DATA PRIVACY AND THE FOREIGN CORRUPT PRACTICES ACT: A STUDY OF ENFORCEMENT AND ITS EFFECT ON CORPORATE COMPLIANCE IN THE AGE OF GLOBAL REGULATION

Katherine Morga‡

I. INTRODUCTION

There has been a tremendous increase in the extra-territorial enforcement of American laws—where jurisdiction is exercised over offenses occurring outside the United States—over the past several years.[1] Enforcement of securities, antitrust, and several other areas of domestic regulation are now commonly applied to extra-territorial conduct, resulting in a growing amount of transnational litigation.[2] For example, the Dodd-Frank Act grants the Securities and Exchange Commission ("SEC") jurisdiction to charge federal securities violations when certain conduct in connection with foreign securities and foreign exchanges occurs outside of the United States, if such conduct has a "foreseeable substantial effect within the United States."[3] Another salient

‡ J.D. Candidate, May 2013, The Catholic University of America, Columbus School of Law. Katherine would like to thank her family for their love and support, as well as the *CommLaw Conspectus* staff for their hard work and efforts throughout the writing process. A special thanks also to Juan Morillo for providing his expert advice on the topic.

[1] Extraterritorial application of domestic law is said to exist when domestic law is applied to foreigners' conduct that occurs outside of the territorial borders of the domestic state. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 402 (1987).

[2] Austen Parrish, *The Effects Test: Extraterritoriality's Fifth Business*, 61 VAND. L. REV. 1455, 1456 (2008). *See also* Joseph P. Griffin, *Extraterritoriality in U.S. and EU Antitrust Enforcement*, 67 ANTITRUST L.J. 159, 159 (1999) (describing how in both the U.S. and the EU extraterritorial enforcement of antitrust and competition law has become routine).

[3] Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 11-203, § 929P, 124 Stat. 1375, 1862-65 (codified at 12 U.S.C. § 5301). *See also SEC Expands Investigative Reach Under New Extraterritorial Jurisdiction Provisions of the Dodd-Frank Act*, MAYER BROWN (Nov. 11, 2010), http://commcns.org/LwgxVP (explaining the implications of § 929P of Dodd-Frank Act).

example is the increased and globalized nature of Foreign Corrupt Practice Act ("FCPA") enforcement.[4] Part II of this Article analyzes the global nature of regulatory enforcement through a focused review of anti-corruption laws, the current state of U.S. enforcement, and the resulting compliance with these laws.

There is, however, an irreconciled conflict inherent between this trend of increased enforcement and current law governing data privacy protection. While the globalization of external investigations, as well as the resulting performance of preventative internal investigations, represent positive movement towards international enforcement of harmful business activity, serious concerns have been raised over the resulting lack of personal data protection. As enforcement expands to cover companies and employees located outside the United States, these investigations increase the collection and review of personal data that is protected by strict foreign privacy laws. This, combined with the increased ease with which data is created, collected, reviewed, and stored, increases the likelihood that companies may fail to protect personal data privacy, as they frequently face a difficult situation of conflicting compliance requirements. Part III briefly addresses the key developments in communication and data management technology driving this increase in data to emphasize the real possibility that a breach of protection of personal data may occur. As a substantial amount of the increased data created and stored by multinational companies is subject to the EU Data Protection Directive, this section also describes the laws and recent enforcement trends that apply specifically to this category of data.

Part IV of this Article analyzes the inherent tension between the globalization of regulatory enforcement, and its exponential growth, and the resulting effect on data protection. The analysis will review in detail how the gathering of data specifically implicates EU data privacy laws and will navigate the tension to offer practical application of various options and currently available solutions.

---

[4] *Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs of the S. Comm. on the Judiciary*, 111th Cong. 1019-1021 (2010) (statement of Andrew Weissman, Partner, Jenner & Block LLP). The benefits of strong anti-bribery legislation is undisputed amongst the business community, enforcement agencies, and legislators alike, as all support the premise of the FCPA and agree it benefits business by promoting confidence in the global marketplace. *Id. See also* Eric Holder, U.S. Att'y Gen., Remarks at the Organisation for Economic Co-operation and Development, Paris (May 31, 2010), *available at* http://commcns.org/JInchy (pointing to the United States' recent efforts to move towards standards similar to those found abroad).

II. THE GROWTH OF ANTI-CORRUPTION ENFORCEMENT

The current enforcement of anti-corruption regulations provides a relevant example of globalized compliance efforts. As a whole, global enforcement of anti-bribery is on the rise.[5] For example, the United Kingdom recently enacted the Bribery Act of 2010 ("UK Bribery Act"), which codifies an aggressive enforcement approach of a broad range of corrupt behavior.[6] The UK Bribery Act applies broadly to any organization that conducts any "part of a business" in the United Kingdom.[7] Therefore, a company can be held criminally liable for failure to prevent bribery regardless of where it is based, maintains operations, or performs the corrupt act.[8] U.S. authorities believe that "national regulators with a global vision" are needed, which "necessarily entails cooperation, coordination and shared responsibilities" amongst nations.[9]

In the United States, anti-corruption laws date back to the passage of the Foreign Corrupt Practices Act in 1977.[10] The FCPA was instituted in response to a Congressional inquiry into the international business dealings of U.S. companies that uncovered illegal corporate payments in excess of $300 million made in exchange for favorable business dealings.[11] The FCPA was designed

---

[5] DAVID LORELLO & THOMAS BEST, RECENT DEVELOPMENTS IN EU SUGGEST INCREASED 'FCPA-STYLE' ENFORCEMENT OF FOREIGN BRIBERY LAWS 1-3 (2010). U.S. enforcement is at an all-time high, and the recently enacted UK Bribery law provides for what many say is even more comprehensive prosecution of corrupt activity. Enforcement of anti-bribery laws in Germany has increased in recent years, as well. For example, Siemens agreed to pay German authorities close to $1 billion and Truckmaker MAN Group agreed to pay over $200 million to settle various anti-bribery proceedings. *Id.* at 1-2.

[6] Bribery Act, 2010, c. 23 (U.K.).

[7] *See id.* §§ 7, 12(5)-(6). *See also* Jon Jordan, *Recent Developments in the Foreign Corrupt Practices Act and the New UK Bribery Act: A Global Trend Towards Greater Accountability in the Prevention of Foreign Bribery*, 7 N.Y.U. J. L. & BUS. 845, 866 (2011) (discussing the comprehensive nature of the U.K. Bribery Act).

[8] Bribery Act, 2010, c. 23, §§ 7, 12(5)-(6) (U.K.). *See also* Jordan, *supra* note 7, at 866. (discussing how all that is needed for jurisdiction is for a company to conduct any part of its business within the United Kingdom).

[9] Ethiopis Tafara, Dir., Office of Int'l Affairs at the U.S. Sec. & Exch. Comm'n, Address at the British American Business Inc.'s Financial Services Forum: Shared Responsibilities in Global Capital Markets (May 8, 2007), *available at* http://commcns.org/KQ83nQ. *See also* Ethiopis Tafara, Dir., Office of Int'l Affairs at the U.S. Sec. & Exch. Comm'n, Address at Chatham House: Tchaikovsky's Fourth or Monk's Mood: Improvisation and Harmony in Cross-Border Regulation (June 15, 2007), *available at* http://commcns.org/Ky7MsE (discussing the necessity for national officials to have a global outlook).

[10] Foreign Corrupt Practices Act of 1977, Pub. L. No. 95-213, 91 Stat. 1494 (codified as amended in scattered sections of 15 U.S.C.).

[11] United States v. Kay, 359 F.3d 738, 746 (5th Cir. 2004) (citing H.R. REP. NO. 95-640, at 4; S. REP. NO. 95-114, at 3). The "recently discovered but widespread bribery of foreign officials" also raised concerns from a foreign policy perspective, as many defense contractors and oil companies had made payments to foreign government officials, including those of Japan, the Netherlands, and Italy. *Id.*

to hold companies criminally and civilly liable for such illegal acts.[12] Analysis of the provisions, recent enforcement, and efforts to comply with the FCPA provides an appropriate backdrop for further discussion.

A. The Foreign Corrupt Practices Act

The FCPA consists of two main sections: the anti-bribery provisions and the accounting provisions. The anti-bribery provisions prohibit bribery of a foreign government official or a political party for the purpose of obtaining or retaining business, directing business to others, or securing an improper business advantage by inducing behavior or influencing the foreign official's decisions in violation of a lawful duty.[13] These provisions apply to the acts of any issuer, domestic concern,[14] United States citizen, resident, or foreign national acting in the territory of the United States, or any officer, director, employee, agent, or stockholder of any of the above.[15] In addition, the provisions cover wrongful payments to any foreign official,[16] including those of a public international party,[17] foreign political party, candidate for foreign political office, or any person while knowing that all or a portion of the thing of value will be promised or given to one of the individuals listed above.[18]

The accounting provisions require all domestic and foreign corporations with publicly traded securities in U.S. markets to implement accounting controls that ensure visibility of such illicit payments.[19] The provisions require

---

[12] H.R. Rep. No. 95-640, at 4 (1997).

[13] 15 U.S.C. §§ 78dd-1, dd-2, dd-3 (2006).

[14] "Domestic concern" is defined as any individual citizen, national, or resident of the United States, or any "corporation, partnership, association, joint-stock company, business trust, unincorporated organization, or sole proprietorship which has its principal place of business in the United States, or which is organized under the laws of a State of the United States or a territory, possession, or commonwealth of the United States." 15 U.S.C. § 78dd-2(h)(1).

[15] 15 U.S.C. §§ 78dd-1, dd-2, dd-3 (2006).

