the EU regime under international law, see Bergkamp L, Dhont J. Data Protection in Europe and the Internet: An Analysis of the European Community's Privacy Legislation in the Context of the World Wide Web. 7 *EDI Law Review 2000,* p71-114.

[96] Swire PP, Litan RE. *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*. Washington DC: Brooking Institution Press, 1998.

[97] Cf. Electronic Commerce is Covered by Services Accord, WTO Report Says. 15 *International Trade Reporter 1998*, p1261.

[98] The GATS applies only if the service at issue is listed in a schedule of market access commitments.

[99] Under the Safe Harbor regime, in addition to the US Federal Trade Commission, a special commission of EU data protection commissioners supervises compliance with the regime and handles complaints. The EU model data transfer contract provides for enforcement under civil law by data subjects as third party beneficiaries.

[100] Article XVII, GATS.

[101] Article VI, GATS.

[102] Article II, GATS.

[103] Article XIV, GATS, which reads in pertinent part: "[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, (…) [members may adopt and

enforce measures that restrict trade if they are] "necessary to secure compliance with laws or regulations not inconsistent with the provisions of this Agreement, including those relating to (…) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."

[104] For an argument that the EU privacy laws do not violate the GATS, see Shaffer G. The Power of EU Collective Action: The Impact of the EU Data Privacy Regulation on US Business Practice. 5 *European Law Journal 1999*, p419-437.

[105] Abrams M. *US Research on the Cost of More Restrictive Privacy Laws*. In: FEDMA/Center for Information Policy Leadership. *Data Flows and Individual Autonomy: The Benefits of Free Flow and the Cost of Privacy*. Brussels, May 22, 2001. The US research has been financed by the Privacy Leadership Initiative, the Information Senior Executives Council at the Direct Marketing Association, the World Bank, and the financial services industry.

[106] Information Law and Commerce Institute. *The Cost of Privacy (2001).*

[107] Gauthronet S, Drouard E. Commission of the European Communities. *Unsolicited Commercial Communications and Data Protection*. ETD/99/B5-3000/E/96. January, 2001.

[108] Commission of the EC. Commission study: *"Junk" email costs internet users euro 10 billion a year worldwide*. Press release, 2 February 2001.

[109] The study's findings and conclusions suggest that it was not so much intended to gather empirical data, but rather to provide support for further EC privacy legislation. For instance, the researchers concluded that: "there is no overstating the relevance of the recent proposal for a Directive by the European Commission (12 July 2000) concerning the processing of personal data and the protection of privacy in the electronic communications sector, because of the fact that it re-affirms the central importance of consent in email marketing." If that were not enough, the researchers go on to state that they "would go so far as to say that this issue is crucial to the very survival of the Internet." Gauthronet S, Drouard E. Commission of the European Communities. *Unsolicited Commercial Communications and Data Protection. ETD/99/B5-3000/E/96*. Summary of Study Findings, January, 2001, p. 8/19. In the full report, they state that: "[a]n extremely rigorous interpretation of the opt-in concept would appear vital to the system's survival." Gauthronet S, Drouard E. o.c, p66. This, of course, has nothing to do with objective empirical research; we are dealing here with opinions, pure and simple.

[110] Gauthronet S, Drouard E. o.c., p66.

[111] They implicitly assume that all 200 marketers would run their mailing systems at full capacity every day.

[112] The study assumes that there are 300 million internet users by the end of 2001; a page down, however, the number goes up to 400 million. Gauthronet S, Drouard E. o.c., p66 and 67.

[113] Indeed, some studies suggest that people that have opted-out may be more likely to purchase than people that have opted-in.

[114] Filtering software may help to reduce spam. Also, once the full cost of email delivery can be charged to the sender (as is the case with respect to conventional mail), spamming should be reduced dramatically.

[115] To avoid confusion, there is a fundamental right to privacy, but that right has little to do with the EU data protection regime.

[116] They want workable and consistent regulatory standards in all countries of the world so that data may cross borders without problems.

[117] According to Abrams, information policy is based on balance between: data subject harm, data subject benefit, data subject autonomy, societal benefit, and corporate interest. Abrams M. US Research on the Cost of More Restrictive Privacy Laws. In: FEDMA/Center for Information Policy Leadership. Data Flows and Individual Autonomy: The Benefits of Free Flow and the Cost of Privacy. Brussels, May 22, 2001.

[118] Recital 2 and Article 1(1) of the Data Protection Directive specify that the protection of the "right to privacy" is the directive's key objective.

[119] Bennett CJ. The Political Economy of Privacy: A Review of the Literature. Paper prepared for the Center for Social and Legal Research, DOE Human Genome Project. Victoria, BC: University of Victoria, 1995.

[120] Flaherty DH. Visions of Privacy: Past, Present, and Future. January 1998.

[122] Abrams M. CRM and Managing Trust: Direct Marketing Privacy in the New Decade. In: Center for Information Policy Leadership@Hunton & Williams. Direct Marketing and Privacy: Techniques, Law and Policy, and Business Strategy. Brussels, February 7, 2001. Abrams argues that "the Holy Grail for marketers is trust, which equals value (real consumer benefit) times security times privacy (appropriate information use)."

[123] Epstein RA. Deconstructing Privacy: And Putting It Back Together Again. University of Chicago Law School, April 1999.

[124] Kitchenman WF. Update on the European Union Directive on Privacy and the Creation of Safe Harbors in the United States (April 2000). Kitchenman argues also that the EU's restrictive data protection regime has limited the Euro's role as a world reserve currency "by restricting the efficient cross-border movement of information and capital."

[125] An analogy may clarify this point. If the concern is that guns are used in terrorist attacks, and regulation is believed to be an effective response to this problem, there are several levels at which regulation could aim. The production of steel could be regulated, even though only a small portion of the steel produced is used for the manufacture of guns. A level down, one could regulate the manufacture of guns, even though most guns are used for peaceful purposes and defence. A further level down, the sale or use of guns could be regulated. Although terrorists would not have guns if steel mills would not sell to gun manufacturers, we do not regulate the manufacture and sale of steel, because regulation at that level would be seriously over-inclusive, very expensive, and probably ineffective. Why then would we want to regulate the production of data?

[126] Litan RE. Balancing Costs and Benefits of New Privacy Mandates. AEI-Brookings Joint Center for Regulatory Studies. Working Paper 99-3, April 1999.

[127] Over and over, the EU refers to a perceived "lack of consumer confidence" to justify its data protection regime for the information society. Data protection is necessary, the EU's logic goes, because the consumer's lack of confidence would otherwise undermine the development of the information society. See, for instance, European Commission Press Release. Council Definitively Adopts Directive on Protection of Personal Data. IP/95/822, July 25, 1995. However, if there is any such lack of confidence, it is probably the joint result of a lack of understanding of how data is used in business and the prolonged, government-supported campaigns against business data use. As I suggested, if there is a lack of consumer confidence, the government should help to educate consumers about business use of data.

[128] Commission of the EC. Commission study: "Junk" email costs internet users euro 10 billion a year worldwide. Press release, 2 February 2001.