THE EU'S DATA PROTECTION DIRECTIVE: HEADED FOR THE ROCKS?

James E. Weber, St. Cloud State University, jweber@stcloudstate.edu
Richard Paulson, St. Cloud State University, rapaulson@stcloudstate.edu

ABSTRACT

The European Commission's Directive on Data Protection (95/46/EC) has the potential to have enormous impact on US firms' business practices if they deal with the personally identifiable information of EU subjects. The Directive has extraterritorial effect; it is intended to be enforced on businesses outside the EU. US firms are not necessarily accustomed to the exercise of extraterritorial authority through the DDP, and they have to deal with issues around the Safe Harbor and Contractual Clause methods of compliance. Furthermore, there are questions of whether organizations will actually comply with the DDP. For US firms it would be useful to have an understanding of the historical underpinnings of the DDP, their options for, and the costs and implications of, compliance, and the impact of potential changes in the DDP. This paper discusses the roots of the Directive, its provisions, options for compliance, the difficulties US firms will find in complying with the directive and its implications for US firms.

Keywords: Directive on Data Protection, 95/46/EC, privacy, data protection

INTRODUCTION

The European Commission's Directive on Data Protection (95/46/EC) was originally drafted in 1995 and formally went into effect in October, 1998, although a moratorium on enforcement was extended until July, 2001 (2, 3, 5, 21). For most non-EC firms, doing business within the EC will require extensive changes regarding data handling. Complying with the Data Protection Directive's (DDP, or Directive) requires that non-EU entities receiving personal data from the EU provide "adequate" data privacy protection. At a minimum, this requirement will result in fundamental changes in the way US businesses handle data, online transactions, and even internal intranets (1, 4, 11, 23). The heart of the issue lies in historic differences between European and US concepts of privacy (1), but is much more extensive. US firms are not necessarily accustomed to the exercise of extraterritorial authority through the DDP (4), have to deal with issues around Safe Harbor and Contractual Clause methods of compliance (8, 13, 16) and there are questions of whether the DDP will actually be complied with (5, 20). For US firms weighing their options, an understanding of the historical underpinnings of the DDP, options for compliance, costs and implications of compliance, and the potential for changes in the DDP would be useful. This paper deals with these issues in a conceptual manner useful for the working manager or IS specialist, leaving legal assessments for other venues.

OVERVIEW

Europeans evaluate the tradeoffs of privacy protection versus public access rights differently than Americans. In Europe, personal information is treated in much the same way intellectual property is treated in the US. That is, personal information is treated as a personally owned

property right or even a fundamental human right (4). In fact, personal data privacy is a constitutional right in many European countries. Data privacy rights were strengthened after repressive regimes such as the Third Reich used personal information in a way that fueled the later development of modern data privacy laws throughout the 70's, 80's and 90's by many European states (4). As time went on, the states that would eventually comprise the EU developed conflicting statutes, leading to extreme occasions where data transfers between EU states were blocked to uphold one of the state's statutes (4). By 1990, differences in law between member states became serious enough for an EU directive to be proposed.

The DDP creates a free zone of information flow within the EU, and establishes rules ensuring personal data is only transferred to entities outside the EU that provide adequate protection for those data (4). The extraterritorial effect of the directive is to create problems for US and other nations' companies that deal with personal data from EU nations, making these firms subject to the adequate protection provisions of the Directive. Within the EU, member states are responsible for actual implementation of the Directive, through Data Protection Agencies that were to be established in each country (15). Although personal data, defined as any information relating to an identified or identifiable individual, is protected, the Directive requires greater protection of sensitive information. Sensitive information reveals racial or ethnic origin, political leanings, beliefs of a religious or philosophical nature, union membership, health or sex life or orientation (4). Data may not be used other than its original purpose, and must be destroyed when no longer necessary for the original purpose. Exceptions exist if the data subject (person about whom data is collected and maintained) gives unambiguous consent, if the data is necessary for fulfilling a contract with the data subject, or if processing the data is a legal requirement (4).

The data subject is accorded certain rights by the DDP. The data subject has a right to: 1) know when a controller of data collects or acquires data on the subject; 2) access the data at reasonable intervals without excessive delay; and 3) withhold consent for the collection and use of personal data. If giving consent, the consent must be unambiguous and explicit (4).

At least three methods are available for non-EU firms who need to exchange personal data with the EU. A firm that does business only in an approved state (e.g. Switzerland or Hungary) already complies with the Directive (2). This option is appropriate for only a few non-EU firms. Reasonable alternatives include the use of approved Contractual Clauses, or, if in the US, firms may certify that they comply with Safe Harbor principles jointly developed in negotiations between the EU and US (15, 16, 21). Both Contractual Clauses and Safe Harbor compliance create certain problems for US firms, and it is an open question as to how these problems will be resolved (5, 15).

