IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/International_Investigations_Principles

The Sedona Conference Working Group Series

wgs

The Sedona Conference

International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices

A Project of The Sedona Conference Working Group
on International Electronic Information Management,
Discovery, and Disclosure (WG6)

May 2017
Public Comment Version
Submit comments by **August 3, 2017**, to
comments@sedonaconference.org

The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices

A Project of The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6)

MAY 2017 PUBLIC COMMENT VERSION

Author:	The Sedona Conference
Editors-in-Chief:	Denise E. Backhouse Peggy Kubicz Hall David C. Shonka
Contributing Editors:	Taylor Hoffman Susan McClain Michael Pomarico
Contributors:	Lara Ballard Michael Becker Craig Earnshaw Michael Flanagan Natascha Gerlach Jennifer Hamilton David Moncure Jeane Thomas

We thank all of our Working Group Series Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the Public Comment Version of The Sedona Conference *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* ("*International Investigations Principles*"), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). WG6 is best known for its groundbreaking publication, The Sedona Conference *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation* ("*International Litigation Principles*"), and The Sedona Conference *Practical In-House Approaches for Cross-Border Discovery and Data Protection*. These publications are part of a series of Working Group publications by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The *International Investigations Principles* is effectively a companion publication to the *International Litigation Principles*. Whereas the *International Litigation Principles* addresses cross-border transfers of data in the context of U.S. civil litigation and legal actions, the *International Investigations Principles* addresses cross-border transfers of data in the context of government and internal investigations. This public comment version of the *International Investigations Principles* represents the collective effort of numerous WG6 members who, over the course of four years of dialogue, review, and revision, have developed a consensus-based set of principles and associated commentary.

I particularly thank Editors-in-Chief Denise Backhouse, Peggy Kubicz Hall, and David Shonka for their leadership and significant commitments in time and attention to this project. I also thank Taylor Hoffman who served as contributing editor. Finally, I thank Lara Ballard, Michael Becker, Craig Earnshaw, Michael Flanagan, Natascha Gerlach, Jennifer Hamilton, David Moncure, and Jeane Thomas for their contributions.

Please note that this version of the *International Investigations Principles* is open to public comment. Please submit comments by **August 3, 2017** to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Craig Weinlein
Executive Director
The Sedona Conference
May 2017

Foreword

In 2011, The Sedona Conference, through its Working Group 6 on International Electronic Information Management, Discovery and Disclosure (WG6) issued its *International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation* ("*International Litigation Principles*").[1] In it, WG6 identified six principles to guide companies navigating the competing demands of U.S. discovery and European data protection regulations. These six principles were accompanied by commentary, suggested best practices, and model practice materials.

The *International Litigation Principles* offers helpful guidance to practitioners and courts in reconciling U.S. Litigation discovery rights with data privacy rights. However, as noted in the commentary herein, the *International Litigation Principles* is not always useful, or even available, in the context of investigations.[2] Accordingly, WG6 formed a committee to study government and internal investigations, in order to explore how to best guide practitioners in addressing the unique issues often present in those matters.

This public comment version of The Sedona Conference *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* ("*International Investigations Principles*") is the culmination of a four-year effort by The Sedona Conference and WG6 to develop practical guidelines and principles to help organizations, regulators, courts, and other stakeholders when they must deal with government or internal investigations that necessitate the transfer of Protected Data across national borders. The *International Investigations Principles* was conceived as a result of dialogue that began in Zurich in 2013 where WG6 recognized that processes that work for handling Protected Data in litigation do not always work in investigations. In 2014, the general content of the *International Investigations Principles* was discussed at Sedona International Programmes and WG6 meetings in London (then in the form of a paper identifying the differences between litigation and investigations and calling for more dialogue on these issues) and New Orleans (then in the advanced form of a paper proposing modifications to the *International Litigation Principles*). Taking into account feedback from WG6 members, the WG6 Steering Committee then directed that the paper be developed into this standalone set of principles with commentary, which was the focus of additional dialogue in Hong Kong in 2015. A few months after the Hong Kong meeting, the European Union Court of Justice invalidated the U.S.-EU "Safe Harbor" program,

---

1 Originally issued for public comment in a European Union edition in 2011, the publication was revised and reissued in 2017 to incorporate received comments and to reflect intervening developments in international data protection and U.S. civil procedure rules and case law. *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/sedona-conference%C2%AE-international-principles-discovery-disclosure-data-protection-best [hereinafter "*International Litigation Principles*"].

2 The *International Litigation Principles* defines U.S. Litigation as "civil proceedings requiring the discovery of relevant information whether in federal, state, or other U.S. fora" and specifically excludes "criminal proceedings or any other government investigations." *See id.* at Sec. II, Definition 6 (incorporated into the *International Investigations Principles* in Definition 6).

which has since been replaced with the EU-U.S. Privacy Shield framework ("Privacy Shield"). Developments related to the Privacy Shield proposals then prompted a close review of the *International Investigations Principles* to ensure that it remains consistent with current law in the EU and elsewhere. The *International Investigations Principles* was developed during a tumultuous period in the evolution of EU-U.S. data protection relations, bookended by the revelations of Edward Snowden in 2013 and the passage into law of the General Data Protection Regulation (GDPR)[3] in May 2016, which will take effect in 2018, and the decision of U.K. voters in June 2016 to leave the EU.

The result is that the *International Investigations Principles* is a standalone document that provides guidance to organizations, regulators, courts, and other stakeholders when they must deal with government or internal investigations that necessitate the transfer of Protected Data across national borders. While the Privacy Shield, The Asia-Pacific Economic Cooperation (APEC) Framework, Mutual Legal Assistance Treaties (MLAT), The Hague Convention, and other intergovernmental arrangements all establish procedures that organizations may—or should—follow, the eight principles herein are intended to guide organizations in planning for and responding to investigations while ensuring that Protected Data is safeguarded at all times against avoidable risks of disclosure. Accordingly, these principles do not provide legal advice for complying with various legal regimens, nor do they purport to tell regulators or courts how they should respond in particular cases. Rather, they provide guidance for safeguarding all sensitive data while working within established legal regimens no matter where, or what, they are.

The *International Investigations Principles* is organized as follows: The Introduction is followed by Part I which highlights key differences between litigation on the one hand and government investigations and internal corporate investigations on the other. Part II sets out the eight guiding international principles for addressing data protection in cross-border government and internal investigations, and provides comments on each.

---

[3] The General Data Protection Regulation [hereinafter GDPR] is a single, binding EU-wide regulatory framework (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, text *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN), which becomes effective in 2018. *See Preparing for the General Data Protection Regulation (GDPR): 12 Steps to Take Now*, ICO (U.K. Information Commissioner's Office), 3 (Mar. 13, 2017) (noting that the GDPR will apply from May 25, 2018), https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf. The GDPR replaces Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, text *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046 [hereinafter the EU Data Protection Directive].

Table of Contents

The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations 1

Definitions 2

Introduction 3

I. Investigations Differ from Litigation in Important Ways 7

A. Public Policy Considerations 7

B. Specific Considerations: Government Investigations 10

C. Specific Considerations: Internal Investigations 16

II. Statement of Principles for Addressing Data Protection in Cross-Border Government and Internal Investigations 19

Principle 1 19

Principle 2 21

Principle 3 22

Principle 4 24

Principle 5 26

Principle 6 28

Principle 7 29

Principle 8 30

The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations

1. In furtherance of corporate compliance and ethics policies, companies doing business across international borders should develop a framework and protocols to identify, locate, process, move, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to government and internal investigations.

2. Regulators and other stakeholders should give due regard to a company's need to conduct internal investigations for the purposes of regulatory compliance and other legitimate interests affecting effective corporate governance, and to respond adequately to government investigations.

3. Courts and regulators should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting a company that must retain and produce information relevant to a legitimate government investigation, and the privacy interests of Data Subjects whose personal data may be implicated in a cross-border investigation.

4. Where the laws and practices of the country conducting an investigation allow it, the company should at an early stage of a government investigation engage in dialogue with investigators concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

5. Companies should consider whether and when to consent to exchanges of information among law enforcement jurisdictions to help coordinate and facilitate parallel investigations.

6. Law enforcement authorities in civil investigations should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

7. Courts and law enforcement authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

8. A party's conduct in undertaking internal investigations and complying with government requests or orders should be judged by a court, government agency, regulator, or data protection authority under a standard of good faith and reasonableness.

Definitions

The following definitions apply to the Principles, Commentary, and associated guidance:[4]

1. "Data Controller" is the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means for the processing and transfer of Protected Data.[5]

2. "Data Protection Laws" include any law or regulation, including U.S. laws and regulations, that restricts the usage or disclosure of data, requires safeguarding data, or imposes obligations in the event of compromises to the security or confidentiality of data. The *International Investigations Principles* is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with obligations pertaining to U.S. government and internal investigations, whether those laws take the form of privacy regulations, blocking statutes, trade secret protections, or other protections.

3. "Data Subject" is any person or entity whose Protected Data is or may be processed, transferred, or disclosed.

4. "Processing" includes any operation, activity, use, or application performed upon Protected Data by automatic or other means, such as collection, recording, storage, alteration, retrieval, disclosure, or transfer.

5. "Protected Data" is any data irrespective of its form (e.g., paper, electronically stored information (ESI), images, etc.) that is subject to Data Protection Laws.[6]

6. "U.S. Litigation" includes civil proceedings requiring the discovery of relevant information whether in federal, state, or other U.S. fora. For the purposes of these Principles, "U.S. Litigation" does not include criminal proceedings or government investigations.[7]

---

[4] Many of the definitions used in the *International Investigations Principles* parallel the terms used in the EU Data Protection Directive and are also found in the GDPR. We use these definitions intentionally in order to establish a common platform of understanding. It should be noted, however, that the *International Investigations Principles* is agnostic relative to the national origin of any Data Protection Law and our usage of similar terminology should not be construed as recognition or acceptance of any particular interpretation given to those terms by others, either now or in the future.

[5] Under the GDPR, a Data Processor who is not also a Data Controller may nevertheless also become subject to a similar level of accountability as a Data Controller, or subject to potential joint liability for processing performed on behalf of a Data Controller.

[6] The use of the word "data" in the *International Investigations Principles* is intended to convey that the Principles, Commentary, and associated guidance apply to all data, from its lowest level of abstraction to any assembly into information and its recordation on any media.

[7] For specific guidance concerning U.S. Litigation implicating cross-border data transfers, *see International Litigation Principles*, *supra* note 1.

