Jackson Janes

The Transformation of the German-American Debate over Privacy

Prior to September 11, 2001, the transatlantic debate over data protection was essentially focused on ways to manage the increasing reach of the World Wide Web and the commerce evolving within it. With billions of dollars at stake on both sides of the ocean, access to markets was – and is – of enormous importance to industries competing with new technological innovations. Yet finding common ground in the management of data protection/privacy regulatory policies has been a continuing challenge for government and corporate leaders. This has as much to do with the legal approaches as it does with political and cultural differences in approaches to this complicated issue.

After September 11, the debate became more dramatically connected to the war against terrorism. The German and American reaction to the attacks in New York and Washington D.C. generated a new set of challenges to the protection of civil society. Germany and the United States quickly called for ways to increase security and both countries passed legislation which was designed to respond to the threats of more terrorism. In both legal frameworks, the legislation enhanced the power and tasks of the security authorities. While the United States considered itself at war after September 11, Germany did not. As a result, the U.S. invoked special powers (military tribunals, inmate-attorney discussions monitored, and expansion of surveillance powers) as it passed the USA Patriot Act. The German legislation evolved amidst more controversy within the Parliament but also focused on the need for collective security measures which also carried with them some restraints on civil liberties.

Even in the shadow of September 11, Germans and Americans will continue to argue among themselves and across the Atlantic about how to achieve the most effective balance between collective security and the rights of the individual. Yet the debate itself has now become charged with concerns about global terrorist threats as well as the challenge of protecting privacy. On both sides of the Atlantic, its evolution will be shaped by the unique combination of history and culture as well as political and legal traditions defining the national dialogues.

What is at stake?

The old and new questions about protecting privacy in the post September 11 environment remain those which center on the role of the government and regulatory powers, the globalization of trade – and now terrorism, on the free flow of information within the world wide web, and the balance between collective security and the protection of the privacy of data and enforcement of that protection.

It is a paradox of modern society that we live in an ever shrinking world in which the increasing interaction of ideas and individuals can enhance our democratic dialogues while it can also lead to confrontation and conflict. As the old adage says, familiarity can breed both understanding and contempt. Yet we have no choice in dealing with both developments emerging from an increasingly interlocked global grid.

The Economic Grid

The information sector and the multitude of services which have evolved within it during just the last two decades alone have made it the largest economic theater on the globe. The growth of the World Wide Web has defined the concept of exponential expansion. In the last ten years, popular web use has come from virtually nothing to many millions of people making use of this global tool. While half of those can be found in the United States, the rest of the world is rapidly catching up. The top four users of the web remain the U.S., Japan, the U.K. and Germany.

Originally an instrument shared only by sophisticated research specialists, the commercial dimension of the web has become the dominant mode, which is reflected in the enormous amount of business being done through it. The estimates of the revenues generated over the Internet have been growing significantly during the past decade, some projecting over a half trillion in the United States where the majority of the web traffic has been produced. However, that will grow dramatically in the future as the markets and masses around the world enter this new era of access to the web. With half the world's population currently concentrated in two countries, China and India, it is probable that both the languages and the content of the web will reflect that fact in the coming decade.

With increasingly larger numbers of people going on line to do their shopping at all levels of business, the incentive for information technology corporations to expand their capabilities and their reach to the markets is virtually unlimited. With that potential comes a corresponding need to maintain both access and protection for all those engaging in these transactions and enforcement of laws which are aimed to prevent the criminal use of the web. Yet arriving at a legal consensus on this need across so many different borders remains a continuing problem. This not only involves the question of the protection of data and personal information. There are many other unresolved issues surrounding the use of the web. The challenge of creating an acceptable taxation system for cyberspace commerce remains unresolved. Regulating e-commerce with an eye on anti-trust concerns offers another difficult issue. Arriving at a fair resolution of these matters is driven by the enormous promise of an exploding market. Yet the post September 11 environment now demands that additional issues be revisited.