DISCUSSION

US firms have a number of problems providing "adequate" protection of personal data. The basic principles on which the Directive are based are:

- Purpose limitation – data collected for a specific purpose should be used only for that purpose.
- Data Quality – data should be accurate, up to date, and not excessive.

- Transparency – individuals should be informed of the use their data will be put to.
- Security – technical and organizational security measures must be taken to secure personal data.
- Right to Access – data subjects have a reasonable right to see and correct personal data.
- Restrictions on transfer – data may only be transferred to entities also holding to these same principles.

Furthermore, "Sensitive" data, information on racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health, criminal proceedings or convictions, or sex life are accorded special protection. Handling of these data requires explicit and unambiguous consent of the data subject (23).

Since the DDP was originally drafted, the information technology arena has undergone significant expansion and advancement. For example, the environment fostered by the rapid increase in Internet based activities raises issues that might not have been foreseen in 1995, when Directive language was being finalized and the Internet was in its early stages of commercialization. The end-result is a law that does not fully recognize the competitive environment in which US businesses find themselves. This conflict between the different rates at which technological advances are implemented and the legal and regulatory environment changes is not new, but that conflict normally occurs with laws long in existence. Regardless, the DDP creates potential problems with profound implications for profitability and business practices because of this conflict.

Some types of electronic data exchanges raise questions about the possibility of certain compliance exceptions. For instance, different data protection requirements may be appropriate for B2B versus B2C transactions, given the nature of personally identifiable information exchanged in corporate, rather than individual trade. In other cases, stringent regulations may already be in place within an industry. The US financial services sector is an example. Although the EU has indicated that current US regulation in this sector is still inadequate, the possibility exists that some sectors may already be in substantial compliance and may deserve exception (18).

A basic problem with the Directive from the business perspective is that it seems to assume that a company can document every time a data subject's data is seen by a non-company employee, that a firm can effectively change a data subject's data throughout the company, and that the information system used by a firm is capable of differentiating access and storage of personal data based on data subject preferences (5). This is unlikely to be the case in US firms with preexisting information systems. A more typical corporate information system may store data in disparate legacy systems in multiple locations with no central method for reconciling the databases. Typically systems that validate the identity of people accessing their own data are only partially implemented. Audits to verify compliance are costly and time consuming. And making personal data accessible to the data subject requires linking databases or making databases separately accessible, a logistical, security and design nightmare (6). Complicating the problem is the existence of personal data not normally considered privileged in the US on company intranets, e-mail or websites that fail to meet minimum Directive standards (23).

The inherent conflict between making information simultaneously more accessible and secure is not simply resolved. Microsoft recently spent $500,000 solely for an audit of their information systems' compliance with the Directive (6). Making changes in systems found not to be in compliance would be much more costly than a simple audit. But conflicts go deeper than accessibility versus security issues. US law at both the Federal and State level often requires employers to acquire, process and store employee data that would be considered sensitive under the DDP, creating a potential conflict if the data subject were reluctant to give unambiguous permission (4). Companies are uncertain of the resolution of these seemingly mutually exclusive requirements. In addition, organizations need to give attention to how future strategic plans they may have for customer data whose use may not be limited by the DDP will be altered (5). In sum, the DDP fundamentally changes the way many US businesses function, and in possibly costly ways. For example, Household International Inc. does 95% of its business within the US. The remaining 5% of the business conducted with EU customers has resulted in Household's maintenance of separate data centers, a not inconsiderable investment (11). Other companies may find that a complete redesign of their information architecture is necessary.

But organizations also have problems unique to both of the reasonable options available for compliance with the DDP. The Contractual Clauses developed by the EU have been characterized by US legal experts as being vaguely worded, leading to speculation that the clauses may create legal problems for US firms using them. Under the clauses, US firms might be required to defend lawsuits in foreign courts. This would result in businesses being subject to the supervisory authority of courts in the country from which the data is being transferred. This is not a prospect that US businesses are likely to welcome (14). Overall, problems with the clauses are severe enough that the US government has expressed reservations about them (15). However, there are certain industries for which the Safe Harbor option is unavailable, thus making the contractual clause a likely alternative for compliance in the transfer of personal data (14).

The Safe Harbor option presents different problems for US organizations. Safe Harbor principles vary slightly from the principles on which the Data Protection Directive is based which were presented earlier. Safe Harbor principles also include:

- Enforcement – readily available independent recourse methods, procedures for verifying commitments the company has made, and an obligation to remedy problems arising from discrepancies from the principles (13, 22).