[16] The FCPA defines "foreign official" as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization." 15 U.S.C. § 78dd-1(f)(2)(A). While not addressed in this Article, exactly who is covered by this definition of "foreign official" has been widely debated, and was a topic of debate before Congress. *See Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 1 (2011).

[17] A "public international organization" is defined as an organization designated by Executive order under the International Organization Immunities Act, or by any other international organization designated by the President by Executive Order. 15 U.S.C. § 78dd-1(f)(1)(B).

[18] 15 U.S.C. §§ 78dd-1(a), dd-2(a), dd-3(a) (2006).

[19] 15 U.S.C. §§ 78m(b)(2), (b)(5). The recordkeeping requirements are not limited to

issuers to devise and maintain accounting practices that will reasonably assure adequate internal controls[20] and are designed to prevent corporations from hiding the existence of bribery payments through accounting devices such as off-book accounts, slush funds, or other creative accounting.[21]

B. Recent Trends in U.S. Enforcement of the FCPA

The U.S. Department of Justice ("DOJ") has recently committed dedicated resources to the enforcement of FCPA, stating that "[f]oreign bribery is a serious crime, and . . . we are investigating and prosecuting it vigorously."[22] Between 2005 and May 2010, the DOJ alone investigated or prosecuted thirty-six corporate FCPA and foreign bribery-related actions and seventy-seven actions against individuals, with fines totaling more than $1.5 billion.[23] Parallel to this increased enforcement activity, cooperation between the United States and the European Union in enforcing regulations has increased as well,

---

suspect FCPA-related transactions, but rather apply to all transactions of the issuer. 15 U.S.C. § 78m(b)(2)(A). Congress amended the act in 1988, largely for clarification purposes, but included a provision granting the DOJ injunctive and subpoena authority over "domestic concerns." *See* Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5003(c), 102 Stat. 1107, 1421 (1988).

[20] Covered entities must also make and keep books, records, and accounts accurately and fairly reflect corporate transactions in reasonable detail. 15 U.S.C. § 78m(b)(2)(A)-(B). The provision defines "reasonable detail" as "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs." 15 U.S.C. § 78m(b)(7). More specifically, the provision requires that the accounting controls are

> sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization; (ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets; (iii) access to assets is permitted only in accordance with management's general or specific authorization; and (iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

15 U.S.C. § 78m(b)(2)(B). The level of detail required for "reasonable assurances" is that which would satisfy a prudent official. 15 U.S.C. § 78m(b)(7). *See also* Jordan, *supra* note 7, at 859 (discussing where reasonable assurance was not found).

[21] Lucinda A. Low et al., *Enforcement of the FCPA in the United States: Trends and the Effect of International Standards*, *in* THE FOREIGN CORRUPT PRACTICES ACT: COPING WITH HEIGHTENED ENFORCEMENT RISKS, at 70 (PLI Corporate Law & Practice, Course Handbook Ser. No. 1588, 2008).

[22] Press Release, Dep't of Justice, JGC Corporation Resolves Foreign Corrupt Practices Act Investigation and Agrees to Pay a $218.8 Million Criminal Penalty (Apr. 6, 2011), http://commcns.org/LXSq4R.

[23] Lanny A. Breuer, Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice, Speech at the Meeting of the Council on Foreign Relations: International Criminal Law Enforcement: Rule of Law, Anti-Corruption and Beyond (Jan. 16, 2012), *available at* http://commcns.org/JpmShB.

demonstrated by increased information sharing and other enforcement assistance.[24]

The DOJ has also increased its focus on individual defendants, charging over fifty individuals with FCPA violations between January 2009 and November 2010.[25] In 2010, the SEC, which shares jurisdiction over anti-corruption enforcement with the DOJ, formed a unit focused specifically on FCPA investigations.[26] As a result, the number of cases investigated has skyrocketed, with the SEC filing 735 FCPA enforcement actions in fiscal year 2011.[27] By itself, the U.S. government's aggressive pursuit of potential FCPA violations would support the argument that prudent companies should provide more stringent preventative measures and prompt response to allegations of

---

[24] Simon Hart et al., REED SMITH, THE IMPACT OF HEIGHTENED FSA/SEC CROSS BORDER COOPERATION (2010). In 2009, the number of times the SEC requested information from foreign regulators increased to 774, a 30% increase over 2008, which had already exceeded any previous year. *Id.* The SEC also receives and cooperates with an increasingly large number of foreign requests for information, over 400 per year in 2008 and 2009. *Id.* In February 2010, the DOJ announced that fifty-six agreements were signed between the United States and the European Union or EU member states to foster increased information sharing or aid in the extradition of individuals charged with transnational crimes. *See* Press Release, Dep't of Justice, U.S./EU Agreements on Mutual Legal Assistance and Extradition Enter into Force (Feb. 1, 2010), http://commcns.org/Jpn2Wm. Seen as a milestone in closing the "gap between the globalization of business and the globalization of business crime enforcement," these agreements represent an increased willingness between regulatory authorities to cooperate across borders. *See* Melissa Aguilar, *U.S., EU Increase Cooperation on Crime Enforcement*, COMPLIANCE WEEK (Feb. 11, 2010), http://commcns.org/JIoDfO (noting the treaties will assist in U.S. and EU investigations of anti-bribery and anti-fraud statutes). The DOJ is also an active participant in the Organisation for Economic Co-operation and Development's ("OECD") Working Group on Bribery, which offers additional opportunities to foster relationships for mutual legal assistance with foreign regulatory authorities. *See Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs of the S. Comm. on the Judiciary,* 111th Cong. 3-4 (2010) (statement of Greg Andres, Acting Deputy Assistant Att'y Gen., Dep't of Justice). Notably, the OECD applauded U.S. authority efforts to investigate and prosecute "the most foreign bribery cases amongst the Parties to the Anti-Bribery Convention." *Id.*

[25] *Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs, of the S. Comm. on the Judiciary*, 111th Cong. 4-5 (2010) (statement of Greg Andres, Acting Deputy Assistant Att'y Gen., Dep't of Justice). At the time of the hearing, there was an additional thirty-five individual defendants awaiting trial or agreements. *Id.* Compared to 2004, when only two individuals were charged with FCPA violations, this represents an unprecedented increase in prosecution of individual offenders. *Id.*

[26] Robert Khuzami, Dir., Div. of Enforcement, Sec. & Exch. Comm'n, Remarks Before the New York City Bar: My First 100 Days as Director of Enforcement (Aug. 5, 2009), *available at* http://commcns.org/KWMrLZ (discussing briefly the objectives for establishing a special unit for FCPA enforcement).

[27] Press Release, Sec. & Exch. Comm'n, SEC Enforcement Division Produces Record Results in Safeguarding Investors and Markets, Agency's Fiscal Year Totals Show Most Enforcement Actions Filed in Single Year (Nov. 9, 2011), http://commcns.org/Jpni7x.

wrongdoing.

Notwithstanding the regularity with which claims are brought or the large dollar sanctions being levied, there is additional cause for corporate concern as the government is using expanded bases to investigate and prosecute FCPA violations. This includes claims brought under the expanded reach of territorial jurisdiction or through the assignment of control person liability to corporate executives who lacked knowledge of wrongdoings.[28]

1. Expanding the Reach of Territorial Jurisdiction

In 1998, FCPA legislation was amended to enable enforcement of the FCPA using extra-territorial jurisdiction, thereby subjecting corporate activities performed outside of the United States to FCPA compliance.[29] Even prior to these amendments, however, foreign companies were subject to FCPA enforcement when wrongful actions could be tied to a territorial jurisdiction or a United States territory.[30] In addition to the above, the U.S. government has recently taken additional steps towards broadening the reach of FCPA enforcement through application of "correspondent account liability"—a concept that appears *de facto* extra-territorial, but in fact is an application of traditional territorial enforcement.[31]

In September 2008, Jack Stanley, the former president of Kellogg Brown & Root LLC ("KBR"), pled guilty to FCPA violations resulting from his

---

[28] Douglas N. Greenburg et al., *Prosecutors Without Borders: Emerging Trends in Extraterritorial Enforcement, in* ENFORCEMENT 2011: MULTI-AGENCY ENFORCEMENT EFFORTS IN THE NEW DECADE, at 1 (PLI Enforcement Practice, Course Handbook Ser. No. 29057, 2011); Melissa Aguilar, *SEC Charges Control Person Liability in Settled FCPA Action*, COMPLIANCE WEEK (Jan. 19, 2011), http://commcns.org/KQ9ySU. *See generally* Complaint, Sec. & Exch. Comm'n v. Nature's Sunshine Prods., Civ. No. 2:09CV0672 (D. Utah July 31, 2009).

[29] *See* Omnibus Competitiveness Act of 1988, Pub. L. No. 100-418, § 5001-5003, 102 Stat. 1107, 1415-25 (1988) (codified at 15 U.S.C. §§ 78m, 78dd-1 to 78dd-3, 78ff (2000)). At the time, there was great concern in the United States and abroad over a collective need to combat bribery of foreign officials. MICHAEL V. SEITZINGER, CONG. RESEARCH SERV., CRS REPORT FOR CONGRESS: FOREIGN CORRUPT PRACTICES ACT (1999). These discussions resulted in the Organization for Economic Cooperation and Development Convention, signed in 1997 by thirty-three member countries, including the most significant world economies. *Id.* at 6. The United States passed the International Anti-Bribery and Fair Competition Act in 1998, amending the FCPA to conform to OECD Convention requirements. *Id.*

[30] Philip Urofsky, *It Doesn't Take Much: Expansive Jurisdiction in FCPA Matters, in* WHITE COLLAR CRIME 2009, at 620-21 (PLI Corps. Law & Practice, Course Handbook Ser. No. 1763, 2009).

