e-Discovery and legal frameworks governing Privacy and Data Protection in European countries

Implications

ORLA LYNSKEY, NEIL ROBINSON, MICHAEL GREENBERG

TR-929-FTI

November 2010

Prepared for FTI Consulting Inc

EUROPE

Preface

RAND Europe was commissioned by FTI Consulting to conduct a short study to explore the conflict between the European legal framework for privacy and data protection and the sometimes competing requirements of e-disclosure imposed on US firms with European subsidiaries by legislation such as the US Foreign Corrupt Practices Act (FCPA).

RAND Europe conducted desk research and interviews with experts in each of the selected countries (France, Germany, Spain, Switzerland and the United Kingdom).[1] A separate Appendix containing further information is available upon request from FTI Consulting.[2]

This report was prepared by Neil Robinson & Orla Lynskey of RAND Europe and Michael Greenberg of RAND's Centre for Ethics and Corporate Governance in the Institute for Civil Justice.

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy and decision making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multidisciplinary analysis.

The authors would like to thank Hans Graux and Matt Bassford for their helpful comments during the preparation of this report.

For more information about RAND Europe or this document, please contact Neil Robinson:

RAND Europe (Brussels)
37, Sq de Meeus,
Brussels
B-1000
Belgium
Neil_Robinson@rand.org

[1] Noting that Switzerland is not a member of the European Union and therefore not subject to the European legal framework regarding privacy and data protection

[2] Readers interested in obtaining the Confidential Appendix may contact Joe Looby, Senior Managing Director FTI Consulting New York joe.looby@fticonsulting.com

Contents

Summary

Rationale

RAND Europe was commissioned by FTI Consulting to prepare a short paper exploring the conflict between the European legal framework for privacy and data protection and the sometimes competing requirements of electronic discovery ('e-discovery') imposed on US firms with European subsidiaries by legislation such as the US Foreign Corrupt Practices Act (FCPA).

Background

The competing and sometimes conflicting requirements of pre-trial discovery and legal obligations regarding the protection of personal data represent a unique and pressing public policy challenge. As the trends of globalisation and electronic storage of data continue and more and more firms are asked to produce materials (often stored electronically) there is an ever greater impact on compliance with different regulatory architectures governing personal data. Given volumes of commerce between the United States and Europe, this problem is particularly pertinent: especially so when the specific requirements of the legal framework governing the protection of personal data of European citizens are taken into account. This study comes at a critical junction in EU policy-making, when there is increased political appetite for improving the legal protection of personal data for European citizens.

The European legal framework governing privacy and data protection

In Europe different legal frameworks currently apply to privacy and data protection in different contexts, whether in the context of private international law within and between commercial entities, or concerning the use of personal data in the pursuit of police and criminal justice activities.[3] Although the applicability of these legal frameworks is currently under review (given the relatively recent entry into force of the TFEU), the divergence in

[3] For a detailed review of the strengths and weaknesses of EU Data Protection Directive 95/46/EC see Robinson, N., Valeri L. et al *Review of the Strengths and Weaknesses of the European Data Protection Directive* RAND; Santa Monica 2009 http://www.rand.org/pubs/technical_reports/TR710/

how these different uses of personal data has evolved historically into being covered by three legal frameworks:

- Directive 95/46/EC and e-Privacy Directive 2002/58 regarding the processing of personal data in the context of the Internal Market (i.e. 'First Pillar')
- Regulation 45/2001/EC in respect of the uses of personal data relating to the Common Foreign and Security Policy (formerly second pillar)
- Framework Decision 2008/977/JHA governing personal data processed in the domain of police and criminal justice co-operation (Formerly the 'Third Pillar' of police and criminal justice co-operation).

The Treaty of Lisbon represents a fundamental shift in how data protection is addressed throughout the Union. Specifically, the removal of the pillar structure of policy-making, combined with the general applicability of Art 16 TFEU means that all areas of EU law could be now covered, including processing in the former First Pillar (Internal Market), Second Pillar (Common Foreign and Security Policy) and Third Pillar (Police and Judicial Co-operation).[4]

The requirements of e-discovery

An important challenge posed to the EU legal framework for privacy and data protection is "e-discovery," or the demand for production of electronic records in connection with civil litigation and a range of other legal and corporate proceedings. In the simplest case, e-discovery involves a plaintiff demand for documents in connection with ongoing litigation, pursuant to formal judicial rules of procedure, which a defendant is obligated to comply with under those rules. In common law jurisdictions, the burdens of e-discovery in a civil case involving corporations can be enormous –literally millions of pages of corporate electronic documents and records can sometimes be demanded by a plaintiff for disclosure, in the context of a specific case. Simply identifying, organising, and producing the relevant documents can represent a Herculean task. Particularly in the U.S., e-discovery has become a big business, as technology vendors have entered the market to help corporations manage demands for large-scale document production in litigation.

E-discovery in situations involving both EU and U.S. actors becomes even more complicated and burdensome. Litigation-based requests for document production under the procedural laws of one country (e.g., the U.S.) can easily run into conflict with the data protection requirements of another (e.g., national transpositions of the EU Data Protection Directive 95/46/EC). Consider hypothetical U.S. litigation that involves a multinational corporate actor based partly in Europe, with a large pool of corporate records tied to individual employees (e.g., internal e-mails), the latter arguably protected under EU privacy law. The corporation in this scenario is targeted as a defendant in a U.S. law suit, and demands are made for the production of corporate records and internal e-mails. In addition to all of the logistical burdens pertaining to e-discovery, the corporation in this instance will also need to worry about the application of EU privacy law to its records. In

[4] Hijmans, H, and Scirocco, A; *Shortcomings in EU Data Protection in the Third and Second Pillars: Can Lisbon be expected to help?* 2009 Common Market Law Review (46) 1485-1525 London

the worst case, the corporation might find itself facing a legal obligation to disclose records in a U.S. court, while simultaneously facing a legal obligation in one or more EU states not to disclose those records, per EU privacy law.

Analysis

Evidence from an analysis of national approaches serves to illustrate the difficulties of international transfers of data for e-discovery purposes. Despite the fact that all EU states are party to the 1970 Hague Evidence Convention (Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters or hereafter Hague Convention) and have transposed the EU Data Protection Directive into national law, stark differences in the legal regime applicable to international transfers for the purposes of e-discovery exist between EU Member States. These differences stem only in part from the fact that EU states have divergent common and civil law legal traditions. Of relevance when considering transfers of evidence for civil proceedings is whether the State concerned has invoked the Article 23 exception to the Hague Convention (which even the United Kingdom, a common law country, has invoked). Transfers of evidence for criminal proceedings are governed by bilateral agreements which differ from state to state. Moreover, some states, for instance France, have enacted 'blocking statutes' entailing harsh criminal sanctions for those who transfer certain types of information abroad. The data protection legislation in place also needs to be complied with. Here, although there are some minor differences between transposition in various countries, the overall legal framework remains similar; transfer to the United States is possible without consent once an 'adequate' level of protection is guaranteed whether that be by resorting to Standard Contractual Clauses, falling with the scope of a Safe Harbor agreement or by respecting Binding Corporate Rules.