A US company either 1) joins an industry-based privacy program that includes recognized enforcement mechanisms; 2) develops their own qualifying principles; or 3) self-certifies to the Department of Commerce that it meets and adheres to Safe Harbor Principles (4), and is then listed on a web-site of complying organizations (12). Although benefits of Safe Harbor are substantial (e.g. automatic acceptance from all 15 EU countries, claims brought by EU citizens will typically be heard in US courts) there are also difficulties for US firms (4).

For example, the intent of the DDP is clearly at odds with post-9/11 practices of many US companies, who are cooperating closely with Federal investigations (10), and is possibly at odds with provisions of the Patriot Act. Under the Patriot act, many forms of electronic communications, including e-mails, voice mails, transactions and account records must be disclosed to the US government under certain circumstances (24). Thus, many US-based

companies are being asked to share information in a way that would seem contrary to Directive precepts and they seem to be complying. What happens if US law makes it impossible for US businesses to comply?

But the primary difficulty with Safe Harbor lies in the nature of compliance with Safe Harbor Principles themselves. The typical way in which US companies handle data such as information on resumes, records on employee training, grievances and disciplinary matters does not meet Safe Harbor standards. Taken in whole, the actual problem is that compliance with the standards is difficult and costly, but not optional for many US companies doing business with EU companies and customers. Furthermore, compliance requires drastic changes in existing business practices, including implementation of new policies and changes in existing information systems. Add in the competitive disadvantages complying companies may face with respect to non-complying companies and problems small organizations with few resources may face in complying with the Directive, and the scope of problems that Safe Harbor brings along with it becomes evident.

But many companies are choosing to wait and see how the DDP and Safe Harbor work in practice (5, 17). In fact, as of May 12, 2003, only 328 companies were listed on the US Department of Commerce's Safe Harbor website as currently complying with Safe Harbor Principles (12). There are a number of reasons for the wait and see approach. First, although the EU has previously denied US proposals from the financial services industry to modify the Directive (7), currently a group of influential companies have formed the Global Privacy Alliance whose goal is to protest the DDP and affect change. This group includes IBM, Oracle, and VeriSign, and the Alliance maintains that the Directive makes doing business more time consuming, expensive and burdensome for US companies to store data on EU citizens (20). Although this approach may seem doomed to failure (why would the EU acquiesce to pressure from firms outside the EU), there is some evidence that the EU is currently considering changes (19).

A second reason US companies may be waiting is uncertainty about enforcement of the Directive. As of September, 2002, Ireland and Luxembourg had still not implemented the Directive (20). This lack of compliance by member states, the EU's history with regard to directives, and the potential for differences in how member states interpret the Directive can give US companies reasonable doubt as to how and whether the Directive will actually be enforced (5, 9). Finally, when US companies look at how the Directive is currently being enforced, compliance seems most often to be secured through discussion and negotiation rather than sanctions (5). US companies may be willing to risk noncompliance when the only result is a (protracted) negotiation.

CONCLUSION AND RECOMMENDATIONS

The DDP has presented many US companies with a serious challenge. It is possible that the Directive may even spark demands by US citizens for privacy coverage equal to the treatment their employers are giving EU citizens (17). Certainly complying with the Directive would be costly for US companies. But a close examination of the principles on which it is based and Safe Harbor Principles reveals that at the heart of the new requirements is basically good data

management (4). As US companies revise and upgrade their information architectures, the security and accountability now required by the EU is something that should be incorporated into systems as a matter of good practice. As US companies make decisions about compliance and architecture modifications, certain common-sense recommendations should be followed:

- Conduct a compliance audit of your existing system that includes tracking current data sets, the information they contain, and authorization for accessing the data. This audit needs to include current intranets, websites and e-mail.
- Determine which EU trading partners you deal with and find out all you can about their specific laws, penalties, and enforcement policies.
- Involve EU legal experts familiar with current practices in countries where you do business.
- Conduct a risk assessment of your exposure.
- Consider your approach to retaining automatic records, logs and copies of e-mail. Not only might they contain personal information, but they also provide an access trail to that personal information.
- Decide how to best comply with DDP principles.
- Look for ways that compliance can help your organization rather than considering compliance solely a burden. For instance, compliance will result in better data practices and might lead to greater organizational efficiency and a more desirable work place.
- Be ready for change.

Organizations following these recommendations will be more ready to adapt and adopt Directive principles and more likely to be ready to change their information systems and handling of data in ways that represent good data practices.