[31] INT'L BAR ASS'N, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 11 (2009).

participation in a decade-long bribery scheme.[32] Under this scheme, KBR, through its subsidiary Halliburton, paid over $182 million in bribes to Nigerian government officials in exchange for the award of engineering, procurement, and construction contracts valued in excess of $6 billion.[33] Stanley agreed to a preliminary sentence of eighty-four months in jail and restitution payments of $10.8 million.[34] In 2009, KBR's successor, KBR LLC, pled guilty to violations based on the same set of facts.[35]

While the illegal activities of Stanley, a U.S. citizen, and KBR, a U.S.-based company, were subject to extra-territorial jurisdiction, the U.S. authorities included allegations that implicated the defendants through correspondent account liability.[36] Though it appears extra-territorial in nature, this type of liability is based on territorial jurisdiction applied when a foreign bank transfer, based on a U.S. dollar transaction, was authorized and cleared through a correspondent account at a bank located in the United States.[37] Commentators speculated at the time that U.S. authorities included correspondent account jurisdictional claims in the Stanley and KBR allegations to exert pressure on other entities involved in the scheme that were not subject to traditional means of jurisdiction.[38] Indeed, the following year, the DOJ and SEC brought related

---

[32] Plea Agreement ¶ 1, United States v. Stanley, No. H-08-597, (S.D. Tex. Sept. 3, 2008) [hereinafter Stanley Plea].

[33] Press Release, U.S. Dep't of Justice, Former Officer and Director of Global Engineering and Construction Company Pleads Guilty to Foreign Bribery and Kickback Charges (Sept. 3, 2008), http://commcns.org/JlqfGD.

[34] *See* Stanley Plea, *supra* note 32, ¶¶ 7, 19. Stanley's sentencing is set for June 23, 2012. *See also Stanley's Sentencing Still On Hold [Updated]*, THE FCPA BLOG (Aug. 3, 2011), http://commcns.org/K6GVr2.

[35] Plea Agreement ¶ 1, United States v. Kellogg Brown & Root LLC, No. H-09-071 (S.D. Tex. Feb. 11, 2009). KBR, LLC paid fines of $402 million. *Id.* ¶ 18a. KBR agreed to retain an independent compliance monitor to assist in the implementation of an FCPA compliance program. *Id.* ¶ 18b. Additionally in 2009, Wojciech Chodan, a former KBR employee, and Jeffrey Tesler, a former agent hired by KBR, were charged for their involvement in the FCPA related activity. Press Release, U.S. Dep't of Justice, Two UK Citizens Charged by United States with Bribing Nigerian Government Officials to Obtain Lucrative Contracts as Part of KBR Joint Venture Scheme (Mar. 5, 2009), http://commcns.org/KQahDD. Chodan plead guilty in December 2010, agreeing to pay $726,885 in fines, and currently awaits sentencing of up to five years in prison. Plea Agreement ¶¶ 1, 7, 16, United States v. Chodan, No. H-09-098 (S.D. Tex. Dec. 6, 2010). After fighting extradition from his home in the U.K., Tessler plead guilty in March of 2011, agreeing to forfeit almost $149 million and facing up to ten years in prison. *Jeffrey Tesler Pleads Guilty To Two FCPA Counts*, WSJ BLOG (Mar. 11, 2011), http://commcns.org/KK3H5H. *See also* Plea Agreement, United States v. Tessler, No. H-09098 (S.D. Tex. Mar. 11, 2011).

[36] Stanley Plea, *supra* note 32, ¶ 22. *See generally* Plea Agreement, United States v. Kellogg Brown & Root LLC, No. H-09-071 (S.D. Tex. Feb. 6, 2009).

[37] SHEARMAN & STERLING LLP, THE OTHER FCPA SHOE DROPS: EXPANDED JURISDICTION OVER NON-U.S. COMPANIES, FOREIGN MONITORS, AND EXTENDING COMPLIANCE CONTROLS TO NON-U.S. COMPANIES 2-3 (2010), http://commcns.org/LBMDLR.

[38] *Id.*

charges against a French entity, Technip S.A., and Snamprogetti Netherlands B.V.—both companies involved in the KBR bribery scheme—based solely on correspondent account liability.[39] The pleadings in these matters are the first example of U.S. authorities extending the reach of FCPA to include territorial jurisdiction over foreign corporations whose sole connection to the United States was a foreign bank transfer, conducted entirely overseas, that used a correspondent account at a U.S. bank to clear a U.S. dollar transaction.[40]

Though never challenged in court as a basis for FCPA liability, claims based on correspondent account liability are accepted under other regulatory schemes, and liability applies regardless of whether the foreign company had knowledge of the U.S. bank pass through.[41] Assuming it can withstand judicial scrutiny, correspondent account liability will have a drastic effect on the future of FCPA enforcement, as jurisdiction is now extended to a large number of foreign entities previously thought to have been immune to prosecution.[42]

2. Assigning Liability Without Knowledge: Control Person Liability

Authorities also have shown a new willingness to hold individual employees liable through an expanded view of executive duty. Holding individuals liable for FCPA violations has been the focus of recent hearings in both houses of Congress.[43] In particular, legislators sought assurance that enforcement

---

[39] In June 2010, both companies entered into deferred prosecution agreements based on charges levied by the DOJ and SEC regarding anti-bribery, books and records, and internal controls provisions of the FCPA. Technip will pay $98 million in SEC fines and disgorgement of ill-gotten gains, as well as an additional $240 million penalty based on DOJ criminal charges. Press Release, Sec. & Exch. Comm'n, Technip to Pay $338 Million to Settle SEC and DOJ Charges; Brings Total Sanctions Against Joint Venture Partners to $917 Million (June 28, 2010), http://commcns.org/Kyanmf. Snamprogetti Netherlands (and its parent company) will pay a combined $365 million for DOJ and SEC charges. Press Release, U.S. Dep't of Justice, Snamprogetti Netherlands B.V. Resolves Foreign Corrupt Practices Act Investigationand Agrees to Pay $240 Million Criminal Penalty (July 7, 2010), http://commcns.org/KQaSVL.

[40] *See* Urofsky, *supra* note 30, at 619, 623. In a past FCPA action against Siemens AG, authorities had skirted the idea that funds transferred through correspondent accounts provided ample jurisdiction, but the claim was largely *dicta*. *Id.* at 623-24. Distinguishable from the Technip and Snamprogetti actions, however, the SEC alleged several other schemes based on clear territorial jurisdictional facts. *Id.* at 623. As such, Technip S.A. and Snamprogetti are the first FCPA defendants charged solely on correspondent account liability. *Id.* at 624.

[41] *See* SHEARMAN & STERLING, *supra* note 37, at 3.

[42] *Id.*

[43] *See, e.g., Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs of the S. Comm. on the Judiciary*, 111th Cong. 5-6 (2010) (statement of Hon. Greg Andres, Acting Deputy Assistant Att'y Gen.) (responding to concerns that the DOJ has yet to charge any individuals in the United States with respect to the Siemens matter).

techniques provide effective deterrence, while numerous commentators argued that increased prosecution of individual defendants would discourage the corporate justification of bribery as a "cost of doing business."[44] Though holding executives liable for their role in corporate wrongdoing is a deterrence strategy employed in the enforcement of numerous corporate governance regulations, it is a relatively recent trend for FCPA enforcement.[45]

Under the FCPA accounting provisions, an actor may not be held criminally liable if he lacked knowledge that his actions were unlawful.[46] Specifically, statutory language prohibits application of criminal liability unless the person "knowingly circumvents or knowingly fails to implement" accurate and reasonable accounting controls.[47] While the accounting provisions contain no similar knowledge element for civil liability, commentators have noted that, generally, the SEC has "limited itself to pursuing executives who had direct knowledge of payments to foreign officials or of the misreporting of such payments in their companies' books."[48] However, this historical view of a

---

[44] *Id.* at 67-68 (statement of Mike Koehler, Assistant Professor of Business Law at Butler University (quoting John Keeney, former Deputy Assistant Att'y Gen. of the United States)). Additionally, the business community has expressed concern that the lack of FCPA case law or guidance has left U.S. companies feeling vulnerable without the ability to protect themselves against liability. *Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) (statement of Rep. Jim Sensenbrenner, Chairman, Subcomm. on Crime, Terrorism, and Homeland Security). Interestingly, Assistant Attorney General Lanny Breuer announced that the DOJ is developing a "lay person's guide" to the FCPA and intends to "release detailed new guidance on the Act's criminal and civil enforcement provisions" in 2012. Lanny Breuer, Assistant Att'y Gen., Speech at the 26th National Conference on the Foreign Corrupt Practices Act (Nov. 8, 2011), *available at* http://commcns.org/K6HVeU.

[45] *Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs of the S. Comm. on the Judiciary*, 111th Cong. 4 (2010) (statement of Hon. Greg Andres, Acting Deputy Assistant Att'y Gen.) (noting that the DOJ has charged over 50 individuals with FCPA violations since January of 2009, while only two individuals were charged with FCPA violations in 2004).

[46] 15 U.S.C. § 78m(b) (2006).

[47] *Id.* § 78m(b)(4)-(5).

> The Conferees agreed that "simple negligence" or "mere foolishness" should not be the basis for liability. However, the Conferees also agreed that the so-called "head-in-the-sand" problem—variously described in the pertinent authorities as "conscious disregard," "willful blindness" or "deliberate ignorance"—should be covered so that management officials could not take refuge from the Act's prohibitions by their unwarranted obliviousness to any action (or inaction), language or other "signaling device" that should reasonably alert them of the "high probability" of an FCPA violation.

SEITZINGER, *supra* note 29, at 4 (quoting H.R. Rep. No. 100-576, at 920 (1988)).

