DEBEVOISE & PLIMPTON LLP

FCPA Update

July 2014 ■ Vol. 5, No. 12

D.C. Circuit Upholds Privilege Protections in Compliance Investigations

On June 27, 2014, the U.S. Court of Appeals for the D.C. Circuit granted a writ of mandamus and overturned a widely publicized decision by the district court, *United States ex rel. Harry Barko v. Halliburton Company et al.*,[1] which had held that documents relating to an internal investigation conducted by defendant Kellogg Brown & Root Services, Inc. ("KBR") were not protected from disclosure by the attorney-client privilege.[2] In vacating the district court's order to produce the documents at issue, the Court of Appeals concluded that the lower court's analysis was inconsistent with the seminal Supreme Court case *Upjohn Company v. United States*, which held that the attorney-client privilege protects confidential employee communications made during a business's internal investigation led by company lawyers.[3]

In so doing, the Court of Appeals expressly recognized that upholding the District Court's order could well have inhibited internal investigations initiated to review issues arising under the FCPA. In this respect, the decision is an affirmation of the important role played by internal investigations in corporate FCPA compliance efforts.

At the core of the D.C. Circuit's opinion was its articulation of the "primary purpose" test to be used in cases in which an attorney-client communication has multiple purposes. According to the court, the privilege applies if "one of the significant purposes" of the communication was to obtain or provide legal advice.[4] In the context of internal investigations, the court reasoned, the privilege applies so long as obtaining or providing legal advice was one of the significant purposes of the internal investigation, "even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion."[5]

CONTINUED ON PAGE 2

1. No. 1:05-cv-1276, 2014 WL 1016784 (D.D.C. Mar. 6, 2014).
2. *In re Kellogg Brown & Root Servs., Inc.*, No. 14-5055, 2014 WL 2895939 (D.C. Cir. June 27, 2014); *see also* Andrew M. Levine, Andy Y. Soh and Sebastian Ko, *U.S. District Court Limits Privilege Protections in Compliance Investigations*, 5(9) FCPA Update (Apr. 29, 2014), *available at* http://www.debevoise.com/files/Publication/16d38047-f25e-4e68-89e3-8616135248d2/Presentation/PublicationAttachment/10b2fcbc-f6e4-4d04-9d6f-9b4e5e47c84a/FCPA_Update_Apr_2014.pdf.
3. *In re Kellogg Brown & Root Servs., Inc.*, 2014 WL 2895939, at *3 (citing *Upjohn Co. v. United States*, 449 U.S. 383 (1981)).
4. *Id.* at *4.
5. *Id.*

Click *here* for an index of all *FCPA Update* articles.

If there are additional individuals within your organization who would like to receive FCPA Update, please reply to ssmichaels@debevoise.com or pferenz@debevoise.com.

D.C. Circuit Upholds Privilege Protections ■ Continued from page 1

The District Court's Opinion

The underlying case was brought by Harry Barko ("Barko"), a whistleblower plaintiff who had alleged that KBR, Halliburton, and other contractors had overbilled the U.S. government in connection with hundreds of war-zone construction contracts. During discovery proceedings before a magistrate judge, Barko moved to compel KBR to produce certain documents related to KBR's prior internal investigation of the alleged billing misconduct. The investigation had been conducted pursuant to statutory and contractual requirements – imposed on all government contractors – that required KBR to establish and administer a compliance program and conduct internal investigations, and, where necessary, make self-reports of misconduct by its employees. The program was overseen by KBR's Law Department.

KBR opposed the motion, arguing that its investigation was protected by the attorney-client privilege under *Upjohn Company v. United States*, which extended the privilege to communications made by corporate employees to in-house counsel conducting an internal investigation on the company's behalf.[6] After the magistrate judge granted Barko's motion to compel and ordered KBR to disclose the documents, KBR sought review by the district court.

