The FCPA REPORT

www.fcpareport.com Volume 5, Number 25 December 21, 2016

Data Privacy

Navigating Data Privacy Laws in Cross-Border Investigations

By Deena Coffman and Nina Gross

Conducting a cross-border investigation or performing global due diligence each has its own set of unique challenges, which only become more formidable when coupled with a formal anti-corruption inquiry. In the E.U. in particular, issues range from confusing and often conflicting privacy laws, to language and cultural barriers, to custodian access and local coordination. According to more than half of those who responded to BDO's 2015 Inside E-Discovery Survey, disparate data privacy laws are the biggest challenge to managing cross-border e-discovery. This article provides insight on the data privacy landscape in the E.U. and how to comply with competing demands during a cross-border investigation.

See "Conflicting Compliance Obligations: How to Navigate Data Privacy Laws While Performing Internal Investigations and Promoting FCPA Compliance in the E.U. (Part One of Three)" (Jan. 9, 2013); Part Two (Jan. 23, 2013); Part Three (Feb. 6, 2013).

Technology in Tension With Privacy

The concept of an individual's right to privacy is hardly new. The assertion that Americans have a constitutional right to privacy is supported by legal precedent. Internationally, the right to privacy is enshrined in both the Universal Declaration of Human Rights (which was adopted by the United Nations General Assembly in 1948), and the European Union's Charter of Fundamental Rights (which became legally binding in 2009 as part of the Lisbon Treaty and included the right to respect for a person's "private and family life, home and communications").

While protecting individual privacy is as important as it has ever been, the way technology allows us to store, duplicate, access and distribute information has challenged our ability to protect sensitive information. No longer is locking a file cabinet or setting up basic internal security controls enough. Confidential data is vulnerable not only to theft by bad actors, but also to abuse by entities with authorized access to the data that then use it in a capacity outside its original intent.

Policymakers around the world are quickly modernizing outdated data protection laws for today's fast-paced, digital environment. Most data privacy laws are based on the premise of notice and consent, but during an investigation, notice and consent are not always practical – or even legal.

See our two-part series on data security in China: "Crossing the River by Feeling the Stones (Part One of Two)" (Sept. 14, 2016); and "Performing Due Diligence and Internal Investigations (Part Two)" (Sep. 28, 2016).

Increasing Enforcement Means Increasing Relevance of Disparate Data Privacy Laws

The U.S. government continues to expend significant time and resources on enforcement and compliance, particularly in the anti-corruption realm. The Yates Memo, the Department of Justice's FCPA Pilot Program and the increase in dedicated agents to the FBI's Anti-Corruption Task Force are all encouraging broader enforcement, raising the threshold on what constitutes cooperation credit and strengthening coordination with foreign counterparts. In the DOJ's own words, "FCPA violations that might have gone uncovered in the past are now more likely to come to light." Organizations must step up their international monitoring and compliance efforts and preemptively investigate potential violations to minimize the fallout.

See "Government and Defense Bar Perspectives on the New Weapons in the FCPA Arsenal" and "Top FCPA Officials Encourage Strong Compliance Programs and Remediation, the Defense Bar Responds", both in this issue.

Herein lies the challenge for compliance officers or lawyers: The rules and restrictions governing the collection, processing

and reporting of evidence necessary in any cross-border investigation are dependent on what jurisdictions are involved and where potentially relevant information is based. More than 75 countries or legal jurisdictions have comprehensive national data privacy laws, and U.S. laws are relatively lenient compared to the strict data regimes of many of the countries in which U.S. companies do business.

Unfortunately, these variances in international data privacy law preclude a blanket approach to obtaining data from non-U.S. jurisdictions. Moreover, organizations investigating an allegation of misconduct or performing basic due diligence overseas may inadvertently violate the law in doing so. Often, data privacy laws impose limitations on cross-border data transfers, meaning a U.S. company with data overseas may not be able to move that data to a less restrictive environment. Investigators find themselves caught between a rock and a hard place: Meet U.S. federal prosecutors' high standards for self-reporting and timely disclosure, or comply with the local data privacy regime. Doing both is not always an option.

Because foreign regulations may not be well known (or considered relevant) by U.S. investigators, it's crucial that those tasked with processing discovery data be able to articulate the foreign data privacy restrictions imposed on them so they can avoid the appearance of noncooperation and understand the methods by which such data can be legally made available to them. These restrictions are evolving quickly, particularly in the E.U.

A Cultural Divide

In an ideal world, international regulators would take a collaborative, consensus-based approach to international data privacy laws, not unlike the OECD/G20 Base Erosion and Profit Shifting Program for tax reform. But divergent views on what the "right to privacy" means and what constitutes "protected information" make a single global data privacy standard far-fetched.

The U.S. and E.U. are prime examples of two fundamentally different structures. U.S. courts traditionally use a broad approach to discovery and generally place less value on personal privacy than the E.U.