[48] Jordan, *supra* note 7, at 859-60 (citing Mary C. Spearing et al., New Developments in FCPA Enforcement: What it All Means, Address Before the Am. Bar Ass'n: 24th Annual Nat'l Inst. on White Collar Crime (Feb. 25, 2010)). *See also* S.E.C. v. McNulty, 137 F.3d 732, 740-41 (2d Cir. 1998) (holding that scienter is not a prerequisite to civil liability under

limited application of the accounting provision to civil liability has been questioned as a result of a recent SEC action brought against corporate executives who seemingly lacked direct knowledge of such violations.[49]

In *SEC v. Nature's Sunshine Products, Inc.*, the SEC not only showed a renewed willingness to apply liability without knowledge, but also for the first time assigned "control person liability" to an FCPA defendant, binding the inaction of a corporate executive to the wrongful actions of the corporation.[50] In this matter, the SEC filed a settlement enforcement that charged Nature's Sunshine Products, Inc. ("NSP") and two of its senior executive officers with violations of the FCPA's anti-bribery and accounting provisions.[51] Between 2000 and 2001, NSP made cash payments totaling over $1 million to Brazilian customs brokers, which were later paid to Brazilian officials, for the unregistered importation of products to be sold by an NSP subsidiary located in Brazil.[52] These payments went undocumented and the company books were falsified.[53]

However, the SEC did not allege, nor do the facts appear to support, that the executives had knowledge of the wrongful bribes.[54] Rather, the SEC asserted that the executives had supervisory responsibilities for the management policies at the company and, therefore, violated the accounting provisions of the FCPA because they "failed to adequately supervise" company personnel in relation to enforcement of the accounting provisions.[55] Assigning "control person liability," the SEC alleged the executives violated the accounting provisions of the FCPA without alleging an affirmative act or knowledge of the underlying wrongful payments.[56]

---

the FCPA because the 1998 amendments to 15 U.S.C. § 78m(b), providing that knowing falsification is required, are limited in application to criminal liability). The absence of discussion of scienter for civil liability plainly implies no such standard is necessary. *Id.*

[49] Jordan, *supra* note 7, at 856-57.

[50] Claudius O. Sokenu, *FCPA News and Insights: An Update on Recent Foreign Corrupt Practices Act and Global Anti-Corruption Enforcement, Litigation, and Compliance Developments*, *in* THE FOREIGN CORRUPT PRACTICES ACT 2010, at 641, 647 (PLI Corp. Law & Practice, Course Handbook Series No. 1814, 2010).

[51] Complaint at 9, 12, 13, SEC v. Nature's Sunshine Prods., Inc., No. 2:09-CV-00672-BSJ (D. Utah July 31, 2009). The claim also alleged violations of other federal security laws. *Id.* at 9-13.

[52] *See* Jordan, *supra* note 7, at 858.

[53] *Id.* at 858-59.

[54] *Id.* at 857.

[55] *Id.* at 859.

[56] "Control person" liability is defined under Section 20(a) of the Exchange Act:

> Every person who, directly or indirectly, controls any person under any provision of this title or of any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable, unless the controlling person acted in good faith and did not directly or indirectly induce the act or acts constituting the

It is yet to be determined if control person liability for FCPA violations is an exception or a reality.[57] While control person liability is a relatively new basis for assigning liability in FCPA matters, it has been used in finding liability in other general corporate fraud cases, and furthers the trend for holding more individuals liable for FCPA offenses.[58] Regardless of its new status, as commentators have noted, it stands as a warning that authorities are not limited to prosecuting individuals with direct involvement in or knowledge of an underlying wrongful act, but rather include the actions of those who "fail[ed] to adequately supervise employees responsible for maintaining the company's books and records and system of internal controls."[59]

III. BALANCING THE INCREASE IN PERSONAL DATA COLLECTION WITH EMERGING PRIVACY ISSUES

Given the increased globalization of business, a continued trend of expanded FCPA enforcement is likely. Corresponding advances in computer and electronic technology, which allow for such globalization, also present important concerns for FCPA enforcement. Business continues to span borders, in large part due to extended connectivity reaching even the most remote corners of the world.[60] The ease of data sharing across offices, states, countries, and continents has been essential to this growth. One example is the increased adoption of cloud computing, which provides the ability to store data remotely over the Internet, rather than on a physical network or personal desktop computer.[61] Cloud computing offers many efficiencies and advantages, especially for transnational companies.[62] Additionally, cloud computing

---

violation or cause of action. 15 U.S.C. § 78t(a) (2006).

[57] Claudius O. Sokenu, *FCPA Compliance Issues in the Global Marketplace: New Challenges for Multinational Clients*, *in* FOREIGN CORRUPT PRACTICES ACT COMPLIANCE ISSUES 7 (2010). The matter was settled out of court; neither NSP nor either executive admitted or denied the allegations of the complaint, but consented to the entry of final judgment and the payment of civil fines. Press Release, Sec. & Exch. Comm'n, SEC Charges Nature's Sunshine Products, Inc. with Making Illegal Foreign Payments (July 31, 2009), http://commcns.org/L86009.

[58] Sokenu, *supra* note 50, at 641, 647.

[59] *See* Jordan, *supra* note 7, at 860 (quoting Abigail Arms, *Discussion Points: SEC Update and Priorities*, *in* PREPARATION OF ANNUAL DISCLOSURE DOCUMENTS (14TH ANNUAL), at 69, 83 (PLI Corporate Law & Practice, Course Handbook Ser. No. 1778, 2009)).

[60] Brahima Sanou, *Championing the Power of Connectivity in Africa*, 2 CORPORATE AFRICA, Issue 54 (2011) at 170, 10-11 (noting that broadband is "a major enabler of social and economic change, a key driver of development" and that the ability to communicate is a strong driver in the growth and development of commerce in third-world nations).

[61] William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1199 (2010).

[62] For example, review of documents can be performed remotely as files can be shared

provides a cost-efficient data management tool, as it is less labor- and software-intensive than other forms of data storage and provides virtually unlimited storage space.[63]

Communication technologies enable great progress in the global marketplace, but also create concerns over exchanges of data and the potential for breaches of personal privacy.[64] With cloud computing, consumers, especially foreign individuals and businesses accustomed to strict data controls, question the lack of privacy protections available when using such technology.[65] Regulators, too, are concerned.[66] The U.S. Department of Commerce issued a report stating that a lack of protection could threaten "the adoption of new technologies by worried consumers and the ability to have international data sent to the U.S."[67] The French data authority, the Commission nationale de l'informatique et des libertés ("CNIL"), launched a public consultation open to all clients, providers, and consultants to consider solutions to the cloud-based privacy problem.[68] Neelie Kroes, the European Commission Vice-President for the Digital Agenda, acknowledged that cloud computing may indeed become a "backbone of our digital future," but expressed concerns over potential inadequacies in personal data protection and invited conversations to ensure that users' fundamental rights and freedoms of data privacy are protected.[69]

A. Data Protection Initiatives

To protect information shared in these advancing communication technologies, data privacy laws restrict or prohibit the transfer of personal data outside of a country or region.[70] While the U.S. federal government and several

---

real-time through the cloud. *See* Christian Arno, *The Advantages of Using Cloud Computing*, CLOUD COMPUTING J. (Apr. 14, 2011), http://commcns.org/Knf7Nc.

[63] *Id.*

[64] VIRGINIA BOYD, FINANCIAL PRIVACY IN THE UNITED STATES AND THE EUROPEAN UNION: A PATH TO TRANS-ATLANTIC REGULATORY HARMONIZATION, 3 (Apr. 29, 2005) (unpublished Select Papers from the Seminar in International Finance, Harvard Law School), *available at* http://commcns.org/JwLtWD.

[65] Paul Taylor, *Privacy Concerns Slow Cloud Adoption*, FINANCIAL TIMES (Aug. 2, 2011), http://commcns.org/Lwopqi.

[66] *Id.*

[67] Justin Brookman, *Why the U.S. Needs a Data Privacy Law—and Why It Might Finally Get One*, ARS TECHNICA (July 18, 2011), http://commcns.org/KzRek8.

[68] Press Release, Comm'n Nationale de l'Informatique et des Libertés, Cloud Computing: CNIL Opening Debate (Oct. 19, 2011), http://commcns.org/K6JF7J.

[69] Neelie Kroes, Vice President for the Digital Agenda, European Comm'n, Address at Les Assises du Numérique Conference, Université Paris-Dauphine (Nov. 25, 2010), *available at* http://commcns.org/KWvTQr.

[70] Stephen R. Reynolds, *Management of International Litigation*, *in* INTERNATIONAL LITIGATION 2010, at 409, 414 (PLI Litig. & Admin. Practice, Course Handbook Ser. No.

U.S. states have enacted sector-specific laws primarily protecting highly sensitive data like health and financial information, the United States lacks a comprehensive data privacy law.[71] In contrast, foreign data protection laws across the globe—in the EU, Canada, Australia and Argentina, for example—are much more comprehensive, covering broader ranges of personal data, including data which "identifies a person's physical, physiological, mental, economic, cultural, or social identity . . . ."[72] However, as global markets expand, national borders, from the business perspective, are blurred, forcing U.S. companies to comply with multiple foreign regulations. The EU's regulation of personal data privacy, and the resulting national enforcement, provides an excellent example.[73]

1. The EU Data Protection Directive

In 1995, the EU passed Data Protection Directive 95/46/EC ("the Privacy Directive"), which protects the privacy rights of EU citizens by limiting the collection or transfer of personal data to restricted circumstances.[74] The Privacy Directive was developed based on rights recognized in the European Convention for the Protection of Human Rights and Fundamental Freedoms, and is intended to protect the free flow of data while providing express recognition of an individual's right to protect personal data.[75] All EU Member States, as well as other countries in the European Economic Area ("EEA"),

826, 2010).