REFERENCES

1. Brostoff, S. (1999). U.S. insurance groups hold their breath as global privacy talks move forward. *National Underwriter/Property & Casualty Risk & Benefits,* 103(27), 10-14.
2. Data protection: Commission approves standard contractual clauses for data transfers to non-EU countries. (2001). *Europa.* Retrieved October 7, 2002 from the World Wide Web: http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2.htm.
3. Data transfer across borders. (2001). *Computer Weekly,* Feb., 52.
4. George, B.C, Lynch, P & Marsnik, S.J. (2001). U.S. multinational employers: Navigating through the "safe harbor" principles to comply with the EU data privacy directive. *American Business Law Journal,* 38(4), 735-783.
5. Harvey, J.A & Verska, K.A. (2001). *The Computer and Internet Lawyer,* 18(4), 17-20.
6. Kemp, T. (2001). Privacy rules across the pond. *InternetWeek,* 869, 1-2.
7. McAuliffe, W. (2001). EU rejects US opposition to privacy directive. *ZDNET.* Retrieved September 30 from the World Wide Web: http://news.zdnet.co.uk/story/0,,t269-s2086070,00.html.
8. McAuliffe, W. (2002). EU creates loophole for personal data transfers. *ZDNET.* Retrieved September 30 from the World Wide Web: http://news.zdnet.co.uk/story/0,,t269-s2103096,00.html
9. Meller, P. (2002). Europe proposes dual plan on disputes in commerce. *New York Times.* Retrieved September 16, 2002 from the World Wide Web: http://www.nytimes.com/2002/05/04/business/worldbusiness/04EURO.html.

10. Olsen, S. (2001). Companies rethink customer data privacy. *ZDNET*. Retrieved September 30 from the World Wide Web: http://news.zdnet.co.uk/story/0,,t269-s2096450,00.html.
11. Rendleman, J. (2001). Europe's eye on privacy. *InformationWeek,* 843, 53-55.
12. Safe Harbor List. (2002). *U.S. Department of Commerce.* Retrieved October 7, 2002 from the World Wide Web: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe%20harbor%list!OpenDocument&start233.
13. Safe Harbor Overview. (2001). *U.S. Department of Commerce.* Retrieved September 16, 2002 from the World Wide Web: http://www.export.gov/safeharbor/sh_overview.html.
14. Shimizu, K. (2002). EU data protection directive model contract: An alternative method to transfer personal data from Europe to the United States. Retrieved November 11, 2002 from the World Wide Web: http://www.kilpatrickstockton.com/site/print/detail?Article_Id=1093.
15. Spies, A. & Bookwalter, T. (2001). EU-U.S. data flow: An unstable connection. *Business Communications Review,* 31(12), 44-46.
16. Standard contractual clauses for the transfer of personal data to third countries – frequently asked questions. (2001). *Europa.* Retrieved October 7, 2002 from the World Wide Web: http://europa.eu.int/comm/internal_market/en/dataprot/news/clauses2faq.htm.
17. Thibodeau, P. (2000). Will Americans envy strong EU protections? *Computerworld,* 45, 1-2.
18. United States Council for International Business. (2002). USCIB comments for the review of the E.U. General Data Protection Directive (95/46/EC). Retrieved December 30, 2002 from the World Wide Web: http://europa.eu.int/comm/internal_market/en/dataprot/lawreport/papers/uscib_en.pdf.
19. Wearden, G. (2002a). Civil liberties group warns of EU surveillance proposal. *ZDNET.* Retrieved September 30 from the World Wide Web: http://news.zdnet.co.uk/story/0,,t269-s2109921,00.html.
20. Wearden, G. (2002b). U.S. tech protests EU privacy laws. *ZDNET*. Retrieved September 30 from the World Wide Web: http://zdnet.com.com/2100-1106-960134.html.
21. Welcome to the Safe Harbor. (2001). *U.S. Department of Commerce.* Retrieved October 7, 2002 from the World Wide Web: http://www.export.gov/safeharbor/index.html.
22. White, M. (2000). The impact of data protection legislation on intranets. *Ecocontent*, 23(4), 45-47.
23. White, M. (2002). Data protection issues for intranet managers. *Intranet Focus LTD.* Retrieved September 16, 2002 from the World Wide Web: http://www.intranetfocus.com/intranets/dataprotegtion.html.
24. Wiley, Rein and Fielding, LLP. (2001). The search and seizure of electronic information: The law before and after the USA Patriot Act. Retrieved May 12, 2003 from the World Wide Web: http://www.ala.org/Content/NavigationMenu/Our_Association/Offices/ALA_Washington/Issues2/Civil_Liberties,_Intellectual_Freedom,_Privacy/The_USA_Patriot_Act_and_Libraries/matrix.pdf .