Consider Americans' relatively apathetic reaction to Edward Snowden's government surveillance revelations. For better or for worse, the impact of the September 11, 2001, terrorist attacks on U.S. soil left Americans generally reconciled with the idea of being constantly monitored – not only by the U.S. government, but also by private entities, which can effectively remove the expectation of privacy via notice and consent upfront. The U.S. has a flexible definition of privacy and it is often traded for assurances of security. For example, two years after the Edward Snowden leaks, according to a Pew research survey, 54 percent of Americans are still opposed to the government collecting bulk phone and internet data on U.S. citizens as part of anti-terrorism efforts, but many generally do support monitoring suspected terrorists.

In Europe, the legacy of the Holocaust during World War II – when individuals were targeted based on personal information and characteristics – has left an indelible mark. European citizens see data privacy as an inalienable right with minimal exceptions.

Consent Under the DPD

The 1995 E.U. Data Protection Directive (DPD) sets forth minimum standards based on seven core principles to govern the "processing of personal data and on the free movement of such data." It is the current law, but is scheduled to be replaced in May 2018 by the General Data Protection Regulation (GDPR), as explained below.

Central to the DPD is the notion of explicit consent: Organizations must provide data subjects the choice to decide at any time whether their personal data may be disclosed to a third party or used for a purpose materially different from the purpose(s) for which consent was originally obtained.

Under the DPD, "personal data" includes any information that can directly or indirectly identify a natural person, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal data can be freely transferred within the European Economic Area and between "Permitted Countries" determined to provide an equivalent or "adequate" level of protection. The United States is not on this list.

U.S. organizations may end up wrestling with E.U. data privacy protections when performing an internal investigation or implementing compliance procedures that require documentation or analysis of international employee or customer data from an E.U. subsidiary. This data may be as simple as a name and email address, but it may also be more sensitive information – such as that included in employment files and email messages – relating to health, financial information or political affiliations. To transfer the pertinent data, the U.S. parent company must follow additional procedures to ensure adequate data protection to the satisfaction of the relevant country data protection authority (DPA).

The DPD does provide legal grounds for processing data based on "legitimate interests," which must be balanced against the interests or fundamental rights and freedoms of the data subject. Derogations for the transfer of sensitive data to third parties without prior consent must meet an even higher bar, limited to conditions where "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims." But how these derogations are applied with regard to law enforcement requests from foreign regulatory authorities and private entities is open to the interpretation of the individual member state. Germany, for example, limits the legal claims exemption to court proceedings, which would exclude internal monitoring and compliance efforts.

Obtaining the individual's consent is the obvious workaround, but it can take time, especially if the individual in question initially refuses or if permission must first be obtained from the local data protection authority. Moreover, consent for one use case does not imply consent in all use cases. An E.U. citizen who gives consent for their personal information to be used in targeted advertisements or offers has not given explicit consent for that data to be used in an investigation. Such consent must be requested in clear language, it must be freely given, the data controller must keep a record of consent, and withdrawal must be as easy as consent. This becomes problematic for obvious reasons in a cross-border investigation where employees may object to the processing of potentially incriminating data.

Currently, discovery teams work to balance E.U. data protection requirements against discovery obligations using a mixture of data minimization, deduplication, redaction and more sophisticated artificial-intelligence-driven data analysis to limit data collection to only the most critical evidence. These case-by-case balancing acts can be nerve-wracking, and many are counting on an earnest, thorough attempt to filter out all non-critical sensitive information as much as possible to provide favor with U.S. and E.U. judges and data protection authorities.

The Next Era of Data Protection

The question of adequacy came to a head in October of 2015 when the Court of Justice of the European Union (CJEU) abruptly invalidated the 15-year-old Safe Harbor Framework, a legal mechanism whereby U.S. companies could self-certify their adherence to the DPD's seven underlying principles. Designed to foster cross-border commerce, Safe Harbor was crucial to streamlining the transfer of personal data for the purposes of litigation and e-discovery. However, the CJEU sided with privacy activists, stating that the existing framework did not adequately protect E.U. citizens' personal data from U.S. government surveillance.

The Privacy Shield

On July 12, 2016, the European Commission determined the E.U.-U.S. Privacy Shield, meant to replace Safe Harbor, met the adequacy standard under the current directive. U.S. companies choosing to self-certify under Privacy Shield voluntarily submit to enforcement by the FTC, Department of Commerce and E.U. DPAs. Many U.S. companies are already subject to FTC enforcement, but the new framework is a more formal structure with specific requirements that arguably increase some aspects of oversight. And while the Privacy Shield further reconciles differences in data privacy protections across E.U. member states, it does not remove all individual member state requirements, particularly in relation to employee personal information.

Self-certification under the Privacy Shield is relatively easy but compliance is a different story and may ultimately prove more burdensome than alternative legal mechanisms, such as Standard Contractual Clauses and Binding Corporate Rules. Organizations need to consider Privacy Shield certification

carefully, as reversing course may not be feasible.