In an opinion issued on March 6, 2014, the district judge upheld the magistrate judge's order, holding that the investigation-related documents were not subject to the attorney-client privilege because KBR failed to show that the communications "would not have been made 'but for' the fact that legal advice was sought."[7] The district court's decision focused on the fact that KBR's compliance program was mandated by regulatory requirements imposed on all government contractors by the Department of Defense. In the court's view, because the investigation would have been conducted in the ordinary course of business, irrespective of whether legal advice was sought or provided, the "primary purpose" of the internal investigation was regulatory compliance and not the obtainment or provision of legal advice.[8]

The district court also distinguished the facts of the case from *Upjohn* by noting that, unlike *Upjohn*: (1) the in-house attorneys did not consult outside lawyers before beginning the investigation;[9] (2) the interviews were generally not conducted by lawyers;[10] and (3) the witnesses interviewed were not expressly informed that the aim of the interview was to facilitate legal advice.[11]

The D.C. Circuit's Opinion

KBR asked the district court to certify the privilege question to the D.C. Circuit for interlocutory appeal. Upon the district court's denial of the request for certification, KBR filed a petition for a writ of mandamus in the D.C. Circuit, which stayed the document

CONTINUED ON PAGE 3

6. *Upjohn*, 449 U.S. at 394.
7. *United States ex rel. Harry Barko v. Halliburton Co.*, 2014 WL 1016784, at *2 (quoting *United States v. ISS Marine Servs., Inc.*, 905 F. Supp. 2d 121, 128 (D.D.C. 2012)).
8. *Id.* at *3.
9. *Id.*
10. *Id.*
11. *Id.*

FCPA Update

FCPA Update is a publication of Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

Moscow
+7 495 956 3858

London
+44 20 7786 9000

Hong Kong
+852 2160 9800

Paris
+33 1 40 73 12 12

Shanghai
+86 21 5047 1800

Frankfurt
+49 69 2097 5000

Paul R. Berger
Co-Editor-in-Chief
+1 202 383 8090
prberger@debevoise.com

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Sean Hecker
Co-Editor-in-Chief
+1 212 909 6052
shecker@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Steven S. Michaels
Executive Editor
+1 212 909 7265
ssmichaels@debevoise.com

Erich O. Grosz
Co-Managing Editor
+1 212 909 6808
eogrosz@debevoise.com

Philip Rohlik
Co-Managing Editor
+852 2160 9856
prohlik@debevoise.com

Erin W. Sheehy
Co-Managing Editor
+1 202 383 8035
ewsheehy@debevoise.com

Noelle Duarte Grohmann
Co-Deputy Managing Editor
+1 212 909 6551
ndgrohmann@debevoise.com

Jane Shvets
Co-Deputy Managing Editor
+1 212 909 6573
jshvets@debevoise.com

Blair R. Albom
Assistant Editor
+1 212 909 6022
bralbom@debevoise.com

Anna V. Maximenko
Assistant Editor
+7 495 139 4014
avmaximenko@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

Please note: The URLs in *FCPA Update* are provided with hyperlinks so as to enable readers to gain easy access to cited materials.

D.C. Circuit Upholds Privilege Protections ■ Continued from page 2

production order pending resolution of the petition. In an opinion issued on June 27, 2014, the circuit court granted KBR's petition and vacated the district court's document production order.

The D.C. Circuit rejected the "but for" test applied by the district court, noting that this "novel approach to the attorney-client privilege would eliminate the attorney-client privilege for numerous communications that are made for *both* legal and business purposes and that heretofore have been covered by the attorney-client privilege."[12] Rather, the correct test is the "primary purpose" test, which, as articulated by the D.C. Circuit, asks whether obtaining or providing legal advice was "a primary purpose of the communication, meaning one of the significant purposes of the communication."[13] The circuit court emphasized that a court should "not draw a rigid distinction between a legal purpose on the one hand and a business purpose on the other," and should not "presume that a communication can have only one primary purpose."[14]

As applied to internal investigations, if one of the significant purposes of the investigation was to obtain or provide legal advice, the privilege will apply under the court's decision, "regardless of whether [the investigation] was conducted pursuant to a company compliance program required by statute or regulation, or was otherwise conducted pursuant to company policy."[15]

The D.C. Circuit also rejected the district court's other attempts to distinguish the case from *Upjohn*. According to the appellate court, *Upjohn* does not require the involvement of outside counsel for the application of the attorney-client privilege, and "[o]n the contrary, the general rule … is that a lawyer's status as in-house counsel 'does not dilute the privilege.'"[16] Even non-lawyers may conduct privileged interviews, provided the non-lawyers are acting as agents of attorneys directing the investigation.[17] Finally, with respect to the fact that KBR did not expressly inform witnesses that each interview was intended to facilitate legal advice, the D.C. Circuit stated that *Upjohn* does not require a company to convey "magic words to its employees" in order to invoke legal privilege for interviews.[18] It was sufficient that KBR's employees knew that the legal department was conducting a sensitive investigation and would protect the information that they disclosed.[19]

> "According to the appellate court, *Upjohn* does not require the involvement of outside counsel for the application of the attorney-client privilege, and '[o]n the contrary, the general rule . . . is that a lawyer's status as in-house counsel "does not dilute the privilege."'"

