Data Protection & Privacy

In 31 jurisdictions worldwide

Contributing editor
Rosemary P Jay

2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Third edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

The Future of Safe Harbor

Aaron P Simpson
Hunton & Williams

Twenty-first century commerce depends on the unencumbered flow of data around the globe. At the same time, however, individuals everywhere are clamouring for governments to do more to safeguard their personal information, especially in the wake of Edward Snowden's explosive revelations last summer regarding government snooping. A prominent outgrowth of this global cacophony has been reinvigorated regulatory focus on cross-border data transfers. The Russian Parliament made headlines in July 2014 by adopting a bill that requires companies transmitting the electronic communications of Russians over the internet to store copies of the data for a minimum of six months in databases located within the Russian Federation. While this is an extreme example of 'data localisation', the Russian bill is not alone in its effort to create impediments to the free flow of data across borders. The Safe Harbor framework, which has been a popular tool used to facilitate data flows from the EU to the US for nearly 15 years, has recently come under attack as well, primarily as a result of the PRISM scandal. These attacks have raised challenging questions regarding the future of the Safe Harbor framework.

Contrasting approaches to privacy regulation in the EU and US

Privacy regulation tends to differ from country to country around the world, as it represents a culturally bound window into a nation's attitudes about the appropriate use of information, whether by government or private industry. This is certainly true of the approaches to privacy regulation taken in the EU and the US, which are literally and figuratively an ocean apart. Policymakers in the EU and the US were able to set aside these differences in 2000 when they created the Safe Harbor framework, which was developed explicitly to bridge the gap between the differing regulatory approaches taken in the EU and the US.

The European approach to data protection regulation

Largely as a result of the role of data accumulation and misuse in the human rights atrocities perpetrated in mid-twentieth century Europe, the region takes an understandably hard line approach to data protection. The processing of personal data about EU citizens is strictly regulated through Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive is implemented by the member states of the EU, which impose onerous obligations through their national laws regarding the collection, use, sharing and safeguarding of personal data, both locally and extraterritorially.

These extraterritorial considerations are an important component of the data protection regulatory scheme in Europe, as policymakers have no interest in allowing companies to circumvent European data protection regulations simply by transferring personal data outside of Europe. These extraterritorial restrictions are triggered when personal data is exported from Europe to the vast majority of jurisdictions around the world that have not been deemed adequate by the European Commission; chief among them from a global commerce perspective is the United States.

The US approach to privacy regulation

Unlike in Europe, and for its own cultural and historical reasons, the US does not maintain a singular, comprehensive data protection law regulating the processing of personal data. Instead, the US favours a sectoral approach to privacy regulation. As a result, in the US there are numerous privacy laws that operate at the federal and state levels, and they further differ depending on the industry within the scope of the law. The financial services industry, for example, is regulated by the Gramm-Leach-Bliley Act, while the health care industry is regulated by the Health Insurance Portability and Accountability Act of 1996. Issues that fall outside the purview of specific statutes and regulators are subject to general consumer protection regulation at the federal and state level. Making matters more complicated, common law in the US allows courts to play an important quasi-regulatory role in holding businesses and governments accountable for privacy and data security missteps.

The development of the Safe Harbor framework

As globalisation ensued at an exponential pace during the 1990s internet boom, the differences in the regulatory approaches favoured in Europe versus the US became a significant issue for global commerce. Massive data flows between Europe and the US were (and continue to be) relied upon by multinationals, and European data transfer restrictions threatened to halt those transfers. Instead of allowing this to happen, in 2000 the European Commission and the US Department of Commerce joined forces and developed the Safe Harbor framework.

The Safe Harbor framework is an agreement between the European Commission and the US Department of Commerce whereby data transfers from Europe to the US made pursuant to the accord are considered adequate under European law. In order to achieve the adequacy protection provided by the framework, data importers in the US are required to make specific and actionable public representations regarding the processing of personal data they import from Europe. In particular, US importers must comply with the seven Safe Harbor principles of notice, choice, onward transfer, security, access, integrity and enforcement. Not only must US importers comply with these principles, they must publicly certify their compliance with the US Department of Commerce and thus subject themselves to enforcement by the US Federal Trade Commission (FTC) to the extent their certification materially misrepresents any aspect of their processing of personal data imported from Europe.