The following offers a high-level overview of alternative legal solutions for facilitating the transfer of personal data in the absence of an adequacy decision or Privacy Shield certification:

1. The data destination country has an adequacy decision in place and its companies can thus access and process data under the current EU Data Protection Directive or, after May 2018, the GDPR, without additional qualifications.
2. The company has Binding Corporate Rules (BCRs) or Standard Contractual Clauses that will support the data transfer.
3. The company has certified its compliance with approved codes of conduct via a mechanism such as Privacy Shield, accompanied by binding commitments.
4. Ad hoc contractual clauses have been approved by DPAs, but approval can require more time than an investigation or litigation allows.
5. The data subject has consented to use of their data in an investigation.
6. The data transfer is necessary for performance of a contract with the data subject.
7. The data transfer is necessary to support the "legitimate interests" of the controller that are not overridden by the rights of the data subject.

See "Key Requirements of the Newly Approved Privacy Shield" (Jul. 27, 2016).

The GDPR Replaces the DPD

Notably, the Privacy Shield, which is subject to joint annual review, was deemed adequate based on the 1995 DPD, which will be replaced by the recently-finalized GDPR that is slated to come into force in May 2018. Whether the Privacy Shield will stand up to the more onerous adequacy requirements of the GDPR remains to be seen.

The GDPR aims to address some of the inconsistencies between member states and will move the E.U. toward becoming a "Single Digital Market." While the regulation provides some much-needed clarity, it also significantly expands the scope and enforceability of the E.U.'s data privacy regime, enabling data protection authorities to levy fines of up to €20 million or 4 percent of annual worldwide turnover for noncompliance.

Perhaps more significantly, the GDPR now holds both the controller and the processor responsible in the event of a data breach. This effectively broadens the territorial reach of the E.U.'s data privacy regime to include any non-E.U. organizations with E.U. "establishments" engaging in "processing activities" in connection with the offering of goods or services to, or monitoring behavior of, European data subjects.

In other words, any business conducting operations in the E.U. could fall under the scope of the GDPR and face the same heavy penalties. This change could have a major impact for those conducting investigations and taking possession of protected data as a "processor," such as when a U.S. law firm or e-discovery service provider collects, processes and hosts data.

The GDPR also intends to further strengthen data protection for individual European citizens – including the "right to be forgotten," originally recognized by the CJEU in its 2014 Google Spain ruling and codified in the GDPR as the right to erasure. Upon receiving an erasure request, controllers must remove the data in question, including all copies and links to it, and inform other controllers about the individual's objection "without undue delay" if the data subject objects to the processing, the data is no longer needed or the processing was not lawful. While the right to be forgotten is not unlimited and must be balanced against, among other things, the public interest and pertinent legal claims, the data controller must honor the erasure request until its legal validity is determined. For investigators, the challenge is that potentially relevant evidence may be temporarily or permanently unavailable – even though that data may be legal in other jurisdictions or the erasure request may ultimately be unwarranted.

In addition to the right to erasure, the GDPR also enhances individual rights to object to automated data processing and provides more stringent conditions for consent as the legal basis for data processing. If consent is withdrawn, controllers must demonstrate a compelling and documented legitimate interest for overriding the individual's right to privacy. The conditions for legitimate interest are virtually equivalent to those stipulated in the current DPD. And, even if a compelling legitimate interest exists that supersedes the requirement for unambiguous consent, the data controller must inform the individual data subject as well as the DPA of the transfer.

Even under the general uniformity and consistency of the GDPR, E.U. member states still have significant room to legislate additional rules and regulations for employee data, which is often the data collected during an FCPA investigation. Some countries are known for aggressive enforcement, while others are not.

The FCPA REPORT

www.fcpareport.com Volume 5, Number 25 December 21, 2016

A Balancing Act

The reality is that the laws governing the use and privacy of information will always struggle to keep up with the pace of changing technology. As a result, technology and the law often seem incompatible. That conflict is further complicated by divergent legal systems and the increasingly global nature of doing business. Companies may think they are caught between deciding which legal risk to take: violating data protection laws, or non-compliance with a U.S. subpoena or discovery requirement.

Processors will want to update their risk models, protocols for handling data, and contract terms and conditions to effectively manage both risks. This may drive more companies to establish "in-country" resources to avoid transporting data across borders and risking a complaint or, worse yet, enforcement at the border. Those companies collecting, transporting, accessing and otherwise processing data that the host country deems protected are well served by engaging local counsel who have experience working with relevant data protection authorities. Ultimately, to make the right decision for their business, organizations must have a full understanding of the consequences domestically and abroad and prove best-effort compliance with both sets of laws.

Deena Coffman is a managing director in BDO Consulting's Technology Advisory Services practice. She has more than 20 years of experience in information security, operations, strategic planning and risk management. Deena has held technology leadership roles involving technology infrastructure, cybersecurity, data privacy, compliance and e-discovery.

Nina Gross leads BDO's global forensics practice in Washington, D.C. She has 30 years of forensic accounting, investigation and consulting experience working with multinational organizations and their counsel as well as significant experience assisting clients in responding to sensitive investigative matters, as well as advising organizations on compliance, due diligence and anti-corruption programs designed to deter and prevent the recurrence of fraud.