Introduction[8]

Cross-border production of documents in civil litigation must account for data protection and privacy regulations of the countries where documents and custodians reside. Practitioners understand that U.S. discovery demands potentially conflict with client obligations under Data Protection Laws in jurisdictions where the client operates—and practitioners have become more adept at balancing these competing demands. WG6 has published a set of principles, provided commentary, and suggested best practices to assist practitioners in addressing these competing concerns. Less work has been done, however, to build consensus around best practices for handling personal data[9] in the context of government and internal investigations.[10] The Sedona Conference *International Principles for*

---

[8] The *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* (hereinafter "*International Investigations Principles*") was developed by the WG6 Committee on Government and Internal Investigations Co-Chairs Denise Backhouse, Peggy Kubicz Hall, and David Shonka, and committee member Taylor Hoffman. The *International Investigations Principles* incorporates much of the content of a paper which considered whether and how WG6 could appropriately address data protection in the context of government and internal investigations. That paper was the focus of dialogue at the 2014 WG6 members meeting in London and the 2014 All Voices Meeting in New Orleans. That paper was prepared by a WG6 task force which included: Denise Backhouse, Lara Ballard, Michael Becker, Craig Earnshaw, Michael Flanagan, Natascha Gerlach, Jennifer Hamilton, Peggy Kubicz Hall, David Moncure, David Shonka, and Jeane Thomas. The Committee especially thanks David Wallace-Jackson, Megan Walsh, and X. Kevin Zhao from the Greene Espel P.L.L.P. law firm; Leeanne Mancari from the DLA Piper LLP (U.S.) law firm; Kimberly J. Duplechain of Littler Mendelson, P.C.; and Shelley O'Hara from the U.S. Federal Trade Commission's (FTC) Office of General Counsel for their assistance with this publication.

[9] Personal Data is defined in the EU Data Protection Directive as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." EU Data Protection Directive, *supra* note 3, art. 2(a). The GDPR broadens this definition to include location data and "an online identifier" as factors. GDPR, *supra* note 3, art. 4(1). Under the EU Data Protection Directive, Processing of Personal Data is regulated in chapter II and specifically by Articles 6 and 7. Heightened protections apply to the processing of certain special categories of sensitive personal data, defined as personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." EU Data Protection Directive, *supra* note 3, art. 8(1). Under the GDPR, processing is again regulated in Chapter II and specifically by Articles 5–11, with sensitive personal data being subject to much more stringent restrictions than other personal data. *Cf.* GDPR, *supra* note 3, arts. 6, 9.

[10] Legal scholars and practitioners have begun to address the unique challenges presented by cross-border investigations. *See, e.g.*, Lucian E. Dervan, *International White Collar Crime and the Globalization of Internal Investigations*, 39 FORDHAM URB. L.J. 361, 373 (2011) ("The starting place for any internal investigation is the collection of relevant documentary evidence for review and analysis. . . . In the international context, however, collection, review, and transfer of documentation can present unique challenges to counsel because of the growing prevalence of data protection laws around the globe."); George J. Terwilliger III, *Transnational Practice in Preventing and Addressing Corruption Cases*, INTERNATIONAL WHITE COLLAR ENFORCEMENT: LEADING LAWYERS ON UNDERSTANDING INTERNATIONAL DEVELOPMENTS, COMPLYING WITH FCPA INVESTIGATIONS, AND ESTABLISHING EFFECTIVE CORPORATE COMPLIANCE PROGRAMS 95 (2011 Ed.), *available at* 2010 WL 5312204, at *2 ("Procedural differences among nations also affect the ability of a company to address suggestions of internal wrongdoing. . . . That does not make doing internal investigations impossible, but adhering to the requirements of local data privacy laws and restrictions in conducting internal investigations can add significantly to their cost and duration.").

Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices (*"International Investigations Principles"*) was developed to help fill that gap.

The following three examples illustrate realistic investigative situations and demonstrate the need for a set of principles and best practice guidelines for practitioners involved in international data processing and transfer in the context of investigations.

Example 1: A publicly traded global company based in the U.S. has operations in the U.K.; the U.K. company has a Brazilian subsidiary that is overseen by the U.K. company's Spanish subsidiary. If the Brazilian subsidiary engages in a foreign bribery scheme, the U.S. ultimate parent could simultaneously be subject to a Foreign Corrupt Practices Act (FCPA) investigation in the U.S., a U.K. Bribery Act investigation, and potentially two additional corruption investigations, one in Brazil and one in Spain. Relevant documents might be located in Spain and subject to Spanish Data Protection Laws. Other documents could be subject to Brazil's Data Protection Laws. As is common in the U.S., the ultimate-parent company, upon learning of the corruption and conducting an internal investigation, may decide to notify the U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC), which would expect the company to conduct an internal investigation, and then share the results with the agencies in order to obtain credit for cooperation and avoid criminal charges or reduce potential fines and penalties. The ultimate parent may also decide to share the results with the U.K. Serious Fraud Office (SFO) for the same reasons. To conduct the investigation, the company would collect relevant documents and data and conduct interviews in multiple jurisdictions. Materials might potentially be produced to the DOJ/SEC, the SFO, and to Brazilian and Spanish anticorruption authorities. Complicating the company's defense and response is the potential for a "dawn raid" in the country where the corruption is alleged—here, Brazil. One major issue, among many facing the company, is how it can effectively and efficiently collect and review relevant materials and negotiate its response with multiple countries' enforcement agencies while giving due respect to each country's Data Protection Laws.[11]

---

[11] This example is not fanciful. *See* Lindsay B. Arrieta, *How Multijurisdictional Bribery Enforcement Enhances Risks for Global Enterprises*, BUSINESS LAW TODAY (June 2016), http://www.americanbar.org/publications/blt/2016/06/08_arrieta.html (describing the "recurring and ongoing investigations and enforcement actions" against French company Alstom S.A. in multiple jurisdictions including the U.S., UK, Switzerland, and Brazil—in 2011, Swiss authorities fined Alstom approximately $40 million for bribery charges; in 2014, the company pled guilty to FCPA violations with penalties of over $772 million in the U.S.; the SFO charged Alstom with bribery in Lithuania and arrested seven executives on criminal charges; Alstom was also subject to a corruption probe in Brazil); *see also* SFO Case Information, Alstom Network UK Ltd & Alstom Power Ltd (Nov. 2, 2016), *available at* https://www.sfo.gov.uk/cases/alstom-network-uk-ltd-alstom-power-ltd/ (detailing charges and alleged offenses committed between 2000 and 2010 relating to projects in India, Poland, Tunisia, Lithuania, and Hungary); Department of Justice Press Release, Alstom Sentenced to Pay $772 Million Criminal Fine to Resolve Foreign Bribery Charges (Nov. 13, 2015), https://www.justice.gov/opa/pr/alstom-sentenced-pay-772-million-criminal-fine-resolve-foreign-bribery-charges (outlining bribery charges in connection with state-owned entity projects in Indonesia, Egypt, Saudi Arabia, the Bahamas, and Taiwan). Commenting on the increased collaboration among various agencies in transnational enforcement activities, one practitioner observed: "[T]he Justice Department's Criminal Division and the SEC work together with the Serious Fraud Office in the U.K., the Investigating Magistrates in France, and other authorities in Germany and elsewhere in Europe. In the future, it is likely that there will be increased cooperation in corruption and fraud cases with the authorities in Asia, with China currently being somewhat of a question mark." Terwilliger, *supra* note 10, at *10.

Example 2: A multinational company intends to acquire another multinational company and the proposed transaction is subject to merger-clearance procedures in multiple jurisdictions. If the deal is subject to U.S. pre-merger review and either antitrust agency makes a "second request,"[12] within a very short period the company may need to provide information about the proposed transaction, the affected lines of commerce, and the likely competitive effects of the proposed transaction. Because the target company does business in multiple jurisdictions outside the U.S., information may need to be collected, reviewed, and produced promptly in order to meet critical financing or business deadlines—and there may be great business pressure to complete the regulatory work necessary to proceed with the deal.[13] These business pressures could lead a company to take data privacy protection shortcuts in order to "clear the deal."

Example 3: Under U.S. Federal Sentencing Guidelines, a company may receive a reduction in fines of up to 95 percent if it has implemented an effective compliance program.[14] Multinational companies often design corporate compliance programs to meet the requirements of those guidelines. To be effective, a compliance program must include a means of investigating potential misconduct and auditing and monitoring the program itself.[15] To achieve these objectives, companies may monitor certain types of employee conduct worldwide to help prevent and detect violations of the company's

---

[12] *See* Fed. Trade Comm'n, *Merger Review*, FED. TRADE COMM'N, http://www.ftc.gov/news-events/media-resources/mergers-and-competition/merger-review (last visited Apr. 18, 2017) (describing process of merger review including potential for second requests).

[13] *See* Melissa Lipman, *5 Tips for Deal Makers to Smooth the 2nd Request*, LAW360 (Mar. 17, 2014), http://www.law360.com/articles/519230 (subscription required). Lipman's five tips are: (1) narrow the scope of the second request by asserting an appropriately narrow market or product definition; (2) hand over information quickly; (3) acknowledge a problem if it exists; (4) know how far your client will go to fix it; and (5) remember an adverse staff recommendation isn't the end. Of course, to know if your client has a problem that should be disclosed to regulators upfront requires a quick yet thorough investigation of the products and markets at issue while under the pressure of the second request response deadline.

[14] *See* Paula Desio, *An Overview of the Organizational Guidelines*, U.S. SENTENCING COMM'N, http://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf (last visited Apr. 18, 2017) (describing the impact of compliance programs on sentencing.)

> [W]hen the Commission promulgated the organizational [sentencing] guidelines, it attempted to alleviate the harshest aspects of this institutional vulnerability by incorporating into the sentencing structure the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range—in some cases by up to 95 percent—if an organization can demonstrate that it had put in place an effective compliance program. *This mitigating credit under the guidelines is contingent upon prompt reporting to the authorities and the non-involvement of high level personnel in the actual offense conduct.*

Id. (emphasis added). To self-report and show that high-level personnel were not involved in the criminal offense, a company must be able to investigate wrongdoing, identify who was involved, and provide evidence supporting its conclusion to the relevant prosecuting agency.

[15] An effective compliance program must include "[r]easonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal . . . [and] [r]easonable steps to respond to and prevent further similar offenses upon detection of a violation." *Id.*; *see also* U.S. SENTENCING GUIDELINES MANUAL § 8B2.1, U.S. SENTENCING COMM'N (2015), *available at* http://www.ussc.gov/guidelines/2015-guidelines-manual/2015-chapter-8.

business conduct policies, whether the conduct relates to fraud, conflicts of interest, embezzlement, corruption, harassment, treatment of confidential information, or other behaviors that could violate company policies and the law. As monitoring tools become more sophisticated, it is reasonable to assume that the company may review Protected Data as part of its compliance monitoring functions and that a surveillance program may conflict with data protection and other laws.[16]

The bottom line is this: government or internal corporate investigations raise issues that are not solved by strategies designed to balance the tension between discovery and privacy considerations in civil litigation. To appreciate why this is so, we must consider the procedural and legal differences between civil litigation and investigations—both government and internal. Accordingly, we examine the differences, *infra*.