The Security Grid

In the information technology environment of the twenty-first century, people who use the web leave their virtual footprints whereever they go. From credit card transactions to mail-order firms, from on-line bank accounts to airline frequent flyer programs, the users of the web are making it possible for companies to know their customers ever more intimately all over the world. The result of these developments has been increased concern about the protection of consumers in electronic commerce with particular emphasis on how information about people is collected, stored and used. If it is easier to secure data about people, how can the security of that data be guaranteed, and by whom should it be controlled or regulated? Both governments and businesses have the capability to know more about the patterns of people than ever before in history. »Big Brother« is no longer a fictional threat. The recent film Enemy of the State provides a dramatic exaggeration of the misuse of that power. Yet any company which is dealing with magazine subscriptions or retail billing maintains a large amount of details concerning the incomes, lifestyles and habits of millions of people all over the world.

On the one hand, such control of information can be of beneficial use if one is trying to improve the efficiency of serving either citizen or consumer by having a better picture of the needs and demands of both within the political process or the market. The ability of a democracy to implement self-correction requires knowing more about the issues and developments in question. This is why we have a census every ten years in the United States, which does more than count heads. It can also address questions about the impact and efficiency of its education, health care and social welfare. Businesses are forever trying to figure out what the consumer wants so that they can introduce new products and services and also deliver operational efficiency at lower costs. Medical information needs to be transferred among doctors, hospitals, insurers, pharmacies and even research centers, sometimes in an expedient manner if there is an outbreak of disease. Democratic governments need to have constant feedback from the citizens in order to maintain their own support and legitimacy.

On the other hand, there is ample room for misuse of this information and there is always a need to be alert to those dangers in an open society. For example, the unregulated transfer of health data among hospitals, pharmaceutical industries or insurance companies without proper controls can be detrimental for individuals and ethnic, racial or sexual groups. The vicious circle of organized crime, terrorist strategies to exploit the open political and social structures of democracies, and the wide presence of political corruption can all combine to undermine the basis of achieving a healthy balance between civil security and stability and individual rights.

Protecting Privacy: beyond September 11

During the past ten years, the European Union and the United States – the two main arenas in which electronic commerce and the use of data collection is most advanced – have been debating the policy responses surrounding these issues within their own respective frameworks as well as across the Atlantic. Those debates reflect different attitudes toward privacy, the degree to which the citizens of a given country show trust and confidence in the governments and their corporate leaders. And these differences have made it difficult to achieve a transatlantic consensus.

When it was implemented in 1998, The Privacy Directive of the EU prompted many in the United States to accuse the data protection policy of limiting the free flow of information and infringing on what some Americans would refer to as constitutional free speech. With regard to the Internet, the prevailing American attitude is to not attempt to control it. Making such an attempt, it is argued, would be no more successful than trying to control the content of the global telephone grid. The American approach has been to emphasize the self-regulatory capabilities and responsibilities of the corporate sector with regard to how they handle data and privacy safeguards. However, there remains a set of questions which still shape the transatlantic debate: what form of dispute mechanisms can be implemented to resolve conflicts, who judges those disputes, and what resolutions can be proposed.

The European Union – and Germany was a primary leader in this context – has been rigorous in enforcing its Privacy Directive. While negotiating with the United States over how the adequacy of data protection can be guaranteed, there has been consistent emphasis on the fundamental right of Europeans to protect privacy and that the enforcement was the responsibility of the governments and their respective agencies charged with implementing it.

Yet after September 11, and within the German legislation which was implemented at the beginning of 2002, there was recognition that to deal with the threat of terrorism, some leeway was needed in gaining access to data. Now the security agencies have the right to ask postal services, telecommunications providers and financial institutions for information on specific individuals. As of this writing, The EU is revising its regulatory policies on data retention for the purposes of enhancing national security. The search for a balance between the needs of law enforcement and the requirement of the right of privacy continues. The fact that information of any sort remains critical to the prevention of the terrorist attacks experienced in September, 2001, will provide evidence to some that the government needs to access a broad range of data to track down those who threaten us. At the same time, the increasing recognition that so much data is available argues for others that we need to be as vigilant about the need to protect personal privacy. There can be no zero sum game played with the needs of security and freedom.