The Importance of the Decision

As the D.C. Circuit noted, the district court's decision had "generated substantial uncertainty about the scope of the attorney-client privilege in the business setting,"[20] and had "the potential to work a sea change in the well-settled rules governing internal corporate investigations."[21] According to the appellate court, the district court's "novel approach would eradicate the attorney-client privilege for internal investigations,"[22] thereby eviscerating the protections secured by *Upjohn*.

Of particular concern was the potentially chilling effect of the decision on communications made in the course of internal investigations conducted by

CONTINUED ON PAGE 4

12. *In re Kellogg Brown & Root Servs., Inc.*, 2014 WL 2895939, at *4 (emphasis added).
13. *Id.* at *5.
14. *Id.*
15. *Id.*
16. *Id.* at *3 (quoting *In re Sealed Case,* 737 F.2d 94, 99 (D.C. Cir. 1984)).
17. *Id.* (citing *FTC v. TRW, Inc.*, 628 F.2d 207, 212 (D.C. Cir. 1980)).
18. *Id.*
19. *Id.*
20. *Id.* at *1.
21. *Id.* at *7 (internal quotation marks omitted).
22. *Id.* at *4.

D.C. Circuit Upholds Privilege Protections ■ Continued from page 3

businesses required by law to maintain compliance programs. As the D.C. Circuit recognized, given the numerous federal laws that require many companies to maintain internal controls or compliance programs, the district court's approach "would disable *most public companies* from undertaking confidential internal investigations."[23]

> "The district court's opinion, if left undisturbed, could have unnecessarily exposed internal compliance investigations, whether required by law or voluntarily undertaken, to compelled production of documents and giving of testimony in both private and government actions."

The FCPA was one such federal law expressly cited by the D.C. Circuit. Not unlike the regulatory requirement that government contractors maintain compliance programs and internal controls systems,[24] the FCPA requires public companies to "maintain a system of internal accounting controls" in order to ensure management's control, authority and responsibility over company assets.[25] Although not mandated under the law, internal investigations are a standard mechanism by which issuers can, and often do, ensure compliance. The Department of Justice and Securities and Exchange Commission have explicitly recognized the value of such investigations as a potentially effective tool. The *FCPA Guide*, published jointly by the two agencies, advises that compliance programs should include a system for "employees and others to report suspected or actual misconduct" and "an efficient, reliable, and properly funded process for investigating the allegation and documenting the company's response"[26]

The district court's opinion, if left undisturbed, could have unnecessarily exposed internal compliance investigations, whether required by law or voluntarily undertaken, to compelled production of documents and giving of testimony in both private and government actions. In overturning the district court's decision, the D.C. Circuit has enabled companies to continue building and investing in robust compliance programs that include self-investigation of potential regulatory violations under the protection of the attorney-client privilege.

Although the D.C. Circuit's decision is a testament to the judiciary's recognition of the privilege's importance, it may not necessarily reflect the view of every court. To best maintain the privilege, companies should ensure that they meet the other requirements articulated by *Upjohn* and its progeny. Internal investigations should retain a focus on legal compliance, and be monitored carefully by attorneys and executed under their direction. Companies and compliance departments also should consider implementing some or all of the following "best practices":

a. Appointing one or more lawyers (internal or external) to assess and document in writing whether the allegations/issues to be investigated warrant legal involvement, and the extent of legal involvement required;

b. Disseminating written policies that: (i) provide threshold guidance for when attorneys should be involved; (ii) identify clear examples of non-routine matters in connection with which litigation or enforcement proceedings could reasonably be expected (*e.g.*, allegations of fraud, improper payments, etc.); and (iii) flag other situations regularly encountered in the company's operating environment, requiring prompt escalation to the legal department;

c. Identifying one or more lawyers to monitor investigative processes and act as gatekeepers for key investigative decisions (*e.g.*, timeline planning, witness selection, report drafting, and review), regardless of whether the relevant function with overall responsibilities for investigating a given matter is audit, compliance, or legal;

d. Providing *Upjohn* warnings to witnesses interviewed by lawyers, noting that the content of their interviews are

CONTINUED ON PAGE 5

23. *Id.* at *7.
24. 48 C.F.R. 52.203-13 (2010).
25. 15 U.S.C. § 78m(b)(2)(B) (2012).
26. U.S. Dep't of Justice & U.S. Sec. & Exchange Comm'n, *A Resource Guide to the U.S. Foreign Corrupt Practices Act* 61 (2012), *available at* http://www.justice.gov/criminal/fraud/fcpa/guide.pdf.