Way forward

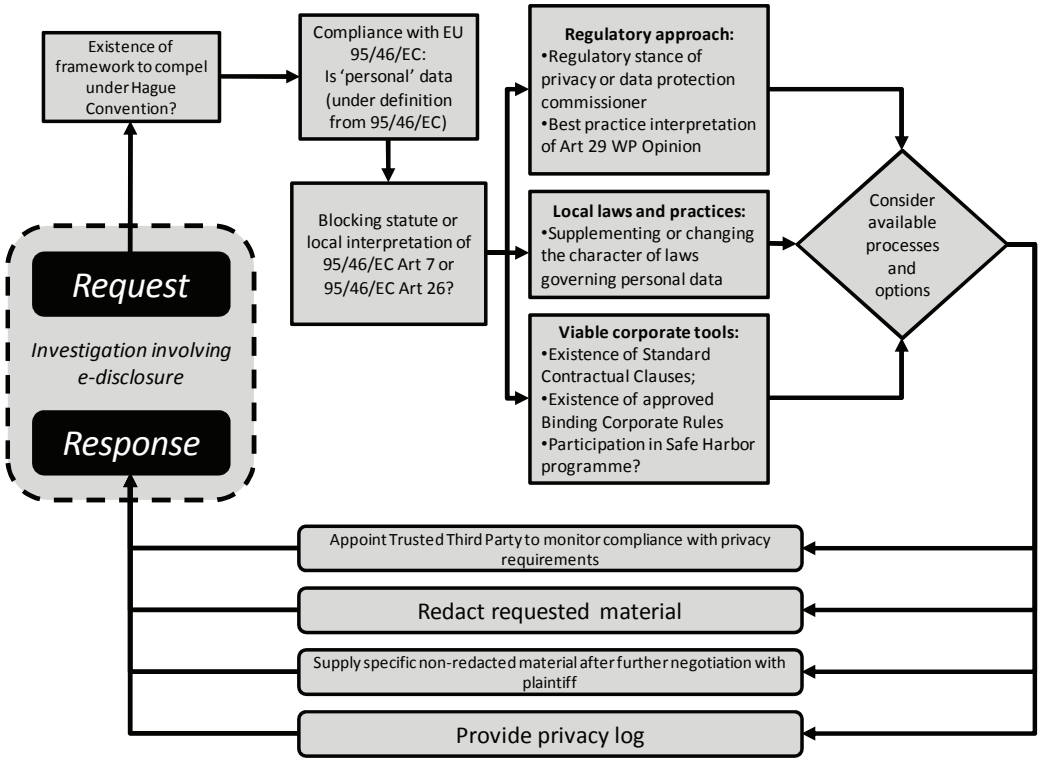
Based on our analysis and noting guidance from the Article 29 Working Party issued in 2009 on the use of personal data in pre-trial discovery and from our review of the situation in different countries, we propose our own suggested approach below:

- First – determine whether there is any potential framework to compel co-operation with US discovery rules. For example under the Hague Convention or other bilateral agreements (depending on the civil or criminal nature of the request).
- Second – consider whether any protected data is likely to be involved – an estimation of the types and character of the data (whether it falls within the scope of EU data protection rules as it relates to an 'identifiable person'; whether the data concerned is 'sensitive data'). If the data concerned fall within the scope of the European Data Protection Directive (Directive 95/96/EC), as transposed into national law, verify whether the data transfer is permitted by the data protection regime. For instance, Article 7 of the Data Protection Directive enumerates the criterion according to which data processing is deemed legitimate. Article 26 sets out derogations to the general rules for transfer of data to third countries.

- Third -consider whether a blocking statute or other local legal restriction or interpretation on data disclosure exists – stemming from relevant Applicable National Law transposing Articles of 95/46/EC e.g. under Art 7(f) and Art 26(1)(d)
    - Whether the company has approved Standard Contractual Clauses (SCC), Binding Corporate Rules (BCRs), or participates in the Safe Harbor scheme which would cover the onward transfer of personal data;
    - Whether there are any unique local regulations or laws supplementing or changing the character of legislation governing the processing and transfer of personal data;
    - Similarly, whether the application of the law in practice differs in any respect given the regulatory stance and strategic approach of the Data Protection or Privacy Commissioner in the interpretation of this guidance (as has been shown elsewhere, EU Member States may differ in how they interpret the official guidance as presented by the Article 29 Working Party).
- Finally, upon answering the above, investigate processes and options that respect the fundamental rights of European citizens under Article 16 of the TFEU and Article 8 of the Charter of Fundamental Rights of the European Union whilst serving the purposes of pre-trial discovery. Such options might include the following:
    - Redacting or anonymising all documents in country, prior to the disclosure and onward transfer to the United States
    - Provision of a Privacy Log which details the information protected from disclosure in order for plaintiffs to determine more clearly the necessity of the disclosure of such data and possibilities for amendment of the Protective Order in order to safeguard defendants from liability for the production of this data
    - For those deemed of specific interest by the litigants in the pre-trial discovery process in the United States the European based subsidiary supply them in non-redacted form
    - Assigning a suitably qualified and appropriate Trusted Third Party to support the adherence of the processing to appropriate level of adequacy of protection in line with the European legal framework for privacy and data protection.

This is illustrated below in Figure 1.

Figure 1. Suggested e-Disclosure workflow



Source: RAND Europe

Methodology

To undertake this research, RAND Europe conducted desk research and interviews with 'in-country' legal experts in each of the selected countries (France, Germany, Spain, Switzerland and the United Kingdom). The countries were selected on a pragmatic basis after consultation with FTI Consulting as a representative selection of jurisdictions likely to be of interest in respect of the research question.

Structure of report

Chapter 1 provides an introduction that highlights the importance of this complex issue. Chapter 2 presents some overarching background detail on the European legal framework for privacy and data protection, noting: the former European 'pillar structure'; relevant legal instruments and the differences in conceptualisation of privacy between common law and civil code countries. Chapter 3 presents the requirements of e-discovery, using the US Foreign Corrupt Practices Act (FCPA) as an example of legislation imposing such requirements on US firms. Chapter 4 summarises the evidence gathered from interviewees at the national level. Chapter 5 presents our conclusions and ways forward, noting by example guidelines produced by both the Article 29 Working Party of EU regulators and the US based Sedona Conference community of legal practitioners.

CHAPTER 1 Introduction

The competing and sometimes conflicting requirements placed on multinational organisations to meet their obligations under US pre-trial discovery rules whilst protecting the personal data of their employees and customers represent a somewhat complex public policy challenge. Trends of globalisation and electronic storage of data continue and more and more firms are asked to produce materials, often stored electronically. There is thus ever greater impact on compliance with different regulatory architectures governing personal data. Given the volumes of commerce between the United States and Europe, this problem is particularly pertinent: especially so when the specific requirements of the legal framework governing the protection of personal data of European citizens are taken into account. Much of the material requested to be disclosed will frequently contain information classified under the European legal framework as personal data (such as that relating to employees or third parties such as customers). This conflict of laws issue has been termed by the Sedona Conference as a 'Catch-22' situation where the need to:

> *"...gather relevant information from foreign jurisdictions 'squarely' competes with blocking statutes and data privacy regulations that prohibit or restrict such discovery."*

Similarly, the Article 29 Working Party published its Opinion on pre-trial discovery and noted that:

> *"There is a tension between the disclosure obligations under US litigation or regulatory rules and the application of the data protection requirements of the EU."*

Given the acceptance of the importance and existence of this conflict of laws issue with its inherent tensions and contradictions, it seems appropriate to try to further explore and understand the specific detail of these contradictions. In the following chapters we aim to answer these and other relevant questions relating to the shape and characteristics of the tension inherent in this challenge.