---

[16] *See, e.g.*, Délibération n° 2014-042 du 30 janvier 2014 modifiant l'autorisation unique n° 2005-305 du 8 décembre 2005 n° AU-004 relative aux traitements automatisés de données à caractère personnel mis en œuvre dans le cadre de dispositifs d'alerte professionnelle [Deliberation n ° 2014-042 of 30 January 2014 modifying the single authorization n ° 2005-305 of 8 December 2005 n ° AU-004 relating to automated processing of personal data implemented within the framework of warning devices], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANCAISE [J.O.][Official Gazette of France], Feb. 11, 2014, *available at* https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=656E3F9168B3D0B618C7903416BB718B.tpdjo04v_2?cidTexte=JORFTEXT000028583464&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000028583033/ (regarding the 2014 amendments to whistle-blowing hotline requirements in France).

I. Investigations Differ from Litigation in Important Ways

A. Public Policy Considerations

Processing data when there are broad prohibitions against doing so is challenging, even when there appear to be exceptions that permit it. For example, Article 7(f) of the EU Data Protection Directive[17] allows the processing of otherwise Protected Data where the Data Controller has a "legitimate interest" that is not overridden by the "fundamental rights" of Data Subjects; to determine whether the exception applies a party must balance the interests and rights of all concerned parties.[18] Although commentators have explored that balance in the context of civil litigation, much of their analysis is inapplicable to government civil and criminal investigations and internal corporate investigations. Determining the appropriate balance requires exploring and weighing a range of public policy issues that are not present in litigation.

In litigation, the primary public policy objective is fair determination of party rights. Practitioners understand that the approach to litigation varies significantly between the U.S. and the EU, and those variations, especially the concept of broad discovery in the U.S., account in part for the tension related to cross-border data transfers. In government investigations, other important government (versus private) considerations are at stake, including the means by which governments enforce national policies (e.g., enforcement of competition policy, government regulation of corporate financial matters, financial regulation of banking institutions, anticorruption enforcement, money laundering, and so forth).

In the case of government investigations, nations have an obvious substantial interest in protecting their economies, the flow of commerce within their borders, and the health, safety, and welfare of

---

17 *Supra* note 3.

18 Article 29 Data Protection Working Party, *Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation*, at 8–9, 00339/09/EN/WP 158 (Feb. 11, 2009), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf [hereinafter WP 158]. In its *Opinion 06/2014 on the Notion of legitimate interest of the data controller under Article 7 of the Directive 95/46/EC*, 19844/14/EN/WP 217 (Apr. 9, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, the Article 29 Data Protection Working Party expanded further on this balancing analysis.

> It is also important to emphasise that Article7(c) refers to the laws of the European Union or of a Member State. Obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes-Oxley Act of 2002 in the United States) are not covered by this ground. To be valid, a legal obligation of a third country would need to be officially recognised and integrated in the legal order of the Member State concerned, for instance under the form of an international agreement. On the other hand, the need to comply with a foreign obligation may represent a legitimate interest of the controller, but only subject to the balancing test of Article 7(f), and provided that adequate safeguards are put in place such as those approved by the competent data protection authority.

Id. at 19 (citation omitted).

their citizens and residents, both human and corporate. Statutes, regulations, and court decisions reflect the societal values and beliefs of the countries that create them. They are among the principal means by which a government establishes national social and economic policy and standards of conduct for its citizens, resident aliens, and businesses that do business directly or indirectly in the country. A nation's law enforcement actions generally, and its law enforcement investigations in particular, are an important means by which it advances the public interest, ensures that its values and principles are honored, and ensures that its citizens and businesses are protected from those who do not share the same values and principles, or are unwilling to abide by them.[19]

In the case of internal investigations, the primary public policy objective is to ensure that companies engage in appropriate corporate governance both to protect their shareholders, employees, and other stakeholders and to protect their own ability to do business, especially where their licenses or operating permits depend on their compliance with local law. Corporate governance public policy considerations differ markedly between the U.S. and Europe. In the U.S., principles of corporate governance have developed through a combination of statutes; the Federal Sentencing Guidelines; rules of the Securities and Exchange Commission; rules of the various stock exchanges, including the New York Stock Exchange Governance Rules; regulations under federal contracting law; banking regulations; and development of the common law of fiduciary duty.[20] Today, it is well accepted in the U.S. and a few other countries, such as the U.K. and the Netherlands, that companies must have business-conduct policies and associated internal procedures designed to prevent, detect, and remediate employee and corporate misconduct in all aspects of a company's global operations: financial, human resources, manufacturing, sales, promotion, and more.[21] In contrast, "[i]n Europe, the emphasis

---

19 *See, e.g.,* U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR INTERNATIONAL ENFORCEMENT AND COOPERATION ¶ 1 *et seq.* (Jan.13, 2017), https://www.justice.gov/atr/internationalguidelines/download ("To protect U.S. consumers and businesses from anticompetitive conduct in foreign commerce, the federal antitrust laws have applied to 'commerce with foreign nations' since their inception.") (citation omitted), [hereinafter ANTITRUST GUIDELINES].

20 *See generally* RICHARD M. STEINBERG, GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE: IT CAN'T HAPPEN TO US—AVOIDING CORPORATE DISASTER WHILE DRIVING SUCCESS (1st ed. 2011); ANTHONY TARANTINO, GOVERNANCE, RISK, AND COMPLIANCE HANDBOOK: TECHNOLOGY, FINANCE, ENVIRONMENTAL, AND INTERNATIONAL GUIDANCE AND BEST PRACTICES (2008); Contractor Code of Business Ethics and Conduct, 48 C.F.R. §§ 52.203–13 (2015); ABA SECTION OF PUBLIC CONTRACT LAW, GUIDE TO THE MANDATORY DISCLOSURE RULE: ISSUES, GUIDELINES, AND BEST PRACTICES (2010).

21 *See generally Responsible Business,* INT'L CHAMBER OF COMM., https://iccwbo.org/global-issues-trends/responsible-business/ (last visited Apr. 18, 2017) ("[M]ore and more businesses are bolstering their principles and policies relating to transparency, ethics and risk management—not just for legal compliance but as an integral element of good management. Enterprises doing business with integrity are more likely to attract and retain motivated employees and attract investors who put their own reputation on the line."); *Corporate Responsibility*, INT'L CHAMBER OF COMM., https://iccwbo.org/global-issues-trends/responsible-business/corporate-responsibility/ (last visited Apr. 20, 2017) ("Companies today are increasingly approaching corporate responsibility as part of their overall policy to manage activities.").

is on voluntary internal controls rather than enforcement of controls by statutes."[22] Likewise, concepts of corporate criminal liability differ and are relatively new in Europe; the potential for a company to be held liable for the acts of non-senior management is much lower in Europe than in the U.S.[23] Arguably, such differences in governance policy may cause U.S. multinational corporations to engage in internal investigations and to assess whether corporate governance obligations require the self-reporting of misconduct to regulators, where EU companies might not. The point is simply this: corporate governance—as that concept is understood by U.S.-based multinationals—requires review of business documents in order to manage the company and to identify and remediate inappropriate behaviors.

For example, every Foreign Corrupt Practices Act (FCPA) investigation of a multinational company will necessarily include a cross-border component requiring collection and review of data from employees in countries alleged to be involved—and these multijurisdictional investigations are increasing.[24] As one commentator explains:

---

[22] *Is Corporate Governance Better Across the Atlantic?*, VALUE WALK (Jan. 11, 2013, 12:55 PM), http://www.valuewalk.com/2013/01/is-corporate-governance-better-across-the-atlantic/?utm_source= feedburner&utm_medium=feed&utm_campaign=Feed%3A+valuewalk%2FtNbc+%28Value+Walk%29; *see also* Global Corporate Governance Forum, *The EU Approach to Corporate Governance: Essentials and Recent Developments*, INTERNATIONAL FINANCE CORPORATION (Feb. 2008), *available at* http://www.ifc.org/wps/wcm/connect/f515ff804af4fc7da869b9b94e6f4d75/IFC_EUApproach_Final.pdf?MOD=AJPERES.

[23] *See* Clifford Chance LLP, *Corporate Liability in Europe*, CLIFFORD CHANCE (Jan. 2012), http://www.cliffordchance.com/content/dam/cliffordchance/PDFs/Corporate_Liability_in_Europe.pdf.

> In all jurisdictions where the concept of corporate, or quasi-corporate, criminal liability exists, it is, with the exception of the UK and the Netherlands, a relatively new concept. Those countries apart, France was the first European country to introduce the concept of corporate criminal liability in 1994, followed by Belgium in 1999, Italy in 2001, Poland in 2003, Romania in 2006 and Luxembourg and Spain in 2010. In the Czech Republic, an act creating corporate criminal liability has just become law as of 1 January 2012. Even in the UK where criminal liability for corporate entities has existed for decades, many offences focusing on corporate criminal liability have been created in recent years. In the Netherlands, until 1976 only fiscal offences could be brought against corporate entities. The movement towards criminal liability for corporate entities is likely to continue. . . . The basis or proposed basis of liability for corporate entities within those countries where liability exists (or is proposed) rests on the premise that the acts of certain employees can be attributed to a corporate entity. The category of employees which can trigger corporate liability is limited in some jurisdictions to those with management responsibilities and the act must generally occur within the scope of their employment activities. The act must also generally be done in the interests of or for the benefit of the corporate entity.

Id. at 2.

[24] Matthew Villmer, *4 Practice Areas Generating Big Billable Hours*, LAW 360 (Apr. 24, 2014), http://www.law360.com/competition/articles/524698?nl_pk=a0916a62-52d3-4f6b-a766-229071168fb0&utm_source=newsletter&utm_medium=email&utm_campaign=competition (subscription required) (discussing practice areas such as investigations under the Foreign Corrupt Practices Act that are "growing by leaps and bounds").

> With the rollout of a new agency to combat corruption in France and the implementation of anticorruption legislation in Brazil, it appears that the landmark UK Bribery Act and the U.S. Foreign Corrupt Practices Act (FCPA) are paving the way for legal reforms across the globe. These two statutes, with which corporate counsel and compliance officers have become intimately acquainted, have long been regarded as the pinnacles of anticorruption legislation. For years they stood alone, but now in addition to France and Brazil, a dozen countries are planning to follow suit with their own legislation.[25]

U.S. regulators often expect companies to conduct internal investigations and provide the results to the SEC and DOJ in order to earn "cooperation" credit.[26] Whether the company receives cooperation credit will depend, in part, on its providing authorities with relevant evidence and identifying relevant actors inside and outside of the company. This form of cooperation often requires disclosure of Protected Data.[27]

The regulatory and corporate governance underpinnings of government investigations and internal investigations make clear that the policy considerations affected by cross-border data transfers in those contexts differ from considerations in the litigation context.