D.C. Circuit Upholds Privilege Protections ■ Continued from page 4

subject to legal privilege and the duty of confidentiality, both held by and owed to the company.[27]

e. Relying on attorneys to conduct sensitive investigations and supervise non-attorney investigators, with outside counsel retained for the most sensitive, high-risk investigations and consideration of sending "*Upjohn* letters" to non-lawyer investigators to deputize them with powers to act under the direction and supervision of a lawyer, and to include explicitly their work product within legal privilege.[28]

f. Relying on counsel to retain and supervise external experts and investigators.

g. Noting expressly those cases in which investigation reports drafted by non-lawyers are being addressed and sent to counsel expressly requesting legal advice.

h. Labeling appropriately those documents subject to attorney-client privilege and the work-product doctrine, recognizing that the courts are suspicious of over-usage and potential abuse and that these labels therefore should not be applied blindly.

The Court of Appeals's decision unquestionably represents a victory for the protections afforded by the attorney-client privilege, helping ensure that internal investigations remain a viable mechanism for assisting compliance with the FCPA and other laws. Companies and their compliance departments nevertheless should remain vigilant and continue taking conscientious steps to protect privileged and otherwise protected communications made in the course of internal investigations.

Helen V. Cantwell
Andrew M. Levine
Colby A. Smith
Bruce E. Yannett
Steven S. Michaels
Blair R. Albom

Helen V. Cantwell, Andrew M. Levine, and Bruce E. Yannett are partners, Steven S. Michaels is a counsel, and Blair R. Albom is an associate, in the firm's New York office. Colby A. Smith is a partner in the firm's Washington, D.C. office. They are members of the Litigation Department and White Collar Litigation Practice Group. They may be reached at hvcantwell@debevoise.com, amlevine@debevoise.com, casmith@debevoise.com, beyannett@debevoise.com, ssmichaels@debevoise.com, and bralbom@debevoise.com.

27. In *Upjohn*, the Supreme Court held that communications between the in-house counsel and employees of a company could attract legal privilege, but the company controls the privilege as the client-beneficiary of the communications. 449 U.S. at 390-91. Hence, the provision of the *Upjohn* warning has become typical practice in investigations to protect the company's interest in legal privilege vis-à-vis potential third parties, including its employees.

28. *Id.* The provision of *Upjohn* letters can be critical to preserving a company's legal privilege during investigations conducted principally by non-lawyers. It does so by memorializing the purpose of the investigation (*e.g.*, to facilitate the provision of legal advice and the creation of litigation work product, and to maintain confidentiality), and by providing relevant instructions to and conferring authority on the investigators in respect of such purposes.

NEWS FROM THE BRICs

Bringing Money and Data Back to Russia

In the first six months of 2014, Russia has moved ahead on a number of initiatives said to target bolstering the country's national security in the financial and data privacy areas. In the shadow of increased tension between Russia and the West, legislative proposals aimed at "domesticating" funds earned in Russia or by Russian nationals, as well as personal information about Russian nationals, have passed various legislative hurdles and appear to be on their way to enactment. This article provides a brief summary of those initiatives, focusing in particular on their potential impact on anti-corruption compliance efforts of companies and business units operating in Russia.

I. De-Offshorization Initiatives

For reasons often related to tax optimization, the use of offshore structures by Russian nationals and companies have long been an ever-present, and lawful, feature of the Russian business landscape. Notwithstanding the lawfulness of using offshore companies, the offshoring of Russian business unsurprisingly has been subject to much criticism in the Russian national media and among top Russian officials and has been viewed as reducing the country's tax base and undermining Russia's security and its legal regime.[1]

The call for de-offshorization initiatives gained strength starting in 2011, when Vladimir Putin, Russia's Prime Minister at the time, announced that offshorization deprives the Russian government of the right to manage the national economy and constitutes a serious threat to national security.[2] In December 2012, in his annual address to the Federal Assembly, President Putin emphasized the need for a comprehensive set of measures designed to reverse the offshoring of the Russian economy and instructed the government to enact corresponding laws and regulations.[3] He reiterated that view in his 2013 address, and a series of steps aimed at returning to Russia what are seen as Russian businesses was included in the list of 2013 Policy Priorities of the Russian Government.[4]

