

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



Copyright 2019, The Sedona Conference.
All rights reserved

THE SEDONA CONFERENCE WORKING GROUP SERIES



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 2018

FINAL/PREPUBLICATON VERSION

Cite as “19 Sedona Conf. J. 557 (forthcoming 2018)”



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)*

Author:

The Sedona Conference

Editors-in-Chief:

Denise E. Backhouse

Taylor M. Hoffman

Peggy Kubicz Hall

David C. Shonka

Contributing Editors:

Natascha A. Gerlach

Jeane Thomas

Contributors:

Lara Ballard

Michael Flanagan

Michael Becker

Jennifer Hamilton

Craig Earnshaw

David Moncure

Staff Editors:

Susan M. McClain

Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers,

Copyright 2018, The Sedona Conference.
All Rights Reserved.

clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series 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.

This publication may be cited as follows:

The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (forthcoming 2018), available at <https://thesedonaconference.org/publication/International%20Investigations%20Principles>.

PREFACE

Welcome to 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). This is one of a series of Working Group commentaries 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 Sedona Conference *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)* (“*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. The *International Investigations Principles* represents the collective effort of numerous WG6 members who, over the course of five years of dialogue, review, and revision, have developed a consensus-based set of principles and associated commentary.

I particularly thank Editors-in-Chief Denise E. Backhouse, Peggy Kubicz Hall, Taylor M. Hoffman, and David C. Shonka for their leadership and significant commitments in time and attention to this project. I also thank Natascha A. Gerlach and Jeane Thomas who served as contributing editors, as well as Lara Ballard, Michael Becker, Craig Earnshaw, Michael Flana-

gan, Jennifer Hamilton, and David Moncure for their contributions. And finally, I thank 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 in its various iterations.

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 2018

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 Organizations 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.² However, as noted in the commentary herein, the *International Litigation Principles* is not always useful, or even available, in the context of investigations. Accordingly, WG6 formed a committee to study Government and Internal Investigations, in order to explore how to best

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/International%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection> [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 11).

guide practitioners in addressing the unique issues often present in those matters.

This 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 five-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 civil Government Investigations or Internal Investigations that necessitate the transfer of Protected Data across national borders.³ The *International Investigations Principles* was conceived as a result of dialogue that began in 2013 in Zurich, where The 5th Annual Sedona Conference International Programme (“*International Programme*”) and a WG6 Meeting were held, and where WG6 recognized that processes that work for handling Protected Data in litigation do not always work in investigations. The general content of the *International Investigations Principles* was discussed at the International Programme and WG6 Meeting in London in July 2014 (then in the form of a paper identifying the differences between litigation and investigations and calling for more dialogue on these issues) and at The Sedona Conference “All Voices” Meeting in New Orleans in November 2014 (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 at the International Programme

3. The *International Investigations Principles* does not address cross-border data transfers in connection with criminal law enforcement investigations, which are governed by different laws, treaties, and protocols from civil (non-criminal) Government Investigations.

and WG6 Meeting in Hong Kong in June 2015. A few months after Hong Kong, the European Union Court of Justice invalidated the U.S.-EU “Safe Harbor” program, 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. These developments prompted further review of the draft commentary, and those changes were in turn the subject of additional dialogue at the International Programme and WG6 Meeting in Berlin in June 2016. The *International Investigations Principles* was developed during a tumultuous period in the evolution of EU-U.S. data protection relations, spanning the revelations of Edward Snowden in 2013, the decision of U.K. voters in June 2016 to leave the EU, and the passage into law of the General Data Protection Regulation (GDPR)⁴ in May 2016 and taking effect in May 2018. These last two developments were largely, but not perfectly, anticipated in time for Berlin; and, consequently, the public comment version of this paper was ready for discussion at the International Programme and WG6 Meeting in Dublin in June 2017.

The resulting *International Investigations Principles* is a standalone document that provides guidance to Organizations, regulators, courts, and other stakeholders when they must deal

4. The General Data Protection Regulation [hereinafter GDPR] is a single, binding EU-wide legislation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>), effective May 2018. 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, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046> [hereinafter the EU Data Protection Directive].

with civil Government Investigations or Internal Investigations that necessitate the transfer of Protected Data across national borders. While the Privacy Shield, The Asia-Pacific Economic Cooperation (APEC) Framework, The Hague Convention, and other intergovernmental arrangements, where available, all establish procedures that Organizations may — or should — follow, the eight principles herein are intended to guide Organizations in planning for and responding to Government and Internal 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 Investigating Authorities or courts how they should respond in particular cases. Rather, they provide guidance for safeguarding Protected 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 civil Government Investigations and Internal 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.

TABLE OF CONTENTS

The Sedona Conference International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations	566
Definitions	568
Introduction	571
I. Investigations Differ from Litigation in Important Ways.....	577
A. Public Policy Considerations	577
B. Specific Considerations: Government Investigations	584
C. Specific Considerations: Internal Investigations	595
II. Statement of Principles for Addressing Data Protection in Cross-Border Civil Government and Internal Investigations.....	599
Principle 1.....	599
Principle 2.....	603
Principle 3.....	606
Principle 4.....	610
Principle 5.....	613
Principle 6.....	617
Principle 7.....	619
Principle 8.....	622

**THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES FOR
ADDRESSING DATA PROTECTION IN CROSS-BORDER
GOVERNMENT & INTERNAL INVESTIGATIONS**

1. Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to Government and Internal Investigations.
2. Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.
3. Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection 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 Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority 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. Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.
6. Investigating Authorities 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 Data Protection 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 Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, or Data Protection Authority under a standard of good faith and reasonableness.