B. Specific Considerations: Government Investigations

The foremost consideration for government-initiated investigations—whether civil or criminal—is to ensure that government investigators gain access to information they need to exercise their regulatory responsibilities while giving appropriate regard to important data privacy issues. Yet, regulators object if companies appear to use Data Protection Laws to stonewall investigations.[28] Regulators

---

[25] *See* Amit Katyal, *Anticorruption Laws Sweeping Across the Globe*, LAW.COM (Feb. 24, 2014), http://www.law.com/sites/articles/2014/02/24/anticorruption-laws-sweeping-across-the-globe/ (subscription required).

[26] According to the U.S. Department of Justice:

> Under DOJ's *Principles of Federal Prosecution of Business Organizations*, federal prosecutors consider a company's cooperation in determining how to resolve a corporate criminal case. Prosecutors consider whether the disclosure was made voluntarily and timely, as well as *the company's willingness to provide relevant information and evidence and identify relevant actors inside and outside the company, including senior executives*. In addition, prosecutors may consider a company's remedial actions, including efforts to improve an existing compliance program or *appropriate disciplining of wrongdoers*. A company's remedial measures should be meaningful and illustrate its recognition of the seriousness of the misconduct, for example, *by taking steps to implement the personnel, operational, and organizational changes necessary* to establish an awareness among employees that criminal conduct will not be tolerated.

U.S. DEP'T OF JUSTICE, CRIMINAL DIVISION AND U.S. SECURITIES AND EXCHANGE COMM'N, A RESOURCE GUIDE TO THE U.S. FOREIGN CORRUPT PRACTICES ACT, 54 (Nov. 14, 2012) (emphases added).

[27] *Id.*

[28] For example, China's State Secrets Law was invoked in an attempt to block the SEC from obtaining documents in a securities fraud investigation of the Chinese affiliates of BDO and the "Big Four" accounting firms—Ernst &

should be able to seek and obtain company cooperation and not need to resort to other means to obtain relevant data.[29] U.S. regulators' requests for information and documents are initiated by agencies pursuant to their statutory authority.[30] Agencies have a number of tools available for obtaining information, including administrative subpoenas, civil investigative demands, access letters, special orders, and turn-over demands. The time allowed to respond may be significantly compressed in the government investigation context. And some businesses believe that regulators do not understand the bind placed on corporations when regulators issue broad requests for information, including Protected Data, "wherever it may be."

Young, KPMG, Deloitte Touche Tohmatsu, and PricewaterhouseCoopers. In 2011 and 2012, the SEC sought documents and audit papers from the Chinese affiliates of these accounting firms to investigate suspected securities fraud by certain China-based issuers. Citing China's State Secrets Law and express directions from the China Securities Regulatory Commission (SCRC), the accounting firms refused to produce the requested documents. After negotiations reached an impasse, the SEC commenced administrative proceedings against the accounting firms, alleging violations of Section 106 of Sarbanes-Oxley Act. In January 2014, an administrative law judge issued a 112-page decision, concluding that the accounting firms had violated § 106 by willfully refusing to comply with the SEC's demands. As a sanction, the judge banned the firms from practicing before the SEC for six months. *See*, *In re* BDO China Dahua et al., Admin. Proc. Nos. 3-14872, 3-15116, Initial Decision (Jan. 22, 2014)*, available at* www.sec.gov/alj/aljdec/2014/id553ce.pdf. The matter was finally resolved in early 2015. *See, In re* BDO China Dahua et al., Admin. Proc. Nos. 3-14872, 3-15116, Settlement Order (Feb. 6, 2015), *available at* www.sec.gov/litigation/admin/2015/34-74217.pdf. *See also* SEC Press Release, SEC Imposes Sanctions Against China-Based Members of Big Four Accounting Networks for Refusing to Produce Documents (Feb. 6, 2015), *available at* www.sec.gov/news/pressrelease/2015-25.html (Under the settlement with the SEC, the SCRC will act as a conduit, enabling the SEC to gain access to Chinese firms' audit documents.). This case underscores the challenges facing companies doing business in China, which often find themselves caught between competing legal regimes.

[29] The *International Investigations Principles* addresses only those situations in which a regulator requires the company to provide information and documents, and the company must determine how best to cooperate while still complying with relevant Data Protection Laws. Consequently, this *International Investigations Principles* does not address how a company should respond to a search warrant or a dawn raid, MLAT arrangement, or the exercise of police powers generally. Article 8(5) of the EU Data Protection Directive states: "Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards." EU Data Protection Directive, *supra* note 3, art. 8(5). *See* Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, 2008 O.J. (L 350) (defining "'competent authorities' [as Member State] agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorized by national law to process personal data within the scope of this Framework Decision").

[30] *See* David C. Shonka, *Responding to the Government's Civil Investigations,* 15 SEDONA CONF. J. 1 (2014). Certain government investigative requests are voluntary, others judicially enforceable, and still others somewhere between voluntary and compulsory in that the recipient is not required to respond but is forbidden from closing a transaction until the information is provided and the waiting period has lapsed or the recipient has filed a detailed statement of why it cannot comply. *Id.* at 3–5.

In contrast, non-U.S. regulators may more often turn to police-like powers to collect information, resorting in particular to "dawn raids" in the context of competition law and corruption investigations.[31] To support collection of evidence in that context, EU investigators may rely on derogations that are not available to the company under investigation.

Companies accordingly must develop protocols that address their production of information to government agencies within reasonable timeframes and provide (where possible) adequate privacy protection. Best practices should reflect, among other things, the following realities differentiating investigations from litigation:

- Government investigations are conducted in a confidential manner in order to protect the integrity of the investigation and the privacy interests of the subjects. Once the government files a case in court, protective orders are routinely sought to protect sensitive personal data and other confidential information from public disclosure.[32] In addition, rules of procedure provide for the sealing of personal and other confidential information.[33]

- Government investigations are not confined to national boundaries.

- Government investigations may occur in parallel with other countries' investigations (criminal or civil) and such parallel proceedings may or may not be cooperative undertakings.

- Government investigations may extend over a lengthy period and change scope over time.

- Government investigations may be broad in scope and appear to have few limits.

---

31 *See, e.g.,* Caroline Binham, *Big increase in SFO raids signals tougher tactics,* FINANCIAL TIMES (June 9, 2013), https://www.ft.com/content/21ae857a-cf9a-11e2-a050-00144feab7de (subscription required) (reporting that the SFO conducts raids at the investigation stage to collect evidence); Jack Ewing and Bill Vlasic, *German Authorities Raid U.S. Law Firm Leading Volkswagen's Emissions Inquiry*, N.Y. TIMES (Mar. 16, 2017), https://www.nytimes.com/2017/03/16/business/volkswagen-diesel-emissions-investigation-germany.html; Practical Law Competition, *Investigations and Dawn Raids by the CMA: A Quick Guide*, PRACTICAL LAW, https://uk.practicallaw.thomsonreuters.com/6-380-1599?__lrTS=20170427190502429&transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1&ignorebhwarn=IgnoreWarns (last visited Apr. 28, 2017) (noting the UK Competition and Market Authority's "wide powers of inspection" include conducting dawn raids); Bloomberg, *HK's anti-corruption body raids JPMorgan CEO's office*, BUSINESS STANDARD (Mar. 31, 2014), http://www.business-standard.com/article/international/hk-s-anti-corruption-body-raids-jpmorgan-ceo-s-office-114033100012_1.html (describing example of a local jurisdiction implementing a dawn raid in the context of a multi-country, anti-corruption investigation).

32 *See* FED. R. CRIM. P. 16(d), 49.1; FED. R. CIV. P. 26(c).

33 *See* FED. R. CRIM. P. 49.1(d); FED. R. CIV. P. 26(c).

- Because investigators are typically not required to set out a specific claim or legal theory when they request data, it may be difficult for a company to assess the relevancy of documents covered by a data request. However, recipients of government demands are typically informed of the general nature of the conduct under investigation and the potential statutory violations. By statute, each Civil Investigative Demand (CID) issued by the DOJ or the Federal Trade Commission (FTC) must state the nature of the conduct or activities under investigation and the law pertaining to such conduct or investigation.[34] Further, the CID statutes require that documents be described with "such definiteness and certainty as to permit such material to be fairly identified."[35] Grand jury subpoenas may also list potential violations.

- Government investigations are not usually the subject of judicial supervision, but some statutes allow the recipient of a government demand to file a motion with the court to quash or modify the demand. The grounds for doing so, however, are limited. For example, the recipient of a CID from the DOJ may seek to quash or modify a demand on the grounds of burden, relevance, or privilege.[36] In contrast, the recipient of a subpoena or a CID from the FTC may only proceed administratively to quash or limit process and may not seek "pre-enforcement review" from a court.[37] However, regulatory demands are not always self-enforcing. Often, only if a company refuses to comply with an agency request (except when statutory or automatic penalties attach to noncompliance) would the agency seek judicial intervention to enforce its requests. Only at that point might a court provide oversight.

- Regulators may assess cooperation credit based on a company's willingness to provide information and identify employees and others involved in the matter under investigation.

- Regulators may use a combination of police powers and civil information requests to gather evidence.

Courts are not always available to assist companies in their attempt to balance their regulatory-disclosure obligations with their obligations under Data Protection Laws. In the U.S., for example, agencies enjoy broad powers to seek information from companies they regulate, and judicial supervision

---

34 15 U.S.C. §§ 57b-1(c)(2), 1312(b)(1); *see* 16 C.F.R. § 2.6.

35 15 U.S.C. §§ 57b-1(c)(3)(A), 1312(b)(2)(A); *see* 16 C.F.R. § 2.7(b).

36 15 U.S.C. §§ 1312, 1314(b); *see also* FED. R. CIV. P. 26(b), 45(d); FED. R. CRIM. P. 17(c)(3); ANTITRUST DIV., DEP'T OF JUSTICE, ANTITRUST DIVISION MANUAL, Chapter III, Part E.8., 69–72 (5th ed., last updated Apr. 2015), https://www.justice.gov/atr/file/761141/download.