This spring, the first significant legislative proposals aimed at limiting offshorization were introduced, including amendments to Russian tax law, proposed on March 18, 2014 by the Ministry of Finance, and the National De-Offshorization Plan, adopted in April 2014. In general terms, these de-offshorization proposals aim to remove tax advantages associated with the use of offshore companies and to provide incentives for Russian beneficiaries of offshore structures to abandon them and "repatriate" funds to Russia.[5]

The tax legislation revisions are currently under consideration by the relevant Russian government bodies[6] and may be amended before they come to the floor of the Russian Parliament this summer. The legislation is expected to take effect, in one form or another, on January 1, 2015. The draft legislation has been the subject of much debate and criticism in the Russian business community, which has already resulted in softening of some of its requirements, such as introducing a 3-5 years' transition period, during which some of the legislation's provisions would not apply.[7]

Further, earlier this month, President Putin proposed legislation that would prohibit government officials involved in decisions relating to Russia's sovereignty and national security from opening or

CONTINUED ON PAGE 7

1. *See, e.g.*, Valentin Katasonov, "Russia Does Not Have Its Own Economy," Svobodnaya Pressa, June 19, 2013, http://svpressa.ru/economy/article/69640/.
2. *Id.*
3. Presidential Address to the Federal Assembly, Dec. 12, 2012, http://www.kremlin.ru/transcripts/17118.
4. Main Activities of the Government of the Russian Federation for the Period until 2018, Jan. 31, 2013, http://government.ru/media/files/41d4469723e7e2a0d5b5.pdf.
5. For tax analysis of the draft bill, *see* Debevoise & Plimpton Client Update, "Russian 'De-Offshorization' News: Publication of Draft of Significant Amendments to Tax Law" (Mar. 24, 2014), http://www.debevoise.com/clientupdate20140324a/.
6. *See* http://regulation.gov.ru/project/13067.html?point=view_project&stage=3&stage_id=9140.
7. *See, e.g.*, Anna Vorobyeva, "Deoffshorization Will Be Softer Than MinFin Wanted," News RBK, June 18, 2014, http://news-rbk.ru/econom/print:page,1,21943-deofshorizaciya-proydet-myagche-chem-hotel-minfin.html; Margarita Papchenkova, "Business Achieved Softening of the Anti-Offshore Draft Legislation," Vedomosti, June 18, 2014, http://www.vedomosti.ru/finance/print/2014/06/18/27874951; Irina Chelchinskaya, "Government Will Ask Putin to Delay the Draft Legislation on De-Offshorization," Investcafe, June 18, 2014, http://investcafe.ru/news/46590.

Bringing Money and Data Back to Russia ■ Continued from page 6

> "As it seeks to counteract the offshorization of funds, Russia has also introduced a set of what could be even more controversial initiatives, aimed at counteracting the 'offshorization' of data and information."

holding bank accounts in foreign banks.[8] The proposal builds on a 2013 law that enacted the same prohibition, but applied it to only the most senior government officials, such as heads of ministries and federal agencies. Although the list of officials subject to the new legislation has not yet been published, it is likely to be much broader. The proposed legislation also requires high-level government officials to disclose transactions the aggregate amount of which exceeds the official's income over the past three years, and also applies that requirement to spouses and children of such officials.

Although the results of Russia's de-offshorization efforts remain to be seen, if successful they could have substantial impact on Russia's anti-corruption efforts. First, offshore structures located in jurisdictions with strong confidentiality protections and weak anti-money laundering and related legislation are widely perceived as serving as safe havens for illegally obtained profits, including proceeds from corrupt transactions.[9] If offshorization is indeed curtailed – rather than just driven into ever more complicated ownership structures – it could help reduce corruption or at least make it more difficult for government officials to conceal funds.

Second, and most importantly for companies operating in Russia that seek to abide by Russian and non-Russian anti-corruption laws alike, successful de-offshorization could lead to greater transparency of their Russian business partners, including sales agents, consultants, and other intermediaries. One of the de-offshorization plan's initiatives is to create a register of beneficial owners of all companies operating in Russia, which is intended to allow government authorities and others to obtain reliable information about the ownership of companies. If successful, that would help remedy one of the recurring problems of conducting due diligence on Russian companies, namely the lack of transparency of ownership that can stop a due diligence effort in its tracks.

II. "Domestication" of Data

As it seeks to counteract the offshorization of funds, Russia has also introduced a set of what could be even more controversial initiatives, aimed at counteracting the "offshorization" of data and information. That effort has been advocated by the Russian government as a means to safeguard personal information of Russian nationals and protect Russian national security, but has been criticized by commentators as an attempt to restrict freedom of speech and impose government control on the Internet.