[71] *Id. See also* Brookman, *supra* note 67 (noting Congress' recent interest in enacting a law, and citing the United States and Turkey as the only developed nations in the world without comprehensive law protecting consumer privacy).

[72] *See* Reynolds, *supra* note 70, at 409, 414-16 (noting that "every day brings news of other non-EU countries toughening their existing data privacy laws or enacting new laws.").

[73] For example, in March 2011, France's data protection authority, CNIL, found that Google breached French data privacy law while collecting data for the search engine's "Street View" function. Press Release, Comm'n Nationale de l'Informatique et des Libertés, Google Street View: CNIL Pronounces a Fine of 100,000 Euros (Mar. 21, 2011), http://commcns.org/MT7obm. Data privacy violations included Google's inadvertent collection of Wi-Fi data without data subject knowledge and the recording of user content data, such as passwords, login details, email exchanges and website connection data. *Id.*

[74] *See generally* Council Directive 95/46/EC, 1995 O.J. (L 281) (EU) (enforcing privacy rights within the European Community) [hereinafter Privacy Directive]. *See also* Breon S. Peace & Jennifer A. Kennedy, *The Impact of EU Data Protection Laws on U.S. Government Enforcement Investigations*, 18 No. 1 INT'L HR J., art. no. 2, (2009) at 1, 4. There are currently 27 Member States in the European Union: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom. *Id.* at n. 3.

[75] Privacy Directive, *supra* note 74, preamble, art. 1

must adopt the minimum requirements set out by the Directive.[76] National laws do, however, vary in application and practice.[77] As such, corporations operating in multiple EU/EEA countries must understand and comply with the varying levels of data protection.[78]

The Directive generally restricts the processing and transfer of personal data that relates to an identified or identifiable "data subject."[79] Personal data includes identifying factors specific to a person's physical, physiological, mental, economic, cultural or social identity.[80] This type of information is commonly collected by employers and corporations for the day-to-day functioning of businesses, in data such as name, address, birthday, religious or political affiliation, employment information or job title, credit information, photographs, criminal records and computer IP addresses.[81]

Strict controls apply to the treatment of personal data, including restrictions

---

[76] Peace & Kennedy, *supra* note 74, at 1. The Agreement on European Economic Area (EEA), signed in 1992 and effective since 1994, is between European Free Trade Association (EFTA) countries—currently Iceland, Liechtenstein and Norway—and the European Economic Community (later transformed into the EU). LOUIS ALTMAN & MALLA POLLACK, CALLMANN ON UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES 28-3, 28-5, 28-7 (4th ed. 2009 & Supp. 2011). The agreement grants participating EFTA countries free movement of people and goods across EU countries, and requires participation in EU competition rules. *Id.* at 28-7. While a member of EFTA, Switzerland, is not an EEA member. Peace & Kennedy, *supra* note 74, at 6 n.4. However, a bilateral agreement between the country and the EU provides Swiss citizens with similar privacy rights protection. *Id.*

[77] Privacy Directive, *supra* note 74, art. 5. Unlike EU regulatory legislation, which becomes immediately enforceable as law, a directive provides minimum guidelines that each member state is required to meet through state-specific enforcement. Consolidated Version of the Treaty on the Functioning of the European Union art. 288, 2010 O.J. (C 115) 171-72 ("A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.").

[78] One aim in enacting the Privacy Directive was to ensure all EU citizens' received similar levels of protection and privacy rights while diminishing obstacles to the free flow of information or other burdens to business and citizens alike. THE GALLUP ORG., DATA PROTECTION IN THE EUROPEAN UNION, DATA CONTROLLERS' PERCEPTIONS, ANALYTICAL REPORT 4 (2008), http://commcns.org/KWRgVG. However, data controllers—in many cases, the corporate controller of employee personal data—perceive disparities in the enforced level of protection across the EU. *Id.* at 6, 10.

[79] Privacy Directive, *supra* note 74, art. 2.

[80] *Id.* Determinations for the processing of special categories of personal data is treated separately, and processing of sensitive data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life, generally should be prohibited. *Id.* at art. 8(1). Data relating to criminal offenses or convictions may be processed only under the control of official authority or safeguards. *Id.* at art. 8(5).

[81] Peace & Kennedy, *supra* note 74, at 1. Data remains "personal" for regulatory purposes even when obtained from a public source, including the Internet. *Id.* The Directive requires personal data restrictions apply to all natural persons; however, several countries have extended protection to deceased persons or business entities. *Id.*

on the processing of data wholly or partly by automatic means.[82] The Directive defines "processing" broadly as any operation performed on personal data, including but not limited to the collection, recording, organization, altering, retrieval, destruction, transmittal, or dissemination of the data.[83] Restrictions also apply to processed data that is stored as part of a filing system, electronic or otherwise, including systems that are dispersed on a functional or geographic basis, when data is accessible according to specific criteria.[84]

For example, restrictions apply to the electronic consolidation of employee personal data such as compensation levels, professional skills, and personal preferences by a multinational corporation for the administration of global human resource management, or to the review of emails sent from an employee account on a workplace email system.[85] A common example of this would be maintenance of a human resource management database. Depending on the nature of the data and the proposed purpose cited for its collection and use, acceptable processing of personal data is often limited in scope and must be in accordance with the national law where the collection occurs.

a. Legitimacy of Processing

To ensure privacy is protected, the Directive charges data controllers with ensuring personal data is justified as "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[86] Data must be "processed fairly and lawfully . . . [and] collected

---

[82] Privacy Directive, *supra* note 74, art. 3.

[83] *Id*, art. 2(b). The Directive does not apply to data that "falls outside the scope of Community law . . . ." *Id.* art. 3.

[84] *Id.* art. 2(c).

[85] *See, e.g.*, Ieuan Jolly, *European Union: Europe Clamps Down On Data Protection Violations: U.S. Multinational Fined For Cross-Border Data Transfer, in* MONDAQ BUSINESS BRIEFING 1-2 (2007) (reporting that CNIL fined Tyco Healthcare for improper implementation of a global human resource database for the cross-border management of personnel that resulted in data privacy violations). *See also* Beryl A. Howell & Laura S. Wertheimer, *Data Detours in Internal Investigations in EU Countries: Part I, in* METROPOLITAN CORP. COUNS. 30 (2008) (discussing a French Supreme Court finding an employer erred in reviewing employee email because the employee had a right to privacy at his place of work).

[86] Privacy Directive, *supra* note 74, art. 6. Data processing is legitimate under the following circumstances: (1) the data subject provided unambiguous consent; (2) processing under a contract to which the data subject is party, at the data subject's request or out of necessity for contract performance (3) processing is necessary for compliance with a legal obligation of a Member State; (4) when processing will protect the vital interests of the data subject; (5) it is necessary for performance of a task carried out in the public interest or in the exercise of official authority; or (6) processing is necessary for the purposes of the legitimate interests pursued by an interested party, except where such interests are overridden by the fundamental rights of the data subject. *Id.*, art. 7.

for specified, explicit and legitimate purposes, and not be used for incompatible purposes."[87] Additionally, the data may not be retained longer than necessary and must be accurate.[88] Data subjects must be informed when personal data is collected for a third party's use,[89] and they retain the right to access the data in order to check its accuracy and rectify incorrect information.[90]

b. Transfers of Personal Data

Once it is established that data processing is legitimate, personal data may be transferred freely across the national borders of the EU/EEA member countries.[91] Additionally, where the European Commission has identified that a third country regulates data privacy with adequate protection through domestic law and international commitments, the Directive allows for a flow of data similar to that within EU countries.[92] The laws and commitments of the United States, however, do not meet the standards for adequate protection.[93]

The transfer of personal data located in an EU/EEA member state to one lacking adequate data privacy controls is prohibited by the Directive. Nevertheless, transfer is permitted in specific circumstances as set out by the EC.[94] Under limited circumstances, a data controller may adopt corporation- or contract-specific controls that, in place of country-wide protections, provide adequate controls for the protection of the transferred data.[95] Set out in Article

---

[87] *Data Protection Working Party Opinion 1/2006 on the Application of EU Data Protection Rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime*, at 8, 00195/06/EN (2006) WP 117 (Feb. 1, 2006) [hereinafter WP 117].

[88] Privacy Directive, *supra* note 74, art. 6.

[89] *Id*, art. 11.

[90] *Data Protection Working Party Working Document on Pre-Trial Discovery for Cross Border Civil Litigation*, at 12, 00339/09/EN (2009) WP 158 (Feb. 11, 2009).

[91] Privacy Directive, *supra* note 74, preamble.

[92] *Id.*, art. 25. The power to determine adequacy of protection has been delegated to the European Commission, and any such determinations are binding on EU/EEA member states. *Id.* Data protection in the following countries has been deemed adequate: Switzerland, Canada (though, limited to transfers made to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act), Argentina, the Bailiwick of Guernsey, the Isle of Man, the Bailiwick of Jersey. *See* Reynolds, *supra* note 70, at 415.

[93] *See* Reynolds, *supra* note 70, at 415.

[94] "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 within the scope of a Safe Harbor agreement or by respecting Binding Corporate Rules." ORLA LYNSKEY ET AL., RAND EUROPE, E-DISCOVERY AND LEGAL FRAMEWORKS GOVERNING PRIVACY AND DATA PROTECTION IN EUROPEAN COUNTRIES: IMPLICATIONS 6 (2010), http://commcns.org/KydGtA.

[95] *Id.* at 21.