37 *See* 16 C.F.R. § 2.7. Under Commission Rule 2.7, a party may raise objections to a subpoena by filing a petition to limit or quash. Such petitions may be resolved by a designated Commissioner, and the designated Commissioner's ruling may thereafter be appealed to the full Commission.

of agency requests is very limited. The government may request information even if there is no certain legal violation "because of the important governmental interest in the expeditious investigation of possible unlawful activity."[38] For example, in assessing a challenge to a FTC administrative subpoena, U.S. courts have observed that "[a]lthough the court's function is 'neither minor nor ministerial,'"[39] it is "strictly limited"[40] to determining whether the Commission can demonstrate that the subpoena is "'within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant'" to the matter under investigation.[41]

Not only is government authority broad, and court review limited, but it also may not serve a company's interest to seek judicial supervision over production disputes with regulators. From a defense point of view, government investigative requests are often challenging. Timing may be crucial. The company may not want to force the agency to turn to a court when an impasse appears because the company may not want to irritate the agency with a legal challenge to its request. Any potential defendant that pushes the agency into court to seek judicial enforcement runs the risk of damaging its working relationship with the agency and any cooperation credit it might otherwise receive. It also runs the risk of adverse publicity from not cooperating with a law enforcement investigation. Thus, judicial oversight of data requests is unlikely. Although judicially supervised protective orders are a best practice regularly used in litigation to govern the use and disclosure of documents and information produced during discovery, they are rarely, if ever, available in government or internal investigations. Various statutes, however, provide protections regarding the use and disclosure of information provided to the government.[42]

Further, when disputes arise over what information and documents the company should provide in response to an agency request, the government may be in a particularly strong negotiating position. In a merger-related second request, companies have a strong incentive to "get the deal done." Similarly, if the company faces potential criminal exposure because of employee misconduct, the consequences of agency action may be more severe to the company than they would be in private litigation. There may be a sense of greater seriousness, with the company wanting to ensure that it does the right thing (in terms of both compliance and public perception). Tactical considerations often shape the response to an agency request.

In some jurisdictions, particularly the U.S., companies may be able to engage in arm's length, candid discussions seeking to focus the investigation and limit productions to only the most necessary and relevant data and information, especially since the company may face concerns of disclosure of the

---

38 FTC v. Texaco, Inc., 555 F.2d 862, 872 (D.C. Cir. 1977) (en banc) (internal citation omitted).

39 *Id.* (quoting Okla. Press Publ'g Co. v. Walling, 327 U.S. 186, 217 (1946)).

40 *See id.* at 872.

41 *See id.* (quoting United States v. Morton Salt Co., 338 U.S. 632, 652–53 (1950)).

42 *See* ANTITRUST GUIDELINES, *supra* note 19, at ¶¶ 5.1.2, 5.1.4; *see, e.g.,* FED. R. CRIM. P. 6(e); 15 U.S.C. §§ 18a(h), 46(f), 57b-2, 1313(c)–(d), 1314(g); *see also* 5 U.S.C. §§ 552a(b), 552(b)–(c).

same materials in subsequent civil lawsuits (e.g., a damages suit following an antitrust investigation).[43] Statutory time limits, limited budgets, and heavy workloads also create agency incentives to respond to legitimate, reasoned, and well-supported requests to limit an investigation. Despite these incentives, agencies are not obligated to cooperate. Further, one might think that if a company is being investigated by a U.S. agency and wants to cooperate, it should obtain the cooperation of a data protection authority (DPA) in the relevant country. However, some fear that such cooperation during an ongoing investigation might come at the price of triggering an investigation in that country for the same conduct under investigation in the U.S. or may otherwise compromise the confidentiality that often surrounds such investigations. Additionally, in many jurisdictions, such as the U.K., DPAs do not affirmatively approve international data transfer requests; their role is to investigate violations of relevant legislation.

Conversely, some argue that there may be greater risks of tactical abuse of Data Protection Laws in government investigations. A company may be more inclined to use privacy laws as a defense to data production in the government context. A company's tactical decisions about whether to cooperate may depend on its business and legal interests, the type and importance of data requested, whether the matter will resolve quickly or slowly, and the probability that the investigation might otherwise resolve (with or without cooperation) before any data is produced. However, delay does not usually result in avoidance of data production. To the contrary, it may prolong the investigation by forcing the government to seek judicial enforcement, thus forgoing opportunities to narrow the scope of the investigation through candid discussions. In addition, expenses increase, given the costs of court enforcement actions.

Similarly, to the extent Data Protection Laws give Data Subjects legal rights and remedies against disclosure, in principle those laws could give Data Subjects the ability to prevent relevant but incriminating or embarrassing documents from being used by their employer or turned over to a prosecuting authority. An employee may attempt to use these laws to subvert or delay justified adverse employment action or even criminal prosecution.[44] Such attempts interfere with the ability of companies to cooperate with the government in detecting and ending wrongdoing, and ultimately harm the company, consumers, and society.

Companies responding to agency requests for information must also consider the potential for obstruction of justice charges. Such cases usually are predicated on willful loss or destruction of evidence, interference with potential witnesses, or affirmative obstruction of an investigation. A failure to produce all relevant non-privileged documents could result in an obstruction of justice charge

---

[43] *See* Shonka, *supra* note 30, at 8–9.

[44] Other legal obligations may affect the employees' responsibility to cooperate with internal investigations in European countries. For example, certain European labor laws impose regulations as to how investigations may proceed, but a discussion of such laws is beyond the scope of this paper.

against the company or its lawyers—even if the company maintains a good faith belief that the information can be legally withheld.[45] Of course, this presents a dilemma for an organization if the mere preservation of data is considered to be "processing" in violation of the data processing laws.

Complicating matters further, multiple countries' regulators may be involved in an area of investigation. Unlike the discovery context, where the typical pattern involves document movements to the U.S., investigations may involve reciprocal sharing amongst countries, each with different laws governing such exchanges. When one government becomes interested, others may follow.[46] This often appears in the merger context, as well as in the context of antitrust and anticorruption investigations. Such matters require the subject company to manage cross-border document transfer issues in multi-jurisdictional settings and thus raise complex and challenging issues of case management, document processing, review, transfer, and coordination. Indeed a company may find itself in the awkward position in which it submits different sets of documents to different investigating agencies in order to comply with different countries' privacy laws. And if regulators in one country, especially outside the U.S., use search warrants to collect evidence and then share that evidence with other involved governments, the company may be unable to collect (and use in its defense) the very documents that government investigators have already obtained by availing themselves of police power exemptions under Data Protection Laws.

Many of the issues involved in government investigations simply do not arise in the context of litigation-related transfers. Developing and implementing a sound framework and following best practices for investigations is important to global business operations and compliance functions.

C. Specific Considerations: Internal Investigations

As set out previously, a cornerstone of corporate governance in the U.S. is that companies that implement effective compliance programs are entitled—under certain circumstances—to reductions in fines that would otherwise be assessed for criminal conduct. As a result, companies place great weight on "finding and fixing" compliance-related issues. Hotline reports, whistleblower allegations,

---

[45] For example, a corporation lawyer was indicted, in part, for failing to produce documents she concluded were not required to be produced based on advice of outside counsel. *See DOJ Failed Case against GSK Staff Lawyer Lauren Stevens: Lessons Learned*, POLICY AND MEDICINE (Jan. 25, 2012), http://www.policymed.com/2012/01/doj-failed-case-against-gsk-staff-lawyer-lauren-stevens-lessons-learned.html#sthash.XcFe8TXJ.dpuf ("In *Stevens*, the judge specifically relied on favorable evidence found in house counsel's correspondence with outside counsel. The documents showed that outside counsel was intimately involved with GSK's document production that triggered Steven's [sic] indictment. For example, the judge pointed to letters and emails between in house counsel and outside counsel that showed that in house counsel was diligently relying on outside counsel's advice."). The lawyer was subsequently acquitted, but the issue remains of concern to in-house counsel. Imagine that in-house counsel locate incriminating documents as part of an internal FCPA investigation but decide not to disclose them to the DOJ/SEC because of relevant Data Protection Law. The company (and its counsel) are thus in a worse position as a result of attempting to cooperate.

[46] An interesting example of international cooperation is the U.S. SAFE WEB Act, 15 U.S.C. § 46(j), which allows the FTC to provide non-U.S. law enforcement agencies with investigation assistance. *See In re* FTC, No. MJG-13-mc-524, 2014 WL 3829947, at *4 (D. Md. Aug. 4, 2014) (enforcing a subpoena issued under 28 U.S.C. § 1782 to permit the FTC to obtain information on behalf of the Canadian Competition Bureau).

and the SEC's Dodd-Frank rules require prompt investigations to permit companies to manage their compliance obligations. In addition, other countries also have "leniency programs" for companies that self-report law violations. Similarly, various whistleblowing, labor, employment, and civil rights laws in the U.S. protect employees' rights in the workplace and require employers to protect those rights. These programs thus give companies a strong incentive to monitor internal behavior and report any misconduct they find. Of course, such internal policies further important government and social interests in promoting lawful conduct and sanctioning wrongdoers, while conserving government resources.

However, satisfying this corporate governance obligation requires companies to investigate employee misconduct and analyze otherwise Protected Data to determine whether misconduct has occurred—conduct that often involves serious, and potentially criminal, matters such as allegations of competition law violations, tender violation issues, export control issues, fraud, embezzlement, international corruption, and many others.

Investigative needs might often conflict with the underlying principles of consent and transparency incorporated into Data Protection Laws. Indeed, if abused and improperly used as a shield, such laws have the potential to stymie corporate counsel advising the company. Counsel may be prevented from conducting a thorough, meaningful internal investigation as required by bar rules and some laws, such as the Foreign Corrupt Practices Act (FCPA) and the U.K. Bribery Act, or from providing full and meaningful advice to the client company. For example, it makes no sense to seek advance express consent by an employee to investigate potential wrongdoing by that employee. Conceivably counsel could be exposed to a malpractice suit by a client company if he or she does not conduct a thorough internal investigation or provides inappropriate advice based on an incomplete investigation.[47] Accordingly:

- investigators may want to maintain secrecy regarding the subject matter of the investigation to prevent interference with or spoliation of evidence;

- it is often prudent for investigators to issue broad preservation notices in order to accomplish preservation without alerting alleged bad actors to the nature and targets of the investigation;

- it might be in the interest of the investigation for collection to occur simultaneously with the issuance of a preservation notice (an internal "dawn raid") to preserve evidence at the moment the organization receives notice of the matter in order to avoid the potential for spoliation of evidence;

---

[47] *See* Sections of Antitrust & Int'l Law, A.B.A., Comments Of The American Bar Association Sections of Antitrust Law And International Law On The Proposed Regulation Of The European Parliament And Of The European Council On The Protection of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, at 7 (Nov. 20, 2012), http://www.americanbar.org/content/dam/aba/administrative/antitrust_law/at_comments_eu_privacy.authcheckdam.pdf.

- personal consent may not be sought at all or may be delayed until the moment of collection because an employee who is requested to consent may destroy evidence or confer with other involved employees in an attempt to initiate a cover-up;[48]

- employees may refuse to provide consent if they distrust the employer or think they may be subject to discipline or termination if the investigative findings disclose misconduct, a lapse in judgment, or even mere negligence;

- the company may need to disclose the investigation and its results as part of a self-report to a regulator in order to obtain cooperation credit for the company;

- because the company will not know what the investigation may uncover, the company may be unable to tell employees how the information will be used or how long it will be retained; and

- disclosures may need to be made in countries that do not have laws that provide the same protections as those in the country from which the documents were collected.

In short, best practices in internal investigations may conflict with best practices in cross-border document transfer in litigation.