CHAPTER 2

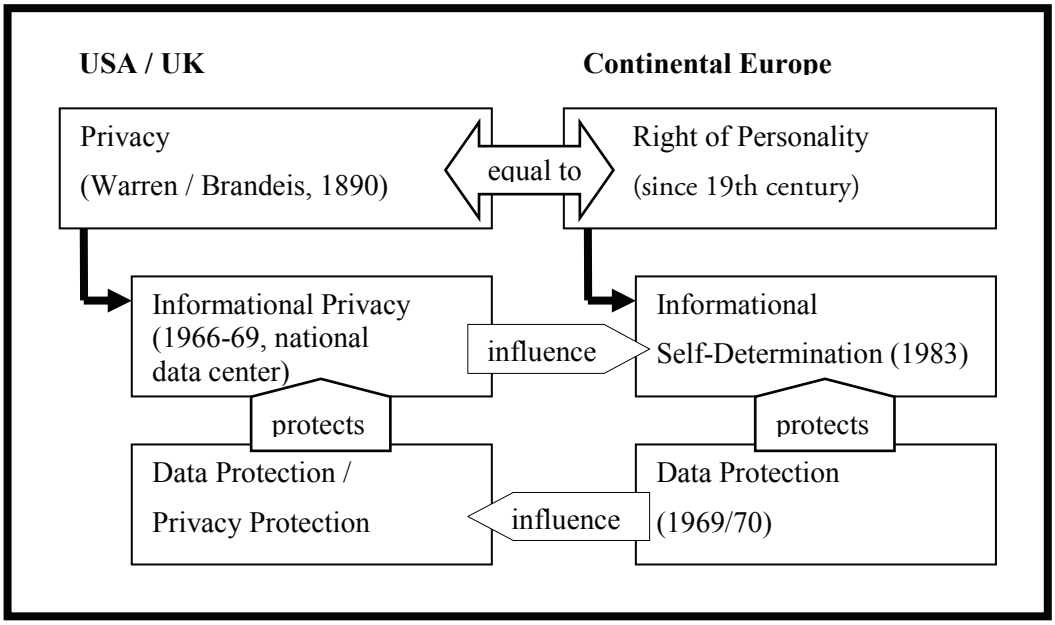
The European regulatory architecture governing privacy and data protection

Much of the current body of EU law concerning privacy (e.g. the Data Protection Directive 95/46/EC) focuses specifically on the protection of personal data ("data protection").

Europe has different legal instruments covering data protection and privacy across a range of related policy domains, from the use of personal information by commercial entities (in the Internal Market), to the intrusions into 'the right to be let alone' that are sometimes necessary in order to address important transnational threats, such as international terrorism and organised crime (in the context of the co-operation between law enforcement authorities).

This regime reflects long established differences in how various Member States have conceptualised and enacted basic privacy rights and responsibilities, depending on their common law/civil law approaches. Figure 2 explains.

Figure 2: Common law vs. Continental Law traditions of privacy



Source: ITM - University of Munster

Article 286 EC and Article 8 of the Charter of Fundamental Rights of the Union both contain references to the right to data protection which anchor many, if not all, of the relevant legal norms in Europe. Article 16 of the Treaty of the Functioning of the European Union (TFEU) replaces the Treaty Provision on Data Protection in the First Pillar, describing the right to data protection, namely that:

"Everyone has the right to the protection of personal data concerning him or her"

This represents a fundamental shift in how data protection is addressed throughout the Union. Specifically, the removal of the pillar structure of policy-making, combined with the general applicability of Art 16 TFEU means that all areas of EU law are now covered, including processing in the former Second Pillar (Common Foreign and Security Policy) and Third Pillar (Police and Judicial Co-operation).[5]

[5] The pillar structure has its roots in historical context of EU policy making and as a way to respect the sovereignty of individual member states in respect of markedly differing approaches to criminal justice, interior affairs and policing. This is known as the subsidiarity principle.

CHAPTER 3 The requirements of e-discovery

An important challenge posed to the EU framework for data protection and personal privacy is "e-discovery," or the demand for production of electronic records in connection with civil litigation and a range of other legal and corporate proceedings. In the simplest case, e-discovery involves a plaintiff demand for documents in connection with ongoing litigation, pursuant to formal judicial rules of procedure, which a defendant is obligated to comply with under those rules. In common law jurisdictions, the burdens of e-discovery in a civil case involving corporations can be enormous – literally millions of pages of corporate electronic documents and records can sometimes be demanded by a plaintiff for disclosure, in the context of a specific case. Simply identifying, organizing, and producing the relevant documents can represent a Herculean task. Particularly in the U.S., e-discovery has become a big business, as technology vendors have entered the market to help corporations manage demands for large-scale document production in litigation.

E-discovery in situations involving both EU and U.S. actors becomes even more complicated and burdensome. Litigation-based requests for document production under the procedural laws of one country (e.g., the U.S.) can easily run into conflict with the data protection requirements of another (e.g., national transpositions of the EU Data Protection Directive 95/46/EC). Consider hypothetical U.S. litigation that involves a multinational corporate actor based partly in Europe, with a large pool of corporate records tied to individual employees (e.g., internal e-mails), the latter arguably protected under the European legal framework regarding privacy and data protection. The corporation in this scenario is targeted as a defendant in a U.S. law suit, and demands are made for the production of corporate records and internal e-mails. In addition to all of the logistical burdens pertaining to e-discovery, the corporation in this instance will also need to worry about the application of the European legal framework regarding privacy and data protection to its records. In the worst case, the corporation might find itself facing a legal obligation to disclose records in a U.S. court, while simultaneously facing a legal obligation in one or more EU states not to disclose those records, per European legal rules regarding privacy and data protection.

There is a broad range of potential situations and legal proceedings that plausibly could generate e-discovery conflicts for multinational corporations operating in the EU and U.S. Some examples include allegations of corporate bribery involving payments made to foreign government officials; compliance with regulatory reviews and investigations; co-operation with government price fixing investigations; participation in accounting investigations; conduct of internal corporate investigations involving employee theft or

Intellectual Property theft; international arbitration; and involvement in general civil and/or commercial litigation. These various scenarios capture a range of different legal and commercial contexts. Some involve the participation of government actors, while others do not. Some involve disputes between two (or more) parties, and requests for civil compensation. Some involve a mixture civil and criminal proceedings targeting a corporate defendant. And some involve purely internal corporate investigations, without regard to the demands of an external actor in a litigation proceeding. What all of these scenarios have in common is the potential for some form of e-discovery and disclosure: i.e., the need to gather and catalogue large numbers of electronic corporate records from within a multinational firm, and potentially to transmit those records across international boundaries.

For purposes of this report, we will focus our attention on one illustrative category of litigation and e-discovery, involving a combination of U.S. and EU players. Our focus here is on litigation under the U.S. Foreign Corrupt Practices Act (FCPA), which involves allegations of bribery involving both a connection to the U.S. and illicit payments made to foreign officials. As we describe below, FCPA is a major category of investigation and litigation in its own right, involving enormous potential liabilities to U.S. and EU companies. It is also similar in purpose and intent to the U.K.'s Bribery Act of 2010. More important for current purposes, FCPA cases can involve huge e-discovery burdens for defendants, and demands for document production in the U.S. that are problematic under the European legal framework regarding privacy and data protection. FCPA hypotheticals illustrate many of the challenges in e-discovery that are likely to arise in connection with other types of litigation, or legal activity involving corporations. In all such instances, the disclosure or transmission of electronic records across international boundaries will be involved, including records that are arguably protected under the European privacy and data protection framework.