26(2) of the Directive, these circumstances include the use of protective measures such as safe harbor agreements, model contracts or standard contractual clauses, and binding corporate rules.[96]

The options available for data transfer discussed thus far are preferred, as each establishes adequate levels of protection. If these options are truly impractical or infeasible, data controllers may consider using the provisions of Article 26(1).[97] Provided the controlling member state's data authority finds it acceptable, a transfer may take place if one of the following conditions is met: (1) the data subject has given unambiguous consent; (2) the transfer is required on important public interest grounds for the exercise or defense of legal claims; (3) the transfer is necessary to protect the vital interests of the data owner; (4) the transfer is necessary under a contract; or (5) for the exercise or defense of legal claims.[98]

2. *EU Enforcement of Data Protection*

The Directive undoubtedly increased treatment of data privacy protection to a consistently high standard across the EU.[99] Even so, compliance with the Directive standards can be challenging as member state regulations differ greatly in both form and application.[100]

The Working Party, the lead advisory body for issues arising related to the Directive, calls upon member states to strictly enforce data privacy laws.[101] In particular, it states that compliance with U.S. laws or government investigations does not qualify as a legal obligation whereby the processing of data would be legitimate.[102] For example, the Working Party reviewed personal

---

[96] Privacy Directive, *supra* note 74, art. 26.

[97] *Id.*

[98] *Id.* The Directive states that each member state may define these qualifying circumstances differently.

[99] In fact, anticipated amendments to the Directive highlight the need for increased protection, particularly in areas surrounding data owner consent, and a belief that "consumers must be more empowered than they are today." Viviane Reding, Vice President, European Comm'n, Address in Brussels: Stronger Data Protection Rules at EU Level (Nov. 7, 2011), *available* at http://commcns.org/JItGZ4.

[100] Viviane Reding, Vice President, European Comm'n, Address at European Business Summit: The Reform of the EU Data Protection Directive: The Impact on Businesses (May 18, 2011), *available at* http://commcns.org/L87S9b (recognizing that "[f]irms handling personal data in several Member States are currently subject to different decisions in different Member States . . . [which] creates legal uncertainty and costs," and stating her intent to simplify and increase harmonization amongst EU laws).

[101] Privacy Directive, *supra* note 74, preamble.

[102] *Id. See also* WP 117, *supra* note 87, at 5. For example, in discussing the whistleblowing provision of the U.S. Sarbanes-Oxley Act and the resulting requirement for data collection, the Working Party acknowledged that U.S. companies and European companies listed in U.S. stock markets face "risks of sanctions from EU data protection

data that was transferred from the Society for Worldwide Interbank Financial Telecommunication ("SWIFT"), a corporation based in Belgium that facilitates international money transfers, to the U.S. Treasury.[103] These transfers were in response to post-9/11 subpoenas from the U.S. Treasury requiring SWIFT to provide access to information held at its U.S. operation center.[104] The Working Party determined that SWIFT acted in violation of the Directive because transfer of personal data by SWIFT to the U.S. Treasury did not meet the "necessity test," requiring a substantial connection between the transfer's purpose and the data subject's interests, and was without legal grounds and/or adequate protection by supervisory authorities.[105]

While there are no documented cases where the collection of data has been prohibited by member state data authorities for FCPA investigations or enforcement measures, member states have imposed strict enforcement and penalties for the breach of data privacy laws. As an example, 2009 amendments to the German Federal Data Protection Act provide that German data protection authorities may order cessation of the collection or processing of data and fines of up to €300,000 for violations of local law.[106] In addition, several States have enacted blocking statutes that explicitly prevent disclosure of certain categories of information and entail harsh criminal sanctions for its transfer abroad.[107]

CNIL has consistently stated its view that the protection of personal data is of highest priority. In 2008, CNIL issued a memorandum on the protection of data during U.S. civil litigation, particularly concerned with copies of employees' hard drives and e-mail folders.[108] In its annual report, released in July 2009, CNIL commented on a recommendation it made in response to requests for guidance from French companies implicated in U.S. litigation.[109] In

---

authorities . . . on the one hand, and from U.S. authorities if they fail to comply with U.S. rules, on the other." *See also* Jacqueline C. Wolff & Daniel P. Cooper, *FCPA Due Diligence and Data Privacy Laws, How to Reconcile the Irreconcilable,* BUS. CRIMES BULLETIN, Nov. 2008, at 1, 2 (stating "[c]ollecting information to comply with U.S. laws" is not one of the limited grounds for legitimate collection of personal data).

[103] *Working Party Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, at 2, 01935/06/EN, WP 128 (Nov. 22, 2006).

[104] *Id.*

[105] *Id.* at 2, 23-24. (reiterating its view that "even in the fight against terrorism and crime fundamental rights must remain guaranteed").

[106] Katharina A. Weimer, *The German Federal Data Protection Act and Its Recent Changes*, BNA INT'L: WORLD DATA PROTECTION REP., Sept. 2009, at 5, 7.

[107] Most notable are France and Switzerland's blocking statutes. Lynskey, *supra* note 94, at 21, 28.

[108] MARK E. SCHREIBER & ALEXANDRA RADCLIFFE, EDWARDS ANGELL PALMER & DODGE, EUROPEAN DATA PROTECTION AND FCPA AND SEC INVESTIGATIONS GLOBALLY 1 (2008), http://commcns.org/MT8La9.

[109] COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, 30TH CNIL ACTIVITY

this recommendation, CNIL affirmed its commitment to data privacy in regulating the disclosure and transfer of data to foreign authorities.[110] Citing the "so-called French 'lock-up' law of 26 July 1968," CNIL reiterated that

> subject to international treaties or accords and to applicable laws and regulations, all persons are prohibited from requesting, seeking or transferring, whether verbally, in writing or in any other form, any documents or information of an economic, commercial, industrial, financial or technical nature intended to serve as evidence in foreign criminal or administrative litigation procedures.[111]

In April 2011, CNIL stated it intends to increase enforcement of French data privacy laws through additional inspections of corporate transfers of data outside of France.[112]

IV. TENSION BETWEEN THE GLOBALIZATION OF ENFORCEMENT AND INTERNATIONAL DATA PROTECTION LAWS

There is an inherent tension between the globalization of enforcement and related compliance efforts, of which anti-corruption is a relevant example, and the data privacy concerns surrounding the growth in personal data. As enforcement expands to cover companies and their employees located or acting outside of U.S., the data held by these companies becomes subject to the collection and review by government authorities.[113] Responding proactively to the increased threat of prosecution, companies are taking preventative steps to deter and detect potential violations through increased use of internal investigations.[114] Both the increased number and globalized nature of external investigations and the resulting performance of preventative internal investigations raise data privacy concerns, as these investigations undoubtedly will require the collection and review of personal data held by the company.[115] With the amount of personal data subject to collection, review, and storage increasing exponentially due to the advances in data management tools such as

---

REPORT 2009 75 (2010), http://commcns.org/MXcEZ4.

[110] *Id.* at 18.

[111] *Id.* at 75. It is also noted that non-compliance with this provision may result in imprisonment or fines. *Id.*

[112] Catherine D. Brewer et al., *French Data Protection Authority Announces Increased Inspections for Compliance with French and European Union Data Privacy Requirements*, GIBSON DUNN PUBLICATIONS (May 11, 2011), http://commcns.org/L88oUQ (stating CNIL intends to complete at least 400 such inspections in 2011, which represents an increase of 100 inspections from the previous year).

[113] Hart, *supra* note 24, at 1.

[114] *E.g.*, Press Release, Saimpen S.p.A., Snamprogetti Netherlands BV Enters Agreement with Federal Government of Nigeria (Dec. 20, 2010), http://commcns.org/JprsfV.

[115] Beryl A. Howell & Laura S. Wertheimer, *Data Detours in Internal Investigations in EU Countries: Part II*, THE METROPOLITAN CORP. COUNS., Nov. 2008, at 38 (noting how French companies have complained that legal obligations under U.S. law requires them to collect and retain personal information to protect themselves from criminal liability).

cloud computing, companies are finding themselves subject to a difficult situation of conflicting compliance requirements.

In *Nature's Sunshine Products,* the SEC opened the door for assigning control person liability to individual defendants in FCPA matters.[116] In doing so, the government effectively increased the pool of potential FCPA defendants and sent a strong message that executives will not be immune from prosecution. Furthermore, the examples of Technip and Snamprogetti show the extent to which U.S. authorities are willing to exercise jurisdiction over offenses that seemingly occur outside of the U.S.[117] While neither control person liability nor extra-territorial jurisdiction is an original exercise of authority, both represent another example of global regulatory enforcement.

A. An Increase in Corporate Internal Investigations and Compliance Efforts

Facing the uncertainty resulting from these decisions, and an overall increased risk of prosecution, corporations and their executives have, in turn, acted with increased diligence to establish, maintain, and supervise preventative compliance systems or internal investigation routines to detect potential anti-bribery violations.[118] Furthermore, in cases when U.S. authorities discover violations or file claims against these organizations, potential defendants have strong incentives to cooperate with the U.S. authorities voluntarily, as enforcement agencies are receptive to voluntary cooperation and reward such disclosure.[119] For example, both Technip and Snamprogetti agreed to cooperate with the ongoing investigations and implement internal audit and compliance controls in exchange for deferred prosecution.[120]

---

[116] *See* Jordan, *supra* note 48, at 856, 859-60. *See also* Complaint at 7-8, SEC v. Nature's Sunshine Prods., Inc., No. 2:09-CV-00672-BSJ, (D. Utah July 31, 2009), *available at* http://www.sec.gov/litigation/complaints/2009/comp21162.pdf.

[117] *See* Urofsky, *supra* note 30, at 619, 621.

[118] *See* Jordan, *supra* note 7, at 871.