---

[48] In some countries, obtaining consent after the fact will not excuse a violation of the Data Protection Laws. For example, under German law, consent must be sought in advance of transfer and use. There are different legal terms for consent ("Einwilligung") and assent after the fact ("Genehmigung"). Assent after the fact is not a remedy for a previously-absent consent. *See* BÜRGERLICHES GESETZBUCHES [BGB] [CIVIL CODE], §§ 183,184(1)–(2) (Ger.), *translation at* http://www.gesetze-im-internet.de/englisch_bgb/index.html.

II. Statement of Principles for Addressing Data Protection in Cross-Border Government and Internal Investigations

Principle 1

In furtherance of corporate compliance and ethics policies, companies doing business across international borders should develop a framework and protocols to identify, locate, process, move, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to government and internal investigations.

Comment 1a: In the investigation context, a meaningful Principle 1 process should begin before an investigation enters the realm of possibility or, in the case of compliance monitoring, before the monitoring starts. Many problems can be avoided by setting up appropriate policies, procedures, and processes beforehand. Apart from data protection, labor and other laws (including works council rights, bargaining agreements, and the secrecy of telecommunications) can, under some circumstances, delay or even prohibit use of employee data. Having in place appropriate policies can help a company navigate these issues and demonstrate respect for applicable local laws.

Information Technology (IT) policies should be drafted concisely and clearly with explicit rules regarding the appropriate use of major IT assets and the employer's right of access. Apart from policies for active employees, off-boarding policies should set out what may happen to a former employee's data in the case of an investigation. Departing employees not subject to a legal hold may also be invited to delete—under supervision—any non-business, purely personal communications and documents that they stored in corporate assets. In certain countries, labor laws require employee body representatives to be involved in drafting such policies or, at the very least, to be informed of the policies. In some countries, whistleblower hotlines may need to be approved by the DPA. In most circumstances, it is good practice to bring relevant stakeholders to the table to set standards.

The careful design of an investigation plan is a necessary ingredient for complying with data protection requirements. Concise policies put in place before any investigation occurs provide the building blocks and necessary transparency for Data Subjects.

Comment 1b: A company may be able to earn good will with investigators if it gains the investigators' trust and is cooperative. One way to do this is to have strong compliance and ethics policies in place along with a framework and protocols that anticipate the possibility of an investigation before any actual investigation materializes. Such advance preparation enables a company to come forward, meet, and discuss issues with the regulators promptly. In order to be in this position, companies should consider developing a framework or guidelines that address how they will conduct internal investigations and respond to government investigations so as to pay due respect to relevant Data Protection Laws and the privacy rights of persons subject to such laws, as well as the needs of the company and law enforcement to detect wrongful conduct. Preparing such a framework or guidelines in advance of government and internal investigations helps ensure timely responses and consistent and defensible practices for addressing these potentially conflicting interests.

In addition to what follows this comment, this means that the company should: (a) have a solid grasp of where its data is collected and stored; and (b) have a response team that is prepared to deal with production requests on short notice, knows the company's mission, and understands its business and legal interests and priorities.

Comment 1c: In developing a framework or guidelines, a company should anticipate disclosure to third parties. Companies should consider implementing clear guidelines to assess the potential complexity of internal investigations and give due weight to data protection concerns. Most company investigations conclude as purely internal matters without third-party involvement. Stakes for data protection in this context are comparatively low as data protection exceptions may apply and any third-party involvement and cross-border data transfer is under the company's direct control. However, when an investigation uncovers activity that triggers a reporting duty or that may lead to government action, the data protection stakes increase as companies must anticipate broader data preservation obligations, cross-border data transfers, and third-party disclosures, all of which may conflict with data protection restrictions.

Comment 1d: When an internal investigation reaches a point where the need for third-party disclosure becomes likely, the company should consider the potential need to demonstrate the reasonableness and good faith of its decision-making processes in the event they are challenged. The company should also position itself to explain data protection issues and to propose limitations and alternative sources of data. The company is in the best position to determine the appropriate scope of its initial investigation; whether, when, and how to escalate the investigation; and what measures to take to maximize compliance with Data Protection Laws throughout this process.

Comment 1e: Companies that regularly conduct business in certain jurisdictions—and thus may face regulatory investigations in those jurisdictions—may consider including in their framework or guidelines country-specific information to help ensure consistent and defensible practices. This has the practical benefit of providing a company with a clear plan of action instead of having to start anew for each matter. A company may also determine which jurisdictions in which it does business raise the most significant compliance concerns and then allocate resources to address data protection issues according to the assessed costs and benefits.

Comment 1f: A company addressing a specific cross-border investigation should begin by identifying relevant jurisdictions and relevant laws governing the processing and cross-border transfer of information, and identifying a resource skilled in applying such laws. It is probably impractical for companies to retain counsel in every jurisdiction but, if faced with an investigation, companies should be advised by individuals knowledgeable on the laws of the specific jurisdictions.

Comment 1g: Appropriate protocols should include consideration of invoking specific confidentiality protections when disclosing or producing Protected Data to government regulators. In the U.S. for example, the U.S. Freedom of Information Act (FOIA) contains a specific exemption prohibiting the government from disclosing in response to public requests "records or information compiled for law enforcement purposes [that] . . . could reasonably be expected to constitute an unwarranted

invasion of personal privacy."[49] In addition to this broad, general prohibition, certain U.S. agency investigations are conducted pursuant to authorizing statutes that afford even stronger confidentiality provisions. For example, the Antitrust Civil Process Act, which authorizes the DOJ to investigate potential antitrust violations, contains a specific provision prohibiting the government from disclosing any material produced pursuant to that authority without the consent of the producing party.[50] Similar protections are provided under the False Claims Act,[51] Hart Scott Rodino Act,[52] and other statutes that authorize specific types of government investigations. In other types of investigations, statutes and regulations allow producing parties to request that the government provide confidential treatment under FOIA.[53] These types of confidentiality protections should be referenced in cover letters accompanying productions, production agreements, and/or on the face of individual documents in order to draw attention to the fact that Protected Data is being produced and is subject to heightened confidentiality protection.

Principle 2

Regulators and other stakeholders should give due regard to a company's need to conduct internal investigations for the purposes of regulatory compliance and other legitimate interests affecting effective corporate governance, and to respond adequately to government investigations.

Comment 2a: Companies have legal, regulatory, and governance duties that may at times conflict with data protection obligations. When such interests conflict, a company may need to balance the rights of Data Subjects against the company's legitimate interests. In assessing a company's conduct, those who implement and enforce Data Protection Laws should recognize these competing imperatives.

Comment 2b: This Principle applies where a DPA is evaluating whether a company has complied with relevant Data Protection Laws in response to either a government or an internal investigation. Although there are many substantial differences, similar public policies underlie both regulatory enforcement and corporate governance. Both seek to detect, appropriately punish or discipline, and prevent unlawful conduct and promote lawful conduct. Companies whose data is sought, as well as the jurisdictions in which they reside, have interests in promoting lawful conduct and detecting, eliminating, and punishing unlawful conduct.[54]

---

[49] 5 U.S.C. § 552(b)(7)(C).

[50] 15 U.S.C. § 1313(c)(3).

[51] 31 U.S.C. § 3733(i)(2)(C).

[52] 17 U.S.C. § 18a(h).

[53] *See, e.g.,* 17 C.F.R. § 200.83 (regarding SEC investigations).

[54] *See* EUROPEAN COMMISSION & DIRECTORATE-GENERAL FOR COMPETITION, COMPLIANCE MATTERS: WHAT COMPANIES CAN DO BETTER TO RESPECT EU COMPETITION RULES 9, 20 (2012) ("The prime responsibility for complying with the law, as in any other field, lies with those who are subject to it. EU competition rules applying to

This Principle describes a standard that DPAs, works councils, and regulators may use to determine whether companies are responding appropriately to agency requests or in conducting internal investigations. Courts and DPAs should consider good faith, reasonableness, and proportionality in judging either a company's internal investigations or its responses to government investigations. And in judging a company's responses to government investigations—particularly in the U.S.—best practices should recognize that regulators require great flexibility in requesting data in order to accurately detect the full scope of unlawful conduct. Those requests are generally made without judicial supervision, and companies respond to them with limited recourse to court intervention prior to the regulator's filing of a court action against the company. During a government investigation, determining whether a company's response to an agency's request is sufficient rests primarily in the hands of the regulator making the request, due to the nature of investigatory work. In the case of internal investigations, it rests primarily in the hands of those undertaking the investigation.

Comment 2c: Regulators and other stakeholders should be mindful of company self-governance needs, recognizing the societal and economic benefits that accrue from a company keeping a clean house and complying with its regulatory obligations. Data Protection Laws and blocking statutes should not be used as a shield to prevent the detection of unlawful conduct. Unlawful corporate conduct often causes widespread and long-term damage, harming companies, innocent employees, customers, and societies and economies as a whole. Corporate crime sometimes spans years or even decades. Maintaining lawful conduct and detecting and eliminating unlawful conduct benefits companies, their customers, their employees, and society. Conversely, undetected and unpunished corporate crime often multiplies and replicates when employees escape detection and then recruit coworkers and competitors into their crimes and carry their criminal conduct to new jobs in the same or different industries.[55]

Principle 3

Courts and regulators should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting a company that must retain and produce information relevant to a legitimate government investigation, and the privacy interests of Data Subjects whose personal data may be implicated in a cross-border investigation.

---

undertakings are a fact of daily business life that has to be reckoned with. . . . The Commission welcomes and supports all compliance efforts by companies as they contribute to the firm rooting of a truly competitive culture in all sectors of the European economy."), http://bookshop.europa.eu/en/compliance-matters-pbKD3211985/?CatalogCategoryID=8BYKABstR7sAAAEjupAY4e5L.

55 *See generally Position Paper: Business Compliance With Competition Rules*, BUSINESSEUROPE (Nov. 28, 2011), http://ec.europa.eu/competition/antitrust/compliance/businesseurope_compliance_en.pdf ("Abiding by antitrust rules is fundamental for creating and sustaining a competitive economy. . . . Being compliant with rules and maintaining a strong reputation are fundamental matters for every enterprise. . . . [C]ompliance action brings the following benefits: . . . [b]eing seen as a progressive and ethical business[,] . . . [a]ttracting ethically conscious consumers and investors[,] . . . attracting and retaining ethically conscious talent[,] . . . [and] [r]educing the risk of fines, or benefiting from competition authorities' settlement or leniency procedures . . . . The code of conduct of the company must make it absolutely clear that violation of any law, including competition law, will not be tolerated and will lead to disciplinary action[.]").