In the latest development on this issue – and the one that may well have a serious impact on non-Russian companies operating in Russia – on July 4, 2014, the Russian Parliament adopted an amendment to the Federal Law No. 152-FZ on Personal Data, which was approved by the Council of Federation on July 9, 2014.[10] If signed by President Putin, the amendment will become effective on September 1, 2016. With certain limited exceptions, the law requires all "personal data operators" to maintain identifying information about their Russian users on servers located in Russia.[11]

Public discussion of the law and arguments for it have focused on information stored at social networking sites, electronic mail services, airline

CONTINUED ON PAGE 8

8. Alexander Ratnikov, "Putin Proposed to Forbid Officials from Opening Accounts Abroad," RBK, June 23, 2014, http://top.rbc.ru/politics/23/06/2014/932098.shtml.
9. *See, e.g.*, Georgy Neyaskin, "How Corruption Attracts Foreign Investment to Russia," Slon.ru, May 6, 2013, http://slon.ru/economics/kak_korruptsiya_prityagivaet_v_rossiyu_inostrannye_investitsii-939089.xhtml; "Study: Cyprus and Its Offshores Are Responsible for Russian Corruption," Rambler: Finansy, June 18, 2013, http://finance.rambler.ru/news/analytics/130261510.html.
10. Legislation No. 553424-6, "On Amendment to Certain Legislation of Russian Federation (in the Area of the Procedure for Processing Personal Data in Information and Telecommunication Networks," http://asozd2.duma.gov.ru/main.nsf/%28SpravkaNew%29?OpenAgent&RN=553424-6&02.
11. *Id.*

Bringing Money and Data Back to Russia ■ Continued from page 7

booking websites, and similar Internet portals that handle personal information of millions of users.[12] The amendment as drafted, however, may have a much broader impact and affect every company in Russia that stores information about its Russian clients or employees, including emails of its employees, on servers that may be located or transferred abroad. For example, a U.S. company operating in Russia that operates a centralized email system located outside of Russia – or that backs up servers located in Russia on foreign servers – can be viewed as within the scope of the legislation and may run afoul of it.

This may present challenges for companies subject to government investigations or inquiries outside of Russia, which may be required to produce to foreign regulators various documents, including emails, of Russian employees. In addition to the already difficult task of complying with the pre-amendment provisions of the existing Law on Personal Data, such companies may need to make sure that the various steps in the data collection and review process take place using or on Russian servers, even when consents of personal data subjects for such collection and review have been obtained.

Further, the sponsors of the legislation have stated that it is aimed at providing an opportunity for Russian nationals to request that their personal data be deleted from search websites and similar services, on the heels of the European Court of Justice's "right to be forgotten" decision. It is not clear whether Russian nationals could take that rationale a step further and request, for example, deletion of their personal data from work emails located on employers' servers, after employment terminates. If so, that would create a further hurdle for the companies operating in Russia that are subject to foreign regulator inquiries, or even to routine corporate disclosure or similar obligations outside of Russia.

De-offshorization and data domestication can be seen as two sides of the same policy coin, aimed at strengthening Russian security and control over its money and data, but the two initiatives may operate at cross-purposes when it comes to efforts by companies operating in Russia to conduct external due diligence or internal investigations. While de-offshorization, if successful, may result in greater transparency of Russian business, data domestication and attendant limitations on companies' ability to handle data of their employees and third parties may further complicate their anti-corruption compliance efforts in Russia and abroad.

Alan V. Kartashkin
Andrew M. Levine
Dmitri V. Nikiforov
Anna V. Maximenko
Jane Shvets

Alan V. Kartashkin and Dmitri V. Nikiforov are partners, and Anna V. Maximenko is an associate, in the firm's Moscow office, and are members of the Corporate Department. Andrew M. Levine is a partner, and Jane Shvets is an associate, in the firm's New York office, and are members of the Litigation Department and White Collar Litigation Practice Group. They may be reached at avkartashkin@debevoise.com, dvnikiforov@debevoise.com, avmaximenko@debevoise.com, amlevine@debevoise.com, and jshvets@debevoise.com.

12. *See, e.g.*, Daria Luganskaya, "Draft Legislation on Transfer of Services with Personal Data to Russia to Be Considered by Russian Duma," RBK, June 24, 2014, http://top.rbc.ru/politics/24/06/2014/932403.shtml?print.