Brobeck Hale and Dorr

UK-US DataTransfers Under the EU Privacy Directive:

Compliance Options for Multinational Companies

Barry J. Hurewitz
Hale and Dorr LLP
19-20 November 2002

The Technology Law Firm

Brobeck Hale and Dorr

EU Restricts Transatlantic Transfers of Personal Data

- EU Privacy Directive bars transfers of personal data to non-EU countries lacking “adequate” data protection laws
- EU has determined that U.S. privacy laws are not adequate

Brobeck Hale and Dorr

The U.S. Follows a Different Regulatory Philosophy

- Distaste for government regulation
- Government viewed more as potential violator than guardian of personal privacy
- Preference for market-driven industry “self-regulation”
- Sector-specific privacy legislation

U.S. Privacy Law is a Patchwork

- Wiretapping (1968)
- “Unfair or deceptive” practices (1970)
- Consumer credit information (1970)
- Government records (1974)
- Educational records (1974)
- Electronic communications (1986)
- Home video rentals (1988)
- Telecom subscriber data (1996)
- Health information (1996; rules effective 2003)
- Children’s online privacy (1998)
- Consumer financial information (1999)
- Employee records (various federal & state provisions)

Brobeck Hale and Dorr

Bulk Transfers of Employee and Customer Data

- Consent
- Contractual safeguards
- Contractual necessity
- Safe harbour

Compliance Option: Consent

- Must be unambiguous
- Generally must be affirmative “opt-in” authorizations
- Can be withdrawn at any time
- Consent from employees may be unenforceable
- Useful when data subjects can be easily contacted
- Ill-suited for bulk transfers of large HR or customer data

Compliance Option: Contractual Safeguards

- Ad hoc contracts
  - Time-consuming and inefficient for intra-company transfers
  - Subject to government approval
  - Data recipient must comply with EU Member State law
- Model contracts
  - Requirements approximate EU Directive itself
  - Warranty that other laws will not interfere with compliance
  - Joint and several liability
  - Subject to EU Member State jurisdiction
  - U.S. Government: "Not a workable alternative model"

Compliance Option: Contractual Necessity

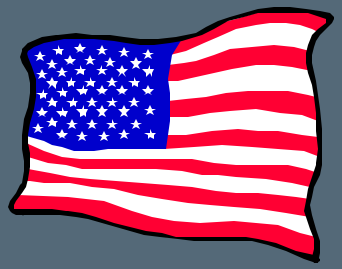
- "Necessity" is narrowly construed
  - Transfer must be essential to meet specific contract obligations
  - Subject to inconsistent interpretations
- Disfavoured by EU Working Party
- Does not promote confidence between the parties
- Probably unavailable for HR data in employment-at-will situations

Brobeck Hale and Dorr

Compliance Option: Safe Harbour

- Compromise framework resulting from bilateral negotiations
- Voluntary annual self-certification by U.S. entities
- Enables U.S. entities to overcome the “adequacy” problem
  - Entity may specify classes of data to be covered (e.g., online, offline, HR)
  - All EU data in specified classes must be protected
  - Does not affect obligations of EU subsidiaries
- Open to companies subject to Federal Trade Commission (or Department of Transportation) enforcement
  - No financial institutions, telecom carriers, or non-profits
  - Continuing discussions about financial institutions
- Launched in Nov. 2000; 258 enrolled as of Nov. 2002
- Public list reassures EU data controllers

Brobeck Hale and Dorr



- What will I have to do?
- Can’t I just wait?

- Will my data be sufficiently protected?

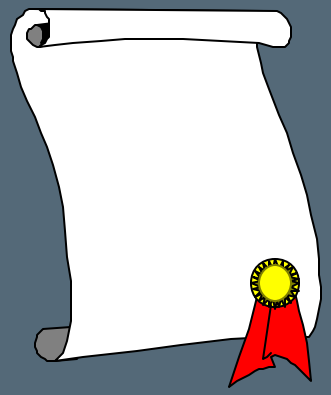
Safe Harbour Principles

- Notice
- Choice
- Onward transfer
- Security
- Data integrity
- Access
- Enforcement

Brobeck Hale and Dorr

Safe Harbour Principle: Notice

- Disclose what information is collected and why it is needed
- Provide point of contact for privacy issues
- Disclose range of uses, disclosures, and available restrictions
- Should be coordinated with HR and customer service policies



Safe Harbour Principle: Choice

- Opt-out for third party disclosures and secondary uses
- Higher opt-in standard for sensitive information
- “Reasonable efforts to accommodate employee privacy preferences”
- Exception to protect legitimate interests of employers in making HR decisions

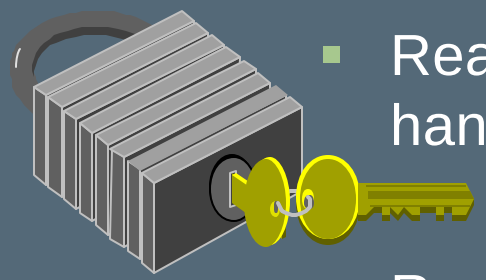
Safe Harbour Principle: Onward Transfer

- Re-transfers generally subject to notice and choice
- Transfers to “agents” permitted without notice and choice, if recipient
  - Is enrolled in the safe harbour, or
  - Is subject to the EU Privacy Directive or an EU “adequacy” finding, or
  - Agrees in writing to “similar standards” providing the “same level of privacy protection”
- No liability for violations by recipients, unless the U.S. entity
  - Knew or had reason to know of violations, and
  - Failed to prevent or stop them

Brobeck Hale and Dorr

Safe Harbour Principles:

Security and Data Integrity



- Reasonable protections against improper handling, loss, misuse
- Reasonable steps to ensure that information is relevant, accurate, complete, and current

Access

- Right to view information about oneself
- Qualified right to correct, amend and delete
  - Right of access is balanced against risks to privacy

Safe Harbour Principle: Private Enforcement

- Verification
  - Annual internal or independent compliance assessment
  - Optional privacy seal programs
- Independent dispute resolution
  - For HR data, disputes resolved through DPAs
  - For other data, private dispute resolution may be used
- Remedies
  - Potential civil liability

Government Enforcement

- Negative publicity
- Administrative enforcement by FTC (or DOT)
- State enforcement of consumer protection laws
- “False Statements” liability
- Suspension of EU data transfers
  - “Flexible implementation” by EU
- Loss of safe harbour listing

Brobeck Hale and Dorr

Assessing the Safe Harbour Option

PROs

- Simpler than the Directive itself
- Predictability throughout EU
- Continuity of data flows
- Protection against private claims
- U.S.-based enforcement

CONs

- Public commitment required
- New burdens on use and disclosure
- Expanded regulatory liability
- Implementation costs
- EU subsidiaries remain exposed
- Not conceived for intra-company transfers
- EU exporters may still insist on higher standards

Steps Toward Compliance

- Before initiating transfers of EU personal data to the U.S. . . .
  - Privacy officer
  - Internal assessment of data practices
  - Select compliance option
  - Develop and implement privacy policy and practices
  - Certify for safe harbour (optional)

Brobeck Hale and Dorr

Questions?

- Barry J. Hurewitz
- Government & Regulatory Affairs
  Hale and Dorr LLP
  Washington, DC
- barry.hurewitz@haledorr.com
- +1 202 942 8413