Comment 3a: The interests of multiple parties are implicated in any investigation that requires information to move across borders. The nation conducting an investigation has a vital interest in securing the information it needs to protect its societal and economic interests. The country hosting the information sought has, at a minimum, an interest in protecting its interests in the information and in ensuring that parties subject to its jurisdiction are treated fairly and in a manner consistent with its policies. The country housing the information also has an interest in: helping to uncover corporate crime or other unlawful conduct committed by entities within its borders; ensuring that companies residing within it are responsible corporate citizens; and ensuring that employees of companies residing within it are not recruited into crime or other unlawful conduct. Similarly, every third party whose information is sought has a significant interest in having its information protected from misuse, as well as in having crime or other unlawful conduct committed against it uncovered and punished. Finally, the corporate subject of the investigation not only has a critical legal interest in the outcome of the investigation and in being treated fairly, it also has a significant legal and economic interest—even if not always legally cognizable[56]—in minimizing its costs and burden in producing information, in minimizing any resulting fines, in cleaning house to uncover any unlawful conduct, in taking appropriate disciplinary action against offending employees, in preventing future violations that could result in even greater costs, and in having a say in whether its responses in one investigation are provided to a different jurisdiction. It also has a significant interest in not having its good faith compliance with one set of investigative demands result in an investigation by a different jurisdiction concerning its conduct in responding to the first investigation. These interests might best be protected if all interested courts and regulators recognize both the potential conflicts that may result from variance in legal regimens and the common interests that may result from convergent public policies. Where possible, they should also give due regard to vital national interests at play in law enforcement investigations.

Comment 3b: Due regard for conflicting interests is especially warranted when the subject is cooperating with the investigators and demonstrating a good faith effort to produce relevant information in a timely manner. Although regulators may not always "reward" good behavior in an investigation by "forgiving" law violations or even granting leniency, they nonetheless may be able to reward good conduct by working with the subject to find workable solutions to problems the subject may encounter because of conflicting legal obligations. Such cooperation on the part of the investigators may ultimately facilitate production of needed information and hasten the investigation while minimizing the subject's expense and burden of compliance. More importantly, a record of working with subjects who manifest good faith and who cooperate in investigations will encourage other parties to cooperate in future investigations.

Comment 3c: One way in which law enforcement investigations differ fundamentally from private litigation is that law enforcement investigations focus on events, and the regulators' theories and perceptions about those events may change as they gather more information. Accordingly, the scope of an investigation may expand over time or become more focused. Moreover, an investigation does

---

[56] At least in the U.S., the expense of defending a legal proceeding brought by the government is a cost of doing business and not a legally cognizable injury.

not end until the investigators determine not to pursue the matter further, or initiate a formal challenge.

As a consequence, when the country hosting relevant information has strict Data Protection Laws and policies, issues of preservation and information processing present one of the most vexing problems for investigators and the subjects of cross-border law enforcement investigations. This is so for investigators because they may be unable to "release" a party from its data preservation obligations until they know with certainty that they no longer need certain information. It is so for the subjects because their efforts to satisfy the investigative needs of one jurisdiction may require them to risk breaking the laws of another.

The difficulties that confront investigators and subjects in this regard can best be addressed through a dialogue in which the subject of the investigation is mindful of the investigators' legitimate need for information and the investigators are mindful of the legal obligations of the subject and the interests of any third party whose information may be implicated in the investigators' demands. In many instances, the investigators should consider whether their needs might be met through alternative mechanisms, such as phased productions, or receipt of aggregated or anonymized information.

Comment 3d: Regulators should retain Protected Data only so long as they are legally obliged to do so. In this regard, there are generally no conflicts between a litigation context and investigation context, except that in the context of investigations it may not be as clear when a legal obligation to retain Protected Data ends. In litigation, the obligation ends no later than when the litigation and any appeals and related litigation end. In investigations, the endpoint may be less clear, particularly given the real risk of follow-on litigation, and parties may need to make appropriate inquiries to investigators to determine the status of an investigation.[57] In responding to inquiries about the status of an investigation, investigators should bear in mind the interests and policies of the host country and those of any third party. One objective should be to "release" parties from their preservation obligations as soon as possible, consistent with the needs of the investigation.[58]

Principle 4

Where the laws and practices of the country conducting an investigation allow it, the company should at an early stage of a government investigation engage in dialogue with investigators concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

---

[57] *See International Litigation Principles*, *supra* note 1, at 25 (Principle 6).

[58] Some authorities have a practice of notifying entities that have submitted data of the conclusion of an investigation and arranging for the return or destruction of the data held by the authority. Those authorities, however, make exceptions to the return or destruction of the data, for example, if the data is relevant to another investigation by the authority or if a document has become a court exhibit, such as in a grand jury proceeding, and thus must be retained in an official government internal file. To address situations in which parties may not know that an investigation has concluded, the Federal Trade Commission has adopted a Rule of Practice that "relieves" a party of its preservation obligations with respect to the investigation if the party has not received any written communication from the agency regarding the investigation for a period of one year. *See* 16 C.F.R. § 2.14(c).

Comment 4a: U.S. experience has shown that there is real value in early and frequent engagement between the government and the parties. When the parties are candid and forthright with investigators, and investigators are willing to listen and engage with the parties, investigations can be focused and concluded efficiently at reduced cost to both the government and the parties. Especially in the absence of civil procedures that can be leveraged to advance data protection goals (including the meet and confer process, discovery and case management by a judge, rules limiting discovery and jurisdiction, and the court-ordered data protection), a company should look for opportunities to proactively alert regulators to potential legal conflicts and propose measures designed to protect data. In jurisdictions where regulators will entertain it, early discussions regarding scope may allow the company to limit potential conflicts with Data Protection Laws and to address those that exist while showing regulators good faith and transparency.

Comment 4b: Even in the absence of formal or informal mechanisms that facilitate frequent dialogue between the government and the parties, in some investigations there may be opportunities to use certain protective mechanisms outlined in the *International Litigation Principles*, including: phased disclosure; sampling; substitution of data; redaction, anonymization and pseudonymization (where viable); and physical and organizational security measures including encryption, access rights management, and access request notification.[59]

Comment 4c: The issues under investigation may evolve over time as clues are followed and threads of information are developed more fully until resolved—favorably or unfavorably. Investigators must be able to go where the evidence leads. In many ways, these needs are antithetical to the transparent, staged, targeted, specific collection, processing, and production strategies contemplated by Principle 3 of the *International Litigation Principles*.

Comment 4d: Some steps in investigations may help demonstrate substantial compliance with Data Protection Laws. In keeping with principles of data quality and proportionality,[60] any investigation should follow a carefully designed process ensuring that only data sources with relevance to the investigation are processed, that the processing is limited to that purpose, and that end-of-matter data disposition policies are followed. In accordance with Article 17 of the EU Data Protection Directive, technical and procedural measures should be adopted to ensure the security and confidentiality of the processed data. In-country evaluation by a local entity versus immediate cross-border sharing and transfer should be considered.[61] Deference should be given to rights of the Data Subject as soon as practicably and appropriately possible, recognizing that notification, for instance, can be a substantial risk to the investigation and may have to be delayed.[62]

Comment 4e: In disclosing information about global operations and educating regulators regarding potential data protection issues, companies should be prepared to explain how proposed measures

---

59 *See International Litigation Principles*, *supra* note 1, at 14–19 (Principle 3).

60 *See, e.g.*, EU Data Protection Directive, *supra* note 3, art. 6.

61 *See, e.g.,* WP 158, *supra* note 18, at 9–16 (discussing whistleblowing schemes).

62 *Id.* at 12.

to limit and channel disclosure meant to minimize data protection law conflicts are compatible with, and not intended to impede, investigation objectives.

Principle 5

Companies should consider whether and when to consent to exchanges of information among law enforcement jurisdictions to help coordinate and facilitate parallel investigations.

Comment 5a: To encourage and facilitate cooperation in government investigations and voluntary compliance with requests for information by their agencies, governments sometimes enact laws that limit agency use of information obtained. For example, the U.S. Internal Revenue Service generally may not share tax-related information with other agencies; the Department of Commerce may not share census information; both the DOJ and the FTC generally may not share with others any information they obtain under pre-merger notification laws; and the FTC may share information it receives in other law enforcement investigations with other federal or state agencies only if the other agencies certify that they will use the information solely for law enforcement purposes and maintain confidentiality.

Exceptions to these rules tend to be limited. For example, in very limited circumstances, the FTC can share information with non-U.S. law enforcement agencies under the U.S. SAFEWEB Act. [63] That law allows the FTC to share information with non-U.S. agencies in consumer protection cases upon request if: (1) the requesting agency seeks the information for law enforcement purposes; (2) the law it is enforcing is analogous to one enforced by the FTC; and (3) the requesting agency will reciprocate in cooperating with requests by the FTC.[64] In some circumstances, law enforcement authorities in criminal matters may have greater leeway in sharing information with their foreign counterparts than do civil law enforcement agencies if the requirements of Federal Rule of Criminal Procedure 6(e) or other statutory provisions are met.

Despite the limitations on their ability to share information, governments often investigate conduct or transactions that cross borders or even span the globe. Some matters may pique the interests of other nations. Examples of non-criminal matters include mergers involving large international companies or other competition cases involving monopolistic or other anti-competitive practices. Examples of criminal matters include price-fixing cases, theft of intellectual property, and foreign bribery. Although regulators often develop cooperative relations with their foreign counterparts, frequently embodied in Memoranda of Understanding or even Mutual Assistance Treaties, such arrangements in civil matters often limit the agencies to generalized discussions about legal theories and investigative strategies because agency authorization statutes preclude sharing actual information about the entities and subject matter of investigations.

---

[63] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 ("U.S. SAFE WEB Act"), Pub. L. No. 109-455, 120 Stat. 3372, extended by Pub. L. No. 112-203, 126 Stat. 1484, codified at 15 U.S.C. §§ 41 *et seq*.

[64] *See* 15 U.S.C. § 46(j)(1)–(4).

Comment 5b: The inability of regulators to share information has consequences for companies subject to investigation by more than one government for conduct involving common facts or transactions. Such companies must often deal with overlapping, burdensome, and redundant demands for information. Some government investigations may begin much later than others; some progress more swiftly than others. At the conclusion, companies may be subject to inconsistent or even mutually exclusive results that leave them in a position of having to disobey one country's orders in order to comply with another's. One strategy for avoiding, or at least minimizing, these risks, is for the company to authorize governments to share information about the subjects of their investigations to the extent they have the authority to do so. By allowing such sharing and information transfers, companies may be able to coordinate the timing of investigations and lessen their burden of producing information to multiple agencies. Most importantly, by encouraging coordination and cooperation among law enforcers, the company may minimize the risk that it will be subject to inconsistent or mutually exclusive orders.

Comment 5c: Significantly, coordination among countries may be the one aspect of a law enforcement investigation that a company can best control. In many instances, only the company can authorize governments to share information that they otherwise could not share.[65] Also, in some instances the company may be the only entity aware of multiple investigations. In many situations, there may be no reason why investigators in one country should know of a similar investigation in another country. In such situations, the company should consider whether its interest may best be served by granting waivers to encourage and facilitate cooperation and coordination among law enforcers. An important factor for the company to consider is that once enforcement actions in one jurisdiction are filed against a multinational entity, or a subject makes required public disclosures, such as under the securities laws, other jurisdictions will become aware of the investigation if they are not already aware. If the company has proactively granted a waiver and cooperated with other jurisdictions, its cooperation can serve to reduce penalties.