3.1 What is the FCPA, and Why Is This an Important Investigation and Litigation Threat?

The U.S. Foreign Corrupt Practices Act (FCPA)[6] basically operates to prohibit U.S. citizens and U.S. listed companies from bribing foreign government officials, in an effort to obtain illicit favourable treatment or business opportunities.[7] Originally passed in 1977 and substantially amended in 1998, the FCPA statute aims to address and deter corruption in international business operations, by making it illegal under U.S. law for U.S. nationals (or their corporate affiliates) to engage in acts of bribery outside the United States, where the recipients of payment are foreign officials.[8] Notably, the amended FCPA standards of 1998 were drafted to correspond to a set of model anti-bribery conventions originally

[6] The FCPA is codified at 15 U.S.C. §§ 78dd-1, et seq.

[7] In tandem with the anti-bribery provisions of the FCPA, the statute also includes a related set of accounting transparency mandates for U.S. public companies, which require accurate bookkeeping mechanisms and adequate internal controls.

[8] Note that additional provisions of FCPA may also apply to non-U.S. firms and officials who, while in the U.S, abet acts of bribery to foreign officials.

developed by the Organisation for Economic Co-operation and Development (OECD). FCPA is jointly enforced by the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) in the U.S.; involves threats of both criminal and civil sanction against violators; and has resulted in a number of high-profile, multi-million dollar settlements with corporate defendants in the years since 2005.[9]

The FCPA provides an important international litigation context within which European data protection standards are likely to present challenges for e-discovery. The substance of FCPA investigations and litigation will typically involve situations where corporations are engaged in complex transactions across national boundaries; where both U.S. and European entities will be involved in those transactions; and where elements of both U.S. and European law may apply to litigation proceedings. As a practical matter, FCPA enforcement will often involve extensive e-discovery efforts undertaken by U.S. authorities, in support of a corporate prosecution. In consequence, FCPA demands for document production under U.S. law have the potential to run up against European data protection rules, in a way that may generate conflicting legal demands for corporate defendants.

FCPA is a particularly important challenge for many U.S. businesses and their European affiliates, in part because enforcement activity under the statute has grown far more vigorous in recent years.[10] According to statistics collected by the law firm Gibsun, Dunn & Crutcher, FCPA prosecutions rose from only two in 2003 to 38 in 2007. By mid-2009, more than 120 FCPA cases were then reportedly under investigation by U.S. authorities, and 40 cases were actually prosecuted in that year.[11] Meanwhile, FCPA settlements by corporate defendants involving tens or hundreds of millions US$ have become increasingly common. Examples of some of the more prominent defendants in such cases have included Siemens, Halliburton, Alcatel-Lucent, Titan, Baker Hughes, York International, and Statoil.[12]

For purposes of exploring the impact of European data protection laws on transfer of records across national borders in the context of threatened litigation, we focus on FCPA as our primary illustrative example. FCPA makes sense as a focal archetype for this kind of analysis, in part because FCPA does present a major investigation and litigation challenge for U.S. firms engaging in business with European affiliates, but also because many of the e-discovery and privacy issues that arise in FCPA litigation may also arise in other forms of international litigation, investigation, and regulatory enforcement activity as well.

---

[9] See, e.g., discussion of 1.6B USD settlement by Siemens of FCPA and other bribery charges in 2008, Schubert, S. & Miller, T.C., December 20, 2008, "At Siemens, Bribery Was Just A Line Item," New York Times, available at http://www.nytimes.com/2008/12/21/business/worldbusiness/21siemens.html?_r=1&em.

[10] See discussion in Searcey, D., May 26, 2009, "U.S. Cracks Down on Corporate Bribes," Wall Street Journal, available at http://online.wsj.com/article/SB124329477230952689.html#articleTabs%3Darticle.

[11] See Gibson Dunn, January 4, 2010, "2009 End of Year FCPA Update," available at http://www.gibsondunn.com/publications/pages/2009Year-EndFCPAUpdate.aspx. See also Searcey (2009) above.

[12] See Wong, R. & Conroy, P., January 28, 2009, "FCPA Settlements: It's a Small World After All," NERA, available at http://webcache.googleusercontent.com/search?q=cache:UQVKFoCij7kJ:www.nera.com/image/Pub_FCPA_Settlements_0109_Final2.pdf+FCPA+Settlements:+It%E2%80%99s+a+Small+World+After+Al&hl=en&gl=us.

3.2 What Are the Key Attributes of an FCPA Investigation and Litigation?

The FCPA is a U.S. legislative act that applies primarily to U.S. companies engaged in international business activity. Given that we are concerned here with potentially conflicting applications of European legal norms regarding privacy and data protection, we can conclude that relevant instances of FCPA investigations will typically include the involvement of all of the following: (1) one or more U.S. corporations or persons, or the foreign issuer(s) of U.S. registered securities;[13] (2) one or more European persons, corporations, affiliates, or counterparties; and (3) one or more government officials outside the U.S., who are the target of putative illicit payments made in violation of the Act.

FCPA litigation will always involve enforcement activity on the part of the U.S. SEC and/or the U.S. DOJ. By extension, every FCPA investigation or prosecution is going to involve government requests or demands for document production, pursuant to U.S. law.

FCPA cases will typically involve a litigation or investigative context, in which documentary evidence is sought by law enforcement authorities and prosecutors for admission in U.S. courtroom or regulatory proceedings. Some FCPA scenarios may involve pre-trial settlements on the part of defendants, seeking to obtain lenient or favourable treatment from U.S. authorities in lieu of courtroom or regulatory proceedings. In some such instances, corporate defendants may be motivated to co-operate voluntarily with SEC or DOJ requests for evidence, absent formal court subpoenas, investigative warrants, or demands for document production under the U.S. Federal Rules of Civil Procedure.

Drawing on all of the foregoing, a typical FCPA case will involve an attempt by SEC or DOJ to establish that an unlawful payment or equivalent was made by a U.S. national or affiliated party to a foreign government official, in return for favourable treatment. All such cases that are relevant to European privacy and data protection rules will also involve a European nexus – either European companies or nationals will be accused of playing some role in committing the alleged bribery, or European officials will be the targets of the bribery, or both. To establish a successful FCPA case, the SEC or DOJ will need to seek evidence that touches on European nationals, and (in many instances) that resides in the electronic records of European firms or subsidiaries. It is in this context that European data protection standards and restrictions will be implicated.