Since its inception, Safe Harbor has been popular with a wide variety of US companies whose operations involve the importing of personal data from Europe. While many of the companies certified to the framework in the US have done so to facilitate intra-company transfers of employee and customer data from Europe to the US, there are a wide variety of others who have become certified for different reasons. Many of these include third-party IT vendors whose business operations call for the storage of client data in the US, including personal data regarding a client's customers and employees. In the years immediately following the inception of the Safe Harbor framework, a company's participation in the Safe Harbor and the framework in general went largely unnoticed outside the privacy community. In the more recent past, however, that relative anonymity has changed, as the Safe Harbor framework is facing an increasing amount of pressure, primarily from critics in Europe.

Criticism of the Safe Harbor framework begins to mount

Criticism of the Safe Harbor framework from Europe began in earnest in 2010. In a large part, the criticism stems from the perception that the Safe Harbor is too permissive of third-party access to personal data in the US, including access by the US government. The Düsseldorfer Kreises, the group of German state data protection authorities, first voiced these concerns and issued a resolution in 2010 requiring German exporters of data to the US through the framework to employ extra precautions when engaging in such data transfers.

More recently the pressure has intensified and has spread beyond Germany to pan-European concerns at the highest levels of government. This pressure intensified in the wake of the PRISM scandal in the summer of 2013, when Edward Snowden alleged that the US government was secretly obtaining individuals' (including EU residents') electronic communications from numerous online service providers. Following these explosive allegations, regulatory focus in Europe has shifted in part to the Safe Harbor framework, which has been blamed in some circles for facilitating the US government's access to personal data exported from the EU.

As a practical matter, in the summer of 2013, the European Parliament asked the European Commission to examine the Safe Harbor framework closely. Last autumn, the European Commission published the results of this investigation, concluding that the framework lacks transparency and calling for its revision. In particular, the European Commission recommended more robust enforcement of the framework in the US and more clarity regarding US government access to personal data exported from the EU under the Safe Harbor framework.

The future of Safe Harbor

While it is reasonable to predict that there will be refinements of the Safe Harbor framework as a result of these concerns, it remains highly unlikely that the framework will be formally unravelled as some have suggested. In the wake of the PRISM scandal, concerns regarding the US government's access to personal data are certainly valid and relevant. As they pertain to the framework alone, however, they are misguided. The Safe Harbor framework is not unique in its permitting of limited government access to personal data transferred from Europe to the US. Other legal bases that support such cross-border data transfers, including both model contracts and binding corporate rules, similarly permit limited government access to personal data.

A far more likely scenario than a complete unravelling of the framework is increased enforcement of the framework by the FTC and enhanced scrutiny from the US Department of Commerce when companies are certifying, or reaffirming, their compliance with the framework. Beginning earlier this year, the FTC began to increase its enforcement efforts by bringing 13 actions against companies that deceptively represented they were Safe Harbor certified. This approach has continued as the Commission recently brought a similar deception action against the clothier American Apparel, who had let its Safe Harbor certification lapse without making the corresponding changes to its public representations. Similarly, the Department of Commerce, which is responsible for administering the programme, is likely to increase the rigour with which it oversees the programme. While the certification process is a self-certification programme and not subject to formal regulatory approval, an increase in substantive focus from the Department of Commerce during the certification phase and thereafter is likely as a result of the pressure from Europe.

Given the popularity of the Safe Harbor framework and its importance to transatlantic commerce, talk of its demise is premature. More likely is a new and improved Safe Harbor, replete with more rigour from the Department of Commerce on the front-end as well as increased enforcement by the FTC for violations on the back-end. With these enhancements, the Safe Harbor framework is likely not only to survive but persist into the future, providing responsible multinational companies with a legal basis for transferring data from Europe to the US. Global commerce depends on it.

HUNTON& WILLIAMS

Aaron P Simpson **asimpson@hunton.com**

200 Park Avenue, 52nd Floor
New York
New York 10166-0005
United States

Tel: +1 212 309 1000
Fax: +1 212 309 1100
www.hunton.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains and Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Partner of the ABA Section of International Law