Comment 5d: Assuming a company decides to grant waivers that allow countries to share information to the extent the company is permitted to do so, it should carefully consider the scope of any waiver it grants, and especially whether it will allow agencies to share privileged information. In this regard, U.S. law generally recognizes that communications between a company's managers and in-house attorneys, as well as communications between the company's managers and other select employees, may be privileged. Not all countries recognize such privileges. Accordingly, when granting waivers to law enforcers, companies may wish to consider whether to limit the waivers to information and communications that are not privileged under the laws of one or more interested jurisdictions.[66] Similarly, by their very nature, dawn raids may result in the capture of more information than the investigators need for their investigation. Indeed, dawn raids may result in the acquisition of

---

[65] The company's ability to authorize such further disclosure may, however, be subject to obtaining appropriate Data Subject input.

[66] Both U.S. antitrust agencies have expressly adopted a model waiver for use in civil investigations. *See* Fed. Trade Comm'n Press Release, Federal Trade Commission and Justice Department Issue Updated Model Waiver of Confidentiality for International Civil Matters and Accompanying FAQ (Sept. 25, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/federal-trade-commission-justice-department-issue-updated-model.

information that is wholly irrelevant to the matter being investigated. In those cases, assuming the subject of the investigation has a chance to allow sharing among multinational regulators, the company should carefully identify the scope of the information that may be shared, taking special care to protect irrelevant Protected Data.

Comment 5e: To the extent that an entity considers granting waivers allowing authorities in different countries to share information, it should also consider the impact of Data Protection Laws on the scope of the waiver. On the one hand, a cooperative effort may facilitate adherence to data protection principles (for example, by ensuring greater control over the process, allowing the entity to negotiate limits on data processing, and minimizing data processing and transfer in a single effort). At the same time, such an effort may raise Data Protection Law concerns (for example, under EU law, considerations for transferring data within the EU are entirely different from those raised by transferring data to a non-approved country such as the U.S.; here, there may also be issues regarding notice and consent requirements and processing data for a single purpose).

Principle 6

Law enforcement authorities in civil investigations should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

Comment 6a: Governments do not enforce each other's laws, but may nonetheless share common interests, values, and goals with respect to certain non-criminal matters. Thus, where possible, dialogue and cooperation among and between foreign law enforcement agencies may generate good will and understanding among nations and advance global commerce and welfare. Nations create law enforcement agencies to enforce domestic laws, and thereby advance and protect the nation's societal and economic interests. They may also advance common interests with other nations either by entering into bilateral or multilateral treaties or by authorizing enforcement agencies to enter into Memoranda of Understanding and other cooperative arrangements with their foreign counterparts. Agencies may sometimes have opportunities to engage in informal discussions with foreign counterparts, although in civil matters such discussions often must remain at higher levels of generality. Cooperation and coordination may help a law enforcement agency leverage scarce resources. It may also benefit business entities subject to bilateral or multilateral investigations by reducing their expense and burden of dealing with multiple overlapping investigations and the risk of inconsistent orders.[67]

Comment 6b: Given the potential benefits, regulators and law enforcement authorities should carefully consider opportunities to engage in dialogue and cooperation with their foreign counterparts on matters of mutual interest and concern. This may be particularly important when business entities that manifest good faith efforts to cooperate in an investigation offer to facilitate the flow of information between governments. By acceding to such offers, regulators may help reduce the subject's

---

[67] *See* ANTITRUST GUIDELINES, *supra* note 19, at ¶¶ 5.1.3, 5.1.4.

costs of compliance with investigative demands and thereby encourage cooperation by other subjects in future investigations. A more immediate benefit is that all concerned regulators may gain access to more complete information and proceed with confidence that they are all working from the same factual basis. At least in principle, when nations share common goals and work with common facts, their legal and economic analysis of information should tend to converge and investigations should reach results that are approximately consistent, if not identical.

Principle 7

Courts and law enforcement authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

Comment 7a: The U.S. Supreme Court in *Aérospatiale* held that "international comity compels 'due respect' for the laws of other nations and their impact on parties in U.S. Litigation subject to, or entitled to benefits under, those laws."[68] As a corollary, the *International Litigation Principles* cautions that "Data Protection Laws should not be advanced for improper purposes or to delay preservation or discovery absent a good faith belief that Data Protection Laws conflict with U.S. preservation or discovery requirements."[69] As noted earlier, government and internal investigations implicate the law enforcement interests of foreign sovereigns, and may involve the specter of corporate criminal exposure. Accordingly, the stakes may be high for both the country conducting the investigation and the company that is the subject of the investigation (the public interest and the collateral consequences of civil or criminal law enforcement proceedings can be far reaching). The company's decisions of whether and how intensely to assert any conflicts-of-laws may be difficult. An interesting question is how courts and DPAs should treat the issue of comity in the context of regulatory enforcement where the conduct being investigated has the potential to support law enforcement actions, since there is an accepted exception to the application of comity principles when the strong public policies of the forum are in actual conflict with the laws of a foreign jurisdiction.[70] Seemingly, such conflicts should be rare because common public interest and welfare of the citizens of all interested nations are furthered when legitimate investigations can be conducted concerning possible improper behavior, such as bribery, theft, dishonesty, deception, and anticompetitive activities by corporations or by individual employees.[71]

Comment 7b: Law enforcement actions differ fundamentally from private actions. Because investigations are an exercise of sovereign power, they represent the means by which nations assert authority over conduct that occurs within their borders or that has a substantial effect within their borders, and help ensure adherence to national values. Because laws set out national values and policies, they

---

[68] *See International Litigation Principles*, *supra* note 1, at 9 (citing Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 546 (1987)).

[69] *Id.* at 10.

[70] *Id.* at 10 n.30.

[71] *See* ANTITRUST GUIDELINES, *supra* note 19, at ¶ 4.1.

express the public interest as identified and defined by the national legislature. Although private litigation often reflects national values and the public interest, law enforcement actions presumptively attempt to implement and protect the public interest and advance public welfare.

When a government decides to seek documents covered by foreign Data Protection Laws, "the government balances the need for the information sought and the public interest in the investigation against the interests of the foreign jurisdictions where the information is located and any potential consequences for [its] foreign relations."[72] Thus, a U.S. "government request for production . . . reflects the Executive Branch's conclusion, in the exercise of its responsibility for both foreign affairs and the enforcement of [criminal and civil] laws requiring production, that disclosure would be consistent with both the domestic public interest and international comity concerns."[73] As reflected in bilateral and multilateral agreements between nations, "many sovereigns recognize that government [law enforcement] document requests reflect important sovereign interests and should be dealt with cooperatively when possible."[74] Thus, companies' production of documents located in foreign jurisdictions in response to U.S. government requests cannot be equated to cooperation with requests by private litigants.

As already noted, nations do not enforce each other's civil laws. However, absent fundamental irreconcilable conflicts in values, they should respect each other's laws. Principles of comity suggest that nations should respect each other's legislative, executive, and judicial acts, at least where such respect is reciprocated. In the context of law enforcement investigations, comity suggests that courts and regulators of a country hosting information needed for an investigation in another country should give due regard to the laws (and interests) of the country conducting the investigation and seek to accommodate those interests where possible. They should also consider the extent to which the investigation reflects, or even furthers, the public, legal, and societal values of their own jurisdiction. Similarly, countries conducting investigations should make reasonable efforts to limit demands for protected information to that which they truly need.

Principle 8

A party's conduct in undertaking internal investigations and complying with government requests or orders should be judged by a court, government agency, regulator, or data protection authority under a standard of good faith and reasonableness.

Comment 8a: While Principle 7 addresses the deference and regard that governments should exercise when considering the legitimate law enforcement needs of another sovereign, Principle 8 primarily treats the standard they should apply when considering the legitimate governance needs of

---

[72] Brief for the United States as Amicus Curiae at *12, Arab Bank, PLC v. Linde, 134 S. Ct. 2869 (2014) (No. 12-1485), 2014 WL 2191224 (citing American Ins. Ass'n v. Garamendi, 539 U.S. 413–15 (2003)).

[73] *Id.* at *12–13.

[74] *Id.* at *13.

corporations in conducting internal investigations and echoes and paraphrases Principle 2 of the *International Litigation Principles*. That Principle provides guidance to parties who must attempt to meet both obligations, and to DPAs, government agencies, and courts that may be required to evaluate the parties' actions. In these situations, standards of good faith and reasonableness should apply, particularly when guidance is unavailable, vague, or inconsistent. Data Controllers and regulators assessing the conduct of an internal investigation should recognize the substantial benefits that accrue to the company and to society when companies detect, stop, prevent, and punish illegal conduct by their employees. When conflicts of law do arise, Data Controllers should make good faith and reasonable efforts to respond to those obligations, recognizing that full compliance with obligations may be impracticable. Conversely, when called upon to evaluate party actions and responses, DPAs, regulators, and courts should consider the conflicting obligations and base their judgments on consideration of the subject's reasonable and good faith efforts made under the circumstances that existed at the time and proportionate to the matters at issue.

For example, a Data Controller must necessarily make determinations regarding the applicability of Data Protection Laws, the country of origin of any Protected Data, and what data is actually protected. The Data Controller must ultimately make determinations about how to effectuate processing and potential transfer of Protected Data. Often these determinations must be made early, before the circumstances and scope of the investigation are known and before there is opportunity to consult with investigators or the DPA. Under Principle 8, the parties' actions—and later judgment of those actions—should be viewed, not in hindsight, but in light of the facts known and the circumstances that existed at the time the action was taken, and governed by a good faith and reasonableness standard.[75]

Comment 8b: There may be situations in which courts, regulators, DPAs, or others may be called upon to evaluate a company's compliance efforts in a law enforcement investigation that the host country finds does not adequately support its values and in which it believes the document demands conflict with the host country's Data Protection Laws. Here too, Principle 8 counsels that the company's actions should be viewed, not in hindsight, but in light of the facts known and the circumstances that existed at the time the action was taken, and governed by a good faith and reasonableness standard.

---

[75] For a discussion of the standard of "good faith" in U.S. Litigation, *see International Litigation Principles*, *supra* note 1, at 11–13 (Principle 2, Comment); for a discussion of preservation and legal hold duties in the context of government investigations, *see* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010), *passim* and Guideline 1, Illustration iii ("An organization learns of a report in a reputable news media source that includes sufficient facts, consistent with information known to the organization, of an impending government investigation of a possible violation of law by the organization stemming from the backdating of stock options given to executives. Under these circumstances, a government investigation (and possibly litigation) can reasonably be anticipated and a preservation obligation has arisen.").