3.3 What Kinds of E-Discovery Challenges Are Likely to Apply in an FCPA Situation?

In thinking about potential FCPA cases involving Europe, it is important to recognise two central considerations relating to e-discovery. First is simply the breadth of electronic records that plausibly might be requested for production in an FCPA case. FCPA-relevant documents could include a range of corporate e-mails and other documents, invoices and

[13] See definitions for the parties covered by the FCPA at 15 U.S.C. §§ 78dd-1, et seq.

accounting records and databases, and other sorts of corporate records and communications systems, notably including data from corporate websites and instant messaging programs. Taken collectively, and in the context of international business transactions touching one or more European firms, FCPA discovery of electronic records may be voluminous, may involve records kept in multiple different languages, and may require retrieval of data from multiple electronic depositories and computer systems. By implication, simple compliance by an FCPA defendant with e-discovery demands alone may sometimes be a very burdensome task, irrespective of the impact of the European legal framework regarding privacy and data protection

This being said, the application of European data protection and privacy rules to different types of documents and records in e-discovery presents another set of considerations, particularly around the management of various categories of documents and electronic materials with different privacy characteristics. Discovery and retrieval of personal e-mails, e.g., might be more likely to raise privacy and data protection concerns than would discovery of corporate accounting records (though, we recognise that such may contain protected customer data) – and perhaps particularly so if personal e-mails from lots of different individuals are being accessed, disclosed, and reviewed simultaneously. Different categories of electronic material may be subject to different levels of protection under European privacy standards, based on the nature of the communications medium and the records at issue. By extension, the specific kinds of discovery that are undertaken in a particular FCPA case may present more or less legal conflict with European privacy and data protection law, and more or less of a compliance burden, depending on the details of what electronic materials are actually sought. Analysis of European privacy and data protecton problems posed by FCPA cases will turn, in significant measure, on factual considerations about the kinds of records that may be sought and disclosed in litigation.

3.4 How Might an FCPA Matter Differ from Other Privacy-Implicated Scenarios Involving U.S.-European Business Dealings?

Clearly, there are many other non-FCPA contexts in which the disclosure of European corporate records, including electronic records, might be sought. As mentioned earlier, examples range from international commercial and civil litigation, to due diligence in connection with mergers and acquisitions, to regulatory reviews or inquiries in many different flavours, to purely internal corporate investigations that may nevertheless span parent-subsidiary relationships and international borders. In analyzing how European privacy and data protection rules apply to these different situations, how should we think about the example cases of e-discovery in the context of FCPA?

Setting aside the legal subtleties of all of these different situations, three general points are worth noting. First is that the basic analysis of privacy problems under European law may have more do with the nature of the records being disclosed, than the specific U.S. legal context in which those records are sought.[14] The distinction in sensitivity between e-mails

[14] Misconduct targeted by the FCPA may very well also be illegal under a MS' law (active/passive corruption is likely to be a criminal act fairly universally, especially when the person bribing/being bribed is a government

and aggregated accounting records, may be more important in regard to understanding European privacy implications, than are the any of the differences between hypothetical FCPA investigations and litigation vs. commercial litigation. Second and notwithstanding the foregoing, FCPA cases are clearly noteworthy for turning on the involvement of a U.S. government agency. In at least some instances, that agency may be acting in a law enforcement or prosecutorial capacity when it seeks electronic records. Possibly, the role of a government actor engaging in law enforcement activity might sometimes be a meaningful distinction for the treatment of disclosures under European privacy law: It surely represents a different kind of litigation scenario from one in which there is no government actor, and no law enforcement involvement.

Finally, hypothetical FCPA scenarios highlight sets of facts that implicate both U.S. and European corporate actors in alleged misconduct. To understand the e-discovery implications, it may well be that the specific EU countries involved in a scenario are particularly important to analyzing the impact of the privacy law. To the extent that this is true, the analysis of FCPA scenarios may offer more general insights about the application of privacy law to other forms of international litigation, particularly where the same countries and national boundaries are involved.

3.5 Conflicting legal obligations for privacy under the law of different European Member States

Because of the complexity inherent in any international litigation scenario, coupled with the uneven and patchy implementation of EU privacy and data protection law across various EU Member States, any analysis of the e-discovery and privacy challenges posed by the scenarios really does depend on the way that individual member states have constructed and implemented their own legal frameworks regarding privacy and data protection. In a separate report[15], we investigate and describe the national approaches to, and interpretation of, the EU Data Protection Directive, across several European countries.

3.6 Example illustrative scenarios Involving FCPA Claims and European Privacy Data Standards

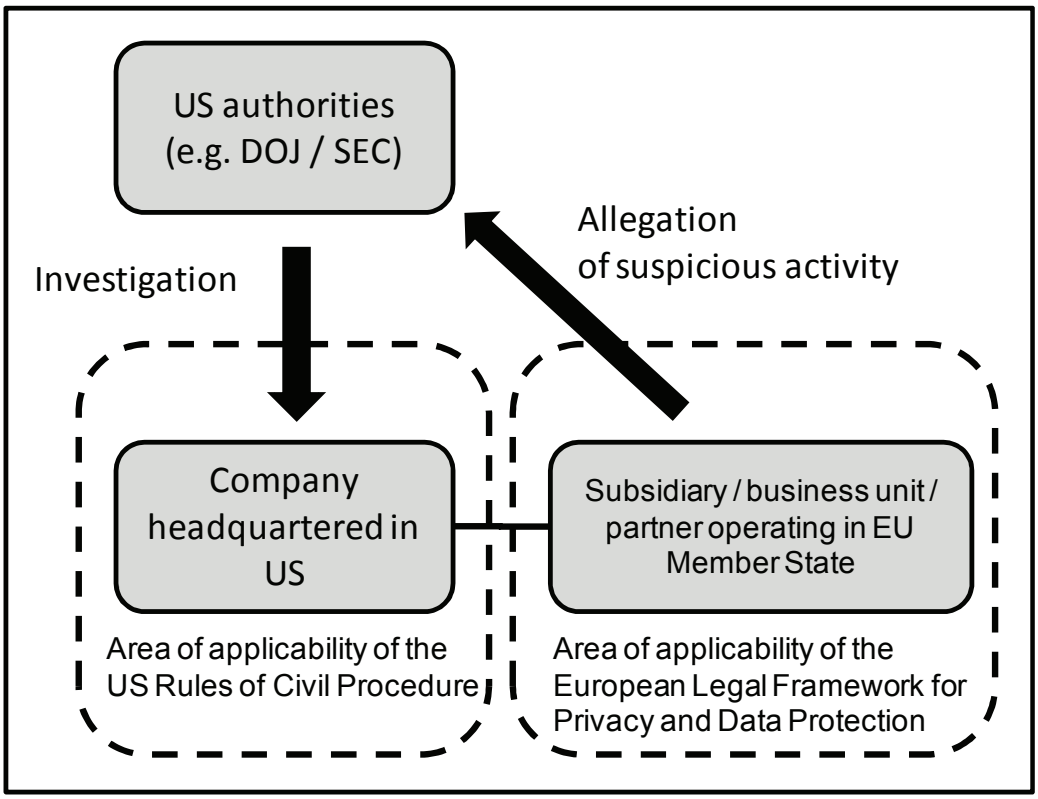
Based on the discussion of FCPA above, we present three examples of hypothetical FCPA cases, in which e-discovery might likely generate privacy problems under EU data protection rules.

official). In that case, the processing of personal data can also be done in collaboration with EU law enforcement bodies and falling under former 3rd pillar (police and criminal justice co-operation).

[15] Readers interested in obtaining the Confidential Appendix may contact Joe Looby, Senior Managing Director FTI Consulting New York joe.looby@fticonsulting.com

A generic model of this is illustrated in Figure 3 below.

Figure 3. Generic model illustrating conflict of laws issue in respect of pre-trial discovery and data protection



Source: RAND Europe

We offer these example scenarios partly to give a sense of some of the kinds of litigation situations where privacy problems are likely to arise, and also to illustrate some specific points of concern in the subsequent analysis of EU data protection and privacy rules in this report.