[119] The DOJ rewards voluntary disclosure and cooperation. DEP'T OF JUSTICE, PRINCIPLES OF FEDERAL PROSECUTION OF BUSINESS ORGANIZATIONS 7-8 (2008) (stating that a company's timely disclosure and willingness to cooperate influence both the decision to prosecute and the severity of sanctions imposed, including deferred prosecution and non-prosecution agreements). On January 13, 2010, the SEC announced various changes in how the Enforcement Division will reward corporate cooperation, aligning the Division more closely with the approach taken by the DOJ. Press Release, Sec. & Exch. Comm'n, SEC Announces Initiative to Encourage Individuals and Companies to Cooperate and Assist in Investigations (Jan. 13, 2010), http://commcns.org/KzUigm. The U.K. Serious Fraud Office also encourages self-reporting and provides guidelines for reporting, investigation, and settlement. *See generally* SERIOUS FRAUD OFFICE, APPROACH OF THE SERIOUS FRAUD OFFICE TO DEALING WITH OVERSEAS CORRUPTION (2009).

[120] Press Release, Dep't of Justice, Technip S.A. Resolves Foreign Corrupt Practices Act Investigation and Agrees to Pay $240 Million Criminal Penalty (June 28, 2010), http://commcns.org/L893Wf.

The *Snamprogetti* deferred prosecution agreement demonstrates well how global enforcement leads to related compliance efforts, and therefore additional privacy concerns.[121] The DOJ's agreement to defer prosecution is conditioned on the company's promise to cooperate with continued DOJ investigations into Snamprogetti's dealings with "its present and former employees, agents, consultants, contractors, subcontractors, subsidiaries, and others" that may have been involved in violations of the FCPA.[122] Furthermore, Snamprogetti is required to disclose "all factual information" related to the matter including "documents, records, or other tangible evidence."[123] Finally, as part of the deferred prosecution agreement, Snamprogetti must implement a compliance program "designed to prevent and detect" FCPA violations.[124]

Given these requirements, as well as a strong incentive to comply with the agreement, Snamprogetti may face challenges where compliance with the EU data protection laws will be of issue.[125] Data owners both inside and outside the company will be affected, as emails, shared documents, travel expenses, and other relevant data from and between directors, employees, contractors, and business partners will be collected and scoured for potential claims. While the agreement excludes information covered by an attorney-client privilege or work product doctrine, under the terms of the Directive, investigations in furtherance of foreign regulatory enforcement likely do not provide a legitimate purpose for the transfer and disclosure of such personal data to U.S. authorities.[126]

Of further concern is the actual collection of this data for even an initial internal review. Much of it is likely in electronic form and therefore stored through data management tools that provide the ability to scour historical data for relevant people, discussions, timing, or other triggering factors. Particularly if personal data is stored in the cloud, data protection authorities have expressed concern over their ability to protect the data from unauthorized

---

[121] Deferred Prosecution Agreement at 7, United States v. Snamprogetti Netherlands B.V., No. 4:10-CR-00460 (S.D. Tex. July 7, 2010), *available at* http://commcns.org/JIvDof. The stakes are high for Snamprogetti, as full cooperation and compliance with the terms of the agreement provides the company with a guarantee that the DOJ will not prosecute for this matter. *Id.*

[122] *Id.*

[123] *Id.* at 3-5.

[124] *Id.* at 8.

[125] *See generally* Peace & Kennedy, *supra* note 74, at 1-3.

[126] Deferred Prosecution Agreement at 5, United States v. Snamprogetti Netherlands B.V., No. 4:10-CR-00460 (S.D. Tex. July 7, 2010), *available at* http://commcns.org/JIvDof; *Culture Clash – E-Disclosure vs. European Data Protection Law in International Arbitration*, MAYER BROWN (Jan. 2011), http://commcns.org/LY1VAT (explaining how Agreements to Disclose do not constitute a legal obligation within Article 7(c) of the Directive).

processing and transfers.[127] Even so, if proper requests for processing are submitted, it may be the case that the internal collection of such data does not fall under legitimate processing standards of the Directive.[128] Furthermore, Snamprogetti will need to create an effective program for compliance and internal investigation that meets the high standards of the DOJ, which will require the company to perform "reasonable inquir[ies]" into the dealings of its employees and, if necessary, "thorough investigation[s]" into suspected violations.[129]

B. Navigating the Tension

As Snamprogetti's situation underscores, the issue remains as to how companies will conduct internal investigations or comply with the requirements of external investigations while simultaneously balancing the requirements of laws governing data protection. Companies must continue to conduct business despite the evident tension between the globalization of enforcement and related data privacy concerns. This Part aims to provide a number of practical suggestions to manage the irreconciled problem at hand.

1. Use Safe Harbors to Transfer Personal Data with Adequate Controls

Several safe harbors have been developed by the U.S. Department of Commerce in conjunction with the European Commission, and approved by the latter as providing adequate privacy protection.[130] A U.S. company may self-certify that it is complying with the safe harbor provisions, which creates a presumption of adequate protection and constitutes representation that the organization will adhere to the established privacy policy that meets these strict

---

[127] Press Release, Comm'n Nationale de l'Informatique et des Libertés, *supra* note 68.

[128] *See* Peace & Kennedy, *supra* note 74, at 1-2 (explaining how the U.S. has inadequate data protection, which requires that processing may only occur under the following circumstances: (1) with consent, (2) in the vital best interest of the data subject, and (3) is a contractual necessity).

[129] The expectations of proper due diligence are high. For example, in Opinion Procedure Release 08-01, the DOJ determined a proposed transaction would not prompt enforcement due to the investors "reasonable inquiry" into the actions of suspect parties, which required the investor to gather personal information from a private party and its family. DEP'T. OF JUSTICE, OPINION PROCEDURE RELEASE NO. 08-01, FOREIGN CORRUPT PRACTICES ACT REVIEW 10 (2008), http://commcns.org/KWYqcA. In a separate opinion, the DOJ stated it would not prosecute a post-acquisition discovery of unlawful activity as long a "thorough investigation" was performed prior to purchase and any past violations were reported shortly after purchase. DEP'T. OF JUSTICE, OPINION PROCEDURE RELEASE NO. 08-02, FOREIGN CORRUPT PRACTICES ACT REVIEW 4 (2008), http://commcns.org/KX707Q.

[130] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://commcns.org/K4aGIg (last visited Apr. 15, 2012).

standards.[131] Thus, U.S. entities adopting the safe harbor may lawfully receive personal data transferred from EU member states. As such, participation in the safe harbor program may be used to satisfy EU privacy requirements for internal investigations conducted as part of a companies' FCPA compliance program.[132] For example, if a company self certifies, the safe harbor may cover the transfer of data stored at a corporate subsidiary located in the EU to a parent company in the U.S. for internal review, if processed and transferred for a legitimate purpose.[133]

The application of safe harbor protection, however, is limited. First, participation in the safe harbor program is only available to organizations subject to the jurisdiction of the Federal Trade Commission or to air carriers and ticket agents under the Department of Transportation.[134] Second, the safe harbor does not cover transfers to U.S. courts or investigating authorities, including the DOJ and SEC.[135] When planning compliance programs or specific internal investigations, companies should ensure coverage of safe harbor protection prior to initiating a personal data transfer.

2. *Institute Binding Corporate Rules to Ensure Adequate Controls*

Binding Corporate Rules ("BCRs") are established voluntarily by corporations, guaranteeing that they will meet adequate safeguards for the transfer of personal data between organizations within their corporate group.[136] BCRs, when used appropriately, are practical and can be effective in the cross-border transfer of data, but are strictly limited to companies within the same corporate group.[137] In addition, two conditions must be satisfied prior to use: the BCRs must be of a binding nature and legally enforceable. BCRs are binding in nature when all members of the corporate group must comply with them.[138] For this reason, BCRs are recommended only for closely-knit

---

[131] *Safe Harbor List*, EXPORT.GOV, http://commcns.org/JwOar2 (last visited Apr. 15, 2012) (maintaining a current list of Safe Harbor agreements).

[132] *Id.*

[133] *Viacom, Inc. Safe Harbor Privacy Policy,* VIACOM, http://commcns.org/KzVwba (last visited Apr. 15, 2012).

[134] *Safe Harbor Workbook,* EXPORT.GOV, http://commcns.org/LBRigG (last visited Apr. 15, 2012).

[135] *U.S.-EU Safe Harbor Overview, supra* note 130.

[136] *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*, EUROPEAN COMMISSION, http://commcns.org/JIx7DK (last visited Apr. 15, 2012). The Working Party endorsed the use of these rules, encouraging national data protection authorities in the individual member states to authorize intra-company transfers when the rules include identified essential content principles and are binding in law and in practice. *Id.*

[137] *Id.*

[138] *Id.*

corporations, not for loose conglomerates, as only in the former can compliance be adequately enforced.[139]

To ensure privacy is properly maintained, BCRs require that the data subject, or original owner of the processed personal data, become a third-party beneficiary of the data.[140] The data subject is also entitled to enforce the terms of the BCR by lodging a formal complaint with the data protection authority in the location where the data originated.[141] As such, legal enforceability may only be obtained if the relevant national law honors these rights of the data subject, or if a contractual arrangement between members of the corporate group can legally enforce them.[142]

BCRs are not ideal for the collection and transfer of data in response to a suspected violation or external investigations because the development of these rules, akin to codes of conduct, is time intensive.[143] Use of BCRs should be limited to small corporate groups looking to implement ongoing FCPA compliance programs.

3. *Request Assistance from U.S. Authorities for the Transfer of Personal Data*

When U.S. authorities are requesting data through external investigations, none of the aforementioned methods provide adequate protection for the transfer of personal data.[144] Some companies may wish, in the nature of cooperation, to communicate difficulties in retrieving personal data from abroad and request assistance from U.S. authorities. For example, under the 2002 SEC Multilateral Memorandum of Understanding with the International Organization of Securities Commissions ("MMOU"), the security regulators of the signatory states sought mutual assistance in the cooperative exchange of information for purposes of regulatory enforcement.[145] Such information would

---

[139] *Id.*

[140] *Data Protection Working Party Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules*, at 4, 1271-04-02/08/EN, WP 155 (Apr. 8, 2009).