- A U.S. oil company engages in a deal in Iran, with the support of an intermediary contract firm based in France, to help develop and exploit a new oil field. Alleged bribes were made to officials in Iran through the intermediary of the French corporate affiliate, in return for a lucrative government contract to the U.S. and French collaboration. Allegations have now been made that multiple U.S. and European executives knew about the bribes to Iranian officials before the fact, and tacitly approved them. At least six French nationals are suspected of having been involved in planning and executing the illicit payments. U.S. investigators are now seeking discovery of tens of thousands of corporate e-mails from both the U.S. company and the French contractor, in connection with the alleged bribery.
- A U.S.-listed plastics company enters into a deal to build and operate a new factory in Slovenia. The company is accused of making illicit payments to government officials to obtain licenses and other necessary approvals to begin construction. Alleged participation in the wrongdoing includes illicit activity by American citizens based in the U.S. who are executives in the company; by

German citizens based in Germany who are also managers in the company; and by two Slovenian contract agents who are believed to have made payments to Slovenian officials under the supervision of both German and U.S. managers. Prosecutors in the U.S. are now demanding discovery of internal audit records concerning business travel and payments made by corporate officials.

- A U.S.-based company and its Spanish subsidiary are accused of paying millions of dollars of illegal surcharges to the Iraqi government and Iraqi officials in connection with purchases of crude oil from third parties, under the Oil-for-Food program. Bribes are believed to have been passed by several Spanish nationals operating on Iraqi soil, but with planning by Spanish executives and financing from bank accounts in Spain, and after-the-fact approval by executives based in the United States. U.S. authorities now demand access to corporate e-mails, travel and financial records, and records from internal control and accounting processes pertaining to the alleged transactions.

In the next chapter we summarise relevant findings from our national research illustrating the practical challenges associated with these issues at the national level.

CHAPTER 4 National contexts - summary

Interviews were conducted with national experts in five European countries (France, Germany, Spain, Switzerland and the United Kingdom) in order to identify the legal framework applicable to e-discovery requests at national level as well as the policy factors that are taken into consideration in each of these jurisdictions. With the exception of Switzerland, all of the countries in which interviews were conducted are EU Member States; they were selected on the basis of their differing legal traditions and approaches to privacy issues. A complete overview of these interviews can be found in the confidential appendix accompanying this report which can be obtained on request from FTI Consulting.[16]

The rules on pre-trial discovery differ significantly between these states. The UK, as a common law jurisdiction, has a well-established set of pre-trial discovery rules in place; a party to litigation is required to disclose any documents which adversely affect its own case as well as documents which support the opposing litigant's case. The other jurisdictions, which are all civil law jurisdictions, have no system of pre-trial discovery. Rather, parties must only offer evidence to the Court to prove that the facts they are asserting are true. In strictly circumscribed circumstances in each of these jurisdictions however an order for disclosure can be sought from a judge.

The legal basis for processing an e-discovery request depends on the nature of the proceedings for which the information concerned is sought. If the request is made to obtain evidence for civil proceedings, the Hague Convention is applicable. However, Article 23 of the Hague Convention allows Contracting States to declare that they will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. All of the jurisdictions considered in this report have invoked this exception. Nevertheless, it is only Germany and Spain that refuse to consider Letters of Request under any circumstances. In France, in accordance with a declaration made by the French government, a Letter of Request will be authorised if it identifies a limited number of documents to be disclosed and the documents have a direct connection with the subject matter of the dispute. In Switzerland Letters of Request are accepted if they comply with strict limitations designed to prevent 'fishing expeditions' for evidence. In the UK evidence can be sought in accordance with the Evidence (Proceedings in Other Jurisdictions) Act 1975; applications must be made to the High Court supported by written evidence

[16] Readers interested in obtaining the Confidential Appendix may contact Joe Looby, Senior Managing Director FTI Consulting New York joe.looby@fticonsulting.com

accompanied by the request as a result of which the application is made. All of the jurisdictions considered have concluded a bilateral agreement with the United States allowing for mutual assistance in criminal matters; evidence for criminal proceedings can be sought by relying on these agreements. In France when documents and information of an economic, commercial, industrial, financial or technical nature are transferred to foreign individuals or entities and the Hague Convention or a Mutual Assistance Agreement is not applied, penal sanctions can be imposed on the transferor. Such a 'blocking statute' also exists in Switzerland and has been applied on numerous occasions.

Pre-trial discovery requests must also comply with the data protection provisions in place in each jurisdiction. As the European Data Protection Directive (Directive 95/46/EC) has been transposed into national law in France, Germany, Spain and the UK the rules in place in these jurisdictions are almost identical. Moreover, the Swiss have followed the scheme set out in the Directive to a large extent. The Data Protection Directive regime does not prohibit data processing (which includes the act of transferring personal data). Rather, according to Article 7, data processing is legitimate provided one of the criteria set out therein is complied with and the quality-assurance principles relating to data processing in Article 6 are respected. The most likely legal basis for legitimate data processing is Article 7(f) according to which processing is legitimate if it is '...necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject'. Indeed, the French data protection agency (the CNIL) specifically referred to this provision as a basis for data transfers in its recommendation concerning e-discovery in civil and commercial proceedings. The application of this provision requires that the data transfer is proportionate. For instance, when this provision has been applied by the British judiciary in the context of freedom of information requests specific attention has been paid to the meaning of the word necessary. This test will be difficult for lay-parties to apply and legal guidance will be needed. Indeed, the Information Commissioner in the UK has urged caution when applying it. As a result some data protection agencies, for instance the Swiss, are happy to provide transferors with ex ante advice concerning the legitimacy and proportionality of the transfer.

According to the Directive an adequate level of protection must be provided by the data recipient when a transfer is made to a third country. In general, the adequacy of the level of protection applied can be proven if the safe harbour principles are complied with, the data recipient has signed up to standard contractual clauses with the data controller or binding corporate rules are in place within a commercial group. Certain national distinctions nevertheless still exist. For instance, in France, non-massive transfers (transfers of small amounts of data on a non-recurring basis) do not require the prior-approval of the CNIL.

At a policy level, data protection authorities operate at a national level in France and the UK and at a regional level in Switzerland and Germany. In Spain, both regional and national data processing authorities exist; the national authority is responsible for processing by private parties. In general in these countries there is little awareness of the provisions of the FCPA. Although the data protection authorities in each of the jurisdictions considered have the power to impose significant sanctions for breaches of the data protection rules, no jurisdiction has exercised this power to sanction the transfer of

data to a third country for discovery purposes. Indeed, it appears that it is only in France that this issue has been given serious consideration. The CNIL has been quite vocal on the issue and has issued a recommendation concerning e-discovery in civil and commercial proceedings. The other data protection authorities have been concentrating their enforcement efforts elsewhere; for instance, in Germany priority has been given to publicly visible privacy issues (although private enterprises continue to be sanctioned) while in the UK the main focus is on security breaches and audit.

CHAPTER 5 Way forward and conclusions

Given these various national differences described in the Confidential Appendix, what would be a suitable way forward for organisations confronted with the conflicting requirements of meeting the standards of European legal framework governing privacy and data protection and US e-discovery requirements? To illustrate some possible avenues to resolving this we firstly present guidelines from both the Article 29 Working Party in its Opinion 158 on pre-trial discovery and also the framework from the Sedona Conference followed finally by our own more comprehensive framework based on the analysis contained in the previous Chapters.

5.1 Article 29 Working Party Guidelines

The Article 29 Working Party in its Opinion 158 on pre-trial discovery proposed a framework, based on four generic stages of pre-trial discovery. As the European group responsible for interpretation of points of law regarding the EU Data Protection Directive 95/46/EC, the Working Party recognised the need for reconciling the requirements of US litigation rules and the provisions of the legal framework governing the protection of personal data. It also noted that whilst Directive 95/46/EC does not prevent transfers for litigation purposes, nonetheless certain requirements must be met in order for lawful pre-trial disclosure to take place using personal data. In order to meet these requirements, a set of guidelines were proposed on pre-trial discovery.

The Working Party argued that ultimately there were three relevant grounds for the processing of personal data in the context of pre-trial discovery: firstly that the processing has the consent of the data subject, secondly that it complies with Article 7(c) or Article 7(f) or finally, transfer is in line with Article 26 of the Directive (and associated national transpositions as detailed above).

5.1.1 Consent deemed unworkable

Grounds under Article 7(c) and 7(f) were deemed to be the most viable since the Working Party concluded that consent is "unlikely...to provide a good basis" for such processing. This is for the obvious reason that the achievement of consent under the criteria of the Directive contradicts the very characteristics of such pre-trial discovery activities. The rejection of consent as a valid ground is based on a number of complex notions. Firstly, that consent in the case of pre-trial discovery with US firms cannot be said to have been 'freely given' since employees or customers could not have exercised any meaningful choice about the company undertaking business in the United States and thereby being subject to

US Rules of Civil Procedure. The Working Party concluded that in this respect data controllers wishing to export personal data would need to produce clear evidence of the data subjects' consent and may also be required to demonstrate that the data subject was informed about the processing. Furthermore, for consent to be deemed valid it must be freely given and by withholding it (or later withdrawing it) the data subject must not be subject to adverse consequences. The only scenario in which the Working Party considered that consent, as referred to in Article 7(a) of the Directive, might be a valid basis on which to transfer data is when the individual data subject may be aware of or even involved in the litigation process, in which case this may be 'properly...relied upon' as a ground for processing.

5.1.2 Possibilities of Article 7 (c) based on Orders of Court

Article 7 (c) states that data processing is deemed legitimate if it is necessary to comply with a legal obligation to which the data controller is subject. However, this only applies where the Member State has enacted legal obligations to comply with Orders of Court from a foreign jurisdiction. Where a reservation under the Art 23 of the Hague Evidence Convention exists, then the Working Party's opinion is that such processing may be possible under Article 7 (f): if it is necessary for the purposes of a legitimate interest, however a balancing exercise is then undertaken to take into consideration the interests and fundamental rights and freedoms of the data subject.

5.1.3 Article 7(f) necessary to pursue purposes of legitimate interest

Under Article 7(f) of the Directive, processing is legitimate if it is necessary for the purposes of the legitimate interests pursued by the controller or the third party to whom the data are disclosed. In this instance, the interests of the controller or third party in processing must be balanced against the interests and fundamental rights and freedoms of the data subject. A proportionality test is therefore necessary and the relevance of the personal data to the litigation and the impact of processing on the data subject is considered. The rights of the data subject under Article 14 also need to be respected. In the Opinion of the Article 29 Working Party, prior to processing Data Controllers should restrict disclosure to anonymised or pseudo-anonymised personal data which may be filtered or culled by a trusted third party in the European Union, prior to disclosure of a much more limited set of personal data as a second step.

5.1.4 Other factors to be taken into account

Other characteristics were noted as being important to bear in mind in any processing, including the principle of proportionality, whether the data being requested constitutes sensitive data (within the meaning of Article 8 of the Directive), provisions made for data security, transparency and upholding the data subject's rights of access, rectification and erasure.

5.1.5 Article 26: Onward Transfer

In the case of transfers to third countries outside the EU, the Working Party noted that Article 25 and 26 apply and highlighted that in the absence of a determination of adequacy for the destination (under Article 25) three main possibilities for the onward transfer of personal data to third country jurisdictions exist, namely:

- The recipient is established under the Safe Harbor Scheme;

- The receipt has entered into a transfer contract containing adequate safeguards, for example the Standard Contractual Clauses based on the templates issued by the European Commission in Decisions of 2001 and 2004;
- A set of approved Binding Corporate Rules (BCRs) are in place.

The Working Party in its Opinion concluded that a possible ground for onward transfer existed under the derogation detailed in Article 26(1)(d) of the Directive, namely that

> *"...transfers of personal data to a third country which does not ensure an adequate level of protection may take place if one of the following conditions are met:*
>
> > *...d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;"*

The Working Party suggested that the use of BCRs or Safe Harbor should be considered in the event of the transfer of significant amounts of data as the derogation in Article 26(1)(d) above should not be used to justify a broader transfer on the basis that such data may be needed for the purposes of legal proceedings one day in US courts.

5.2 The 2008 Sedona Framework

In its document "Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery" in August 2008, Working Group 6 of the US based *Sedona Conference*[17] proposed a framework based on the following points:

5.2.1 Is there jurisdiction?

- Does the forum/court have jurisdiction over the data? Including such questions as the relationship between an affiliate and party, the definition of control of data (particularly relevant with respect to the European legal framework governing privacy and personal data protection) and data controller; the location of data (again, given a core characteristic of European privacy and data protection law being the 'location' of personal data)
- Which non-forum entity has jurisdiction? This domain included answering such questions as whether there is jurisdiction over the activity (data processing or collection) the data, nationality of person or data and data controller, location factors including where the data was created, where the data sits at rest the location of servers and so on).

5.2.2 Provisions limiting cross border data transfer

- Determine whether the data is subject to a provision limiting cross-border transfer including the character of the data (whether it is personal, sensitive or industry specific) the jurisdiction of the limiting provisions – regional, national and sectoral

[17] "The Sedona Conference® is a nonprofit, 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights."

provisions, the existence of derogations to limiting provisions (e.g. if information is in the public domain or a derogation may be permitted to enable compliance with regional or local legal obligations or for example under Article 26(1)(d) of the EU Data Protection Directive 95/46/EC) and finally whether data can be made to fit the limitations of the provisions e.g. via anonymisation, culling or obtaining consent of the data subjects or finally via limitation of the data request (requesting the principle of proportionality).

5.2.3 Is there a blocking statute?

- Those involved in pre-trial discovery should research the existence of a general or industry specific blocking statute.

5.2.4 Is there a treaty, legislation or agreement between the parties which may provide a solution?

- A Treaty, legislation or agreement between parties which may provide a solution to include consideration of the existence of the Hague Convention or failing that ad-hoc consent from a Data Protection Commissioner or other independent supervisory authority and if so whether a Protective Order is necessary to satisfy the conditions.