[141] *Id.*

[142] *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*, *supra* note 136.

[143] Carla L. Reyes, Note, *The U.S. Discovery-EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy*, 19 DUKE J. COMP. & INT'L L. 357, 376-77 (2009).

[144] Because the EU has determined the U.S. does not regulate data privacy with adequate protection through domestic law and international commitments, personal data may not be transferred to U.S. authorities. *See* Brookman, *supra* note 67.

[145] As of 2004, there were twenty-six signatories. SEC. & EXCH. COMM'N OFFICE OF INT'L AFFAIRS, INTERNATIONAL COOPERATION IN SECURITIES LAW ENFORCEMENT 3 (2004), http://commcns.org/JwOFBx.

be particularly useful if the EU member state data authority had performed an investigation on the same set of facts and therefore had information pertinent to the data request.

In addition, the SEC has negotiated several bilateral Memoranda of Understanding ("MOUs").[146] MOUs are individual agreements between the SEC and the regulatory agency of another country predicating collection of personal data on the fact that the other country's securities regulator has legal authority to obtain and provide the requested information to the SEC.[147] In the context of data privacy laws, this would mean the local securities regulator may be able to obtain personal data if it has a legitimate purpose under local corruption laws.

Similar to the MMOU and MOUs, the DOJ Mutual Legal Assistance in Criminal Matters Treaties ("MLTAs") provide another avenue for the collection of data unavailable for direct transfer to the company.[148] Under MLTAs, the United States and a foreign country agree to assist one another with criminal antitrust violations.[149]

4. Obtain Unambiguous Consent of the Data Subject

Another way in which companies may collect data for external investigations while maintaining compliance with EU data protection laws is through consent of the data owner. The Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed," which must be "an express indication of [the data subject's] wishes."[150] In a July 2011 recommendation letter, the Working Party adopted a clearly conservative approach to consent and clarified the requirement for a clear scope and identification of consequences.[151] Blanket statements of

---

[146] *Id.*

[147] *The SEC's Cooperative Arrangements with Foreign Regulators*, U.S. SEC. & EXCH. COMM'N (May 23, 2008), http://commcns.org/KzWCnt.

[148] Scott Kimpel, *Antitrust Considerations in International Airline Alliances*, 63 J. AIR L. & COM. 475, 508 (1997).

[149] *Id.*

[150] Privacy Directive, *supra* note 74, art. 2. *See also Working Party Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, at 11-12, 2093/05/EN, WP 114 (Nov. 25, 2005). For sensitive data, consent must be "express and written." Privacy Directive, *supra* note 74, art. 17.

[151] The EU Justice Commissioner set out four pillars for data protection policy in Europe: the right to be forgotten, transparency, privacy by default, and protection regardless of data location. Rohan Massey, *The EU Article 29 Working Party Opinion on the Definition of Consent: An Unambiguous View of the Future*, BNA INT'L WORLD DATA PROTECTION REP., Aug. 2011, at 1. *See generally Data Protection Working Party Opinion 15/2011 on the Definition of Consent*, 01197/11/EN, WP 187 (July 13, 2011).

consent are not valid.[152] The data subject must be informed, with clear and sufficient detail of the use of such data.[153] The Working Party made it clear that it expects data controllers to carefully assess the risk involved to the individual prior to processing data based on consent.[154] The greater the risk for inadequate protection from things such as third party sharing or international transfers, the more specific and defined the request for consent should be.[155]

Consent is not always the primary or most desirable means for legitimate processing of data and creates numerous challenges to international investigations.[156] The Working Party has expressed concern that, when used in an inappropriate context, consent can lead to great vulnerability and can weaken the position of the data subject.[157] Consent in an employment context presents particular challenges, such as the concern that the data subject's position of subordination may influence, and therefore weaken, the validity of any offered consent.[158] This is especially true when the collection of data is for use by a public authority, as consent for this purpose requires clear obligation, and in the case of an investigation (rather than under court order, as in discovery), a clear obligation is difficult to meet.[159] Accordingly, consent should be used with caution when offered to legitimize processing of data for internal investigations, but is generally inappropriate when offered to legitimize data transfers to a public authority.

5. *Data Minimization*

Another option to consider is minimizing the data that will be processed or transferred by redacting personal data or anonymizing the material in general.[160] Companies can also work to ensure the data, requested through either internal or external investigations, is proportional to the purpose of the

---

[152] *Data Protection Working Party Opinion 15/2011 on the Definition of Consent*, at 17, 01197/11/EN, WP 187 (July 13, 2011).

[153] *Id.*

[154] *Id.* at 19.

[155] *Id.* at 37. The Working Party also suggested that potential drafting changes to the Directive should cover three key areas: the right of individuals to withdraw consent, the notion that consent must be obtained prior to processing commencing where there is no other legal ground for processing, and explicit requirements setting out the quality and accessibility of language used to obtain consent. *Id.*

[156] *Id.* at 10.

[157] *Id.*

[158] *Id.* at 14.

[159] *Data Protection Working Party Opinion 15/2011 on the Definition of Consent*, at 14, 01197/11/EN, WP 187 (July 13, 2011).

[160] *Resolving the Inherent Conflicts Between U.S. Investigations & European Data Privacy Law*, MAIN JUST. (Apr. 21, 2011), http://commcns.org/JptlJx.

request.[161] This can be done, for example, by offering a selective transfer based on quality or relevance.[162] Other forms of data minimization include filtering, where key words are used to remove potential irrelevant documents, or creating a privacy log, where certain material is withheld from processing or transfer until a further determination on its legitimacy for process can be made.[163]

C. Trending Towards Cooperation and Convergence of Law

Global enforcement of strong anti-bribery law is on the rise.[164] In addition to the growing number of countries adopting and enforcing strong anti-bribery legislation, cooperation between national authorities is increasing. In February 2010, the DOJ announced that fifty-six agreements were signed between the United States and the European Union or EU member states to foster increased information sharing or aid in the extradition of individuals charged with transnational crimes.[165] Seen as a milestone in closing the "gap between the globalization of business and the globalization of business crime enforcement," these agreements represent an increased willingness between regulatory authorities to cooperate across borders.[166] The DOJ is also an active participant in the OECD's Working Group on Bribery, which offers additional opportunities to foster relationships for mutual legal assistance with foreign regulatory authorities.[167] Authorities remain committed to enforcement and to continued cooperation with foreign regulators in their globalized enforcement efforts. Concurrent with increased cooperation, there has been an increased convergence in U.S. and, in particular, EU legal standards.[168] This move

---

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] LORELLO & BEST, *supra* note 5, at 1-3. U.S. enforcement is at an all-time high, and the recently enacted UK Bribery law provides for what many say is even more comprehensive prosecution of corrupt activity. *Id.* Enforcement of anti-bribery laws in Germany has increased in recent years, as well. *Id.* For example, Siemens agreed to pay German authorities close to $1 billion and Truckmaker MAN Group agreed to pay over $200 million to settle various anti-bribery proceedings. *Id.*

[165] Press Release, U.S. Dep't of Justice, *supra* note 24.

[166] Aguilar, *supra* note 24 (noting the treaties will assist in U.S. and EU investigations of anti-bribery and anti-fraud statutes).

[167] *Examining Enforcement of the Foreign Corrupt Practices Act: Hearing Before the Subcomm. on Crime and Drugs of the S. Comm. on the Judiciary*, 111th Cong. 2 (2010) (statement of Greg Andres, Acting Deputy Assistant Att'y Gen., Dep't of Justice). Notably, the OECD applauded U.S. authority efforts to investigate and prosecute "the most foreign bribery cases amongst the Parties to the Anti-Bribery Convention." *Id.*

[168] For example, in 2004, the European Commission adopted horizontal merger guidelines, essentially mirroring U.S. merger regulations. *See* Ilene Knable Gotts et al., *Nature vs. Nurture and Reaching the Age of Reason: The U.S./E.U. Treatment of*

towards consistent standards for regulation will also increase the need for transparency and accountability throughout the global business community and may create a more equal global playing field.[169]

V. CONCLUSION

In light of the tension between the globalization of enforcement and related data privacy concerns, the suggested points above may allow companies to assess whether data processing is appropriate. However, it remains that some companies are forced to either comply with U.S. regulations, or with foreign data protection laws. The fact that violations of domestic laws, including the FCPA, are punishable by large fines and imprisonment may well drive these parties to comply with U.S. regulations at the expense of data protection.[170]

Transatlantic Mergers, 61 N.Y.U. ANN. SURV. AM. L. 453, 490-91 (2005). The Commission has similarly moved to a proactive anti-cartel enforcement stance. *See* Christopher Harding & Julian Joshua, *Breaking Up the Hard Core: The Prospects for the Proposed Cartel Offence*, 2002 CRIM. L. REV. 933, 933. Similarly, efforts to improve international financial reporting through the harmonization of international accounting standards are "near [the] final stages" of completion. *See* FIN. ACCOUNTING STANDARDS BOARD & INT'L ACCOUNTING STANDARDS BOARD, PROGRESS REPORT ON IASB-FASB CONVERGENCE WORK 2 (2011), http://commcns.org/KQhUKb.

[169] RICHARD A. SPEHR, MAYER BROWN ROWE & MAW LLP, CURRENT ISSUES IN INTERNAL CORPORATE INVESTIGATIONS: CONCERN OVER THE LIABILITY EXPOSURE OF DIRECTORS AND OFFICERS HAS NEVER BEEN HIGHER (2005), http://commcns.org/Knljob.

[170] 15 U.S.C. § 78dd-2(g) (2004).