5.3 Proposed way forward

Noting these specific and general guidelines and frameworks provided above along with national differences outlined previously, we propose our own simple checklist based approach below:

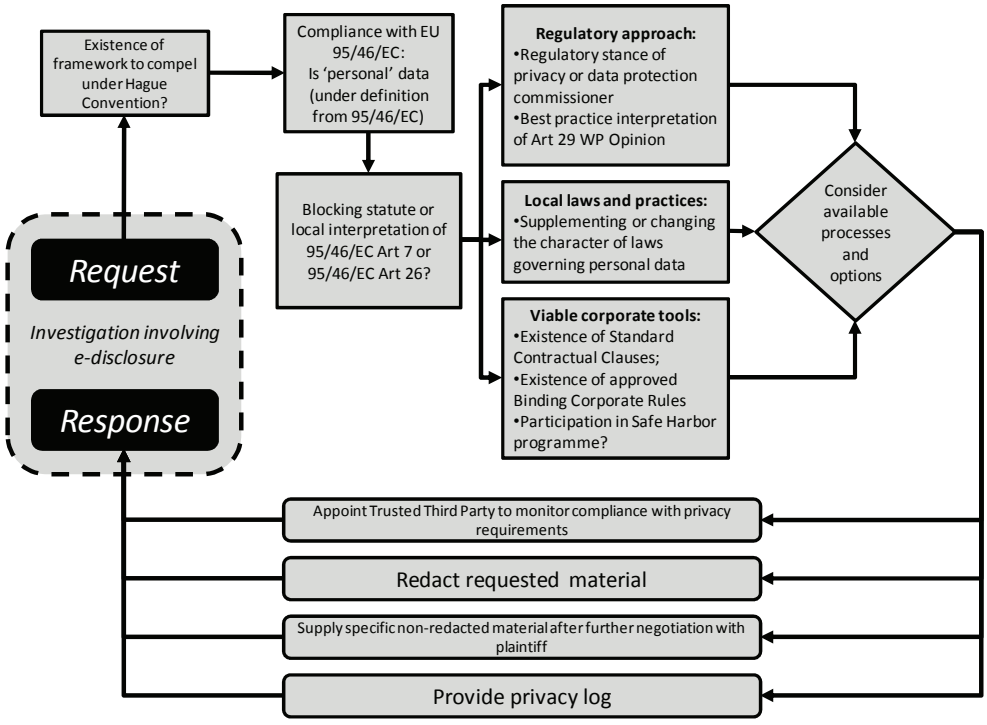
- First – is there any potential framework to compel co-operation with US discovery rules for example under the Hague Convention or other bilateral agreements (depending on the civil or criminal nature of the request)
- Consider whether any data classified as personal under national interpretations of the EU Data Protection Directive 95/46/EC is likely to be involved – an estimation of the types and character of the data (whether it falls within the scope of EU data protection rules as it relates to an 'identifiable person'; whether the data concerned is 'sensitive data')
- Whether a blocking statute or other local legal restriction or interpretation on data disclosure exists – stemming from relevant Applicable National Law transposing Articles of 95/46/EC e.g. under Art 7(f) and Art 26(1)(d)
    - Whether the company has approved Standard Contractual Clauses (SCC) or Binding Corporate Rules (BCRs) in place which would govern the onward transfer of personal data;
    - Whether there are any unique local regulations or laws supplementing or changing the character of legislation governing the processing and transfer of personal data;
    - Similarly, whether the application of the law in practice differs in any respect given the regulatory stance and strategic approach of the

Independent Supervisory Authority (ISA) in the interpretation of this guidance (as we have seen above, EU Member States may differ in how they interpret the official guidance as presented by the Article 29 Working Party).

- Finally, upon satisfactorily answering the above, investigate processes and options that respect the fundamental rights of European citizens under Article 16 of the TFEU whilst serving the purposes of pre-trial discovery. Such options might include the following:
    - Redacting or anonymising all documents in country, prior to the disclosure and onward transfer to the United States
    - Provision of a Privacy Log which details the information protected from disclosure in order for plaintiffs to determine more clearly the necessity of the disclosure of such data and possibilities for amendment of the Protective Order in order to safeguard defendants from liability for the production of this data
    - For those deemed of specific interest by the litigants in the pre-trial discovery process in the United States the European based subsidiary supply them in non-redacted form
    - Assigning a suitably qualified and appropriate Trusted Third Party to support the adherence of the processing to appropriate level of adequacy of protection in line with the European legal framework for privacy and data protection.

Figure 4 below illustrates this approach.

Figure 4. Suggested e-Disclosure workflow



Source: RAND Europe

5.4 Conclusions

This report has illustrated the difficulties of international transfers of data for e-discovery purposes. Despite the fact that many EU states are party to the Hague Convention and have transposed the EU Data Protection Directive into national law, stark differences in the legal regime applicable to international transfers for the purposes of e-discovery exist between EU Member States. These differences stem only in part from the fact that EU states have divergent common and civil law legal traditions. Of relevance when considering transfers of evidence for civil proceedings is whether the State concerned has invoked the Article 23 exception to the Hague Convention (which even the United Kingdom, a common law country, has invoked). Transfers of evidence for criminal proceedings are governed by bilateral agreements which differ from state to state. Moreover, some states, for instance France, have enacted 'blocking statutes' entailing harsh criminal sanctions for those who transfer certain types of information abroad. The data protection legislation in place also needs to be complied with. Here, although there are some minor differences between transposition in various countries, the overall legal framework remains similar; transfer is possible without consent once an 'adequate' level of protection is guaranteed whether that be by resorting to Standard Contractual Clauses, falling with the scope of a Safe Harbor agreement or by respecting Binding Corporate Rules. If certain criteria are met e.g. in respect of either consent or the presence of existing instruments such as Binding Corporate Rules or participation in the Safe Harbor agreement, we propose a set of suitable measures designed to improve accountability in respect of companies meeting their joint and often conflicting obligations under the differing US and European legal frameworks.

REFERENCES

List of References

Article 29 Data Protection Working Party; *WP No. 158 on pre-trial discovery for cross border civil litigation* – 11 February 2009

Article 29 Data Protection Working Party; *WP No. 168 on The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* 1 December 2009

European Council and European Parliament; *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* 24 October 1995

Gibson Dun; January 4, 2010, *2009 End of Year FCPA Update* available at http://www.gibsondunn.com/publications/pages/2009Year-EndFCPAUpdate.aspx

Hijmans, H, and Scirocco, A; *Shortcomings in EU Data Protection in the Third and Second Pillars: Can Lisbon be expected to help?* 2009 Common Market Law Review (46) pp1485-1525 London

Robinson N, Valeri L. et al; *Review of the European Data Protection Directive* RAND; Santa Monica May 2009 http://www.rand.org/pubs/technical_reports/TR710/

Schubert, S. & Miller, T.C.; December 20, 2008, *At Siemens, Bribery Was Just A Line Item* New York Times, available at http://www.nytimes.com/2008/12/21/business/worldbusiness/21siemens.html?_r=1&em.

Searcey, D.; May 26, 2009, *U.S. Cracks Down on Corporate Bribes* Wall Street Journal, available at http://online.wsj.com/article/SB124329477230952689.html#articleTabs%3Darticle.

Sedona Conference Working Group 6; *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery* August 2008

Wong, R. & Conroy, P., January 28, 2009; *FCPA Settlements: It's a Small World After All* NERA, available at http://webcache.googleusercontent.com/search?q=cache:UQVKFoCij7kJ:www.nera.com/image/Pub_FCPA_Settlements_0109_Final2.pdf+FCPA+Settlements:+It%E2%80%99s+a+Small+World+After+Al&hl=en&gl=us

APPENDICES

List of Interviewees

National correspondents consulted for the separate Confidential Appendix included:

- France: Fanny Coudert, time.lex Law Offices, Paris
- Germany: Petra Hansmersmann, Unverzagt von Have, Hamburg
- Switzerland: Martin Eckert, Meyer Müller Eckert Partners, Zurich
- Spain: Cristina de Lorenzo, Sánchez Pintado & Núñez, Abogados, Madrid
- United Kingdom (England and Wales) Ruth Boardman, Dania Rifaat and Sarah Weindling, Bird and Bird, London