DEFINITIONS

The following definitions apply to the Principles, Commentary, and associated guidance:⁵

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.⁶
2. “Data Protection Authority” refers to a local, national, or other government entity authorized to implement and enforce Data Protection Laws.
3. “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 Government Investigations (as defined herein) and Internal Investigations,

5. Many of the definitions used in the *International Investigations Principles* parallel the terms used 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 the 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.

6. Under the GDPR, a Data Processor who is not also a Data Controller may nevertheless 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.

whether those laws take the form of privacy regulations, blocking statutes, specific industry protections (e.g., banking privacy), labor laws, trade secret protections, or other protections.

4. "Data Subject" is any person or entity whose Protected Data is or may be processed, transferred, or disclosed.
5. "Government Investigation" is used broadly to include any inquiry by a duly authorized government entity to acquire information for a purpose other than the investigation or prosecution of a crime or suspected criminal activity. Although a Government Investigation may lead to the filing of civil claims in judicial or administrative courts (considered U.S. Litigation), as used herein, Government Investigation refers only to the pre-filing investigative stage of proceedings.
6. "Internal Investigation" includes any inquiry into relevant facts undertaken by an Organization for the purpose of determining whether conduct attributable to it is or has been consistent with its legal or ethical obligations or whether others are or have been engaged in conduct that is harmful to the Organization.
7. "Investigating Authority" refers to the duly authorized government entity, other than a court, undertaking the Government Investigation at issue or demanding the production of information, but does not include Data Protection Authorities.
8. "Organization" as used herein shall have its ordinary meaning and may include any entity or group of entities that are related whether by ownership or by agreement.

9. “Processing” includes any operation or set of operations, activity, use, or application performed upon Protected Data by automatic or other means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, transfer, or disclosure or otherwise making available.
10. “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.⁷
11. “U.S. Litigation” includes civil proceedings requiring the discovery of 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 pre-lawsuit Government Investigations.⁸

7. 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.

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

INTRODUCTION

Cross-border production of documents in civil litigation must account for the data protection and privacy regulations of the countries where documents and custodians reside. Practitioners understand that the demands of litigation potentially conflict with parties' obligations under Data Protection Laws in jurisdictions where they operate, and practitioners have become more adept at balancing these competing demands. The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (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 Protected Data, particularly personal data,⁹ in the context of Government Investigations and Internal Investigations.¹⁰ The Sedona Conference *International Principles for Addressing Data Protection in*

9. For example, the EU defines "personal data" broadly to encompass virtually any information relating to an identified or identifiable natural person ('data subject'), reaching even location data and online identifiers. See GDPR art. 4(1).

10. In recent years, legal scholars and practitioners have addressed 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.), 2010 WL 5312204, at *2 ("Procedural differences among nations also affect the ability of a company

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 civil Government and Internal Investigations.

Example 1: A publicly traded global corporation based in the U.S. has operations in the U.K.; the U.K. corporation has a Brazilian subsidiary that is overseen by the U.K. corporation’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 corporation, 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 corporation 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,

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.”).

the corporation 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 corporation'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 corporation, 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 corporation Alstom S.A. in multiple jurisdictions including the U.S., U.K., Switzerland, and Brazil: in 2011, Swiss authorities fined Alstom approximately \$40 million for bribery charges; in 2014, the corporation 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 also was subject to a corruption probe in Brazil); see also U.S. Dep't 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 corporation intends to acquire another multinational corporation 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 corporation may need to provide a broad scope of information about the proposed transaction, the affected lines of commerce, and the likely competitive effects of the proposed transaction, including emails and other business records maintained by individual custodians. Because the target corporation 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 corporation to take data privacy protection shortcuts in order to “clear the deal.”

Example 3: Corporations have a vital interest in protecting their reputations, ensuring that their resources are not being misused or attacked, and ensuring that they are in compliance

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 May 16, 2018) (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, knowing whether a client has a problem that should be disclosed to regulators requires a quick yet thorough investigation of the products and markets at issue while under the pressure of the second request response deadline.

with their legal, moral, and social obligations. Indeed, this is one area in which their civil interests have the potential to overlap with criminal law violations. For example, under the U.S. Federal Sentencing Guidelines, a corporation may receive a reduction in fines of up to 95 percent if it has implemented an effective compliance program.¹⁴ Multinational corporations 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, corporations may monitor certain types of employee

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> (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, an Organization 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.

conduct worldwide to help prevent and detect violations of the corporation's 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 corporation policies and the law. As monitoring tools become more sophisticated, it is reasonable to assume that the corporation 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 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 both Government and Internal Investigations. We examine the differences, *infra*.

SENTENCING COMM'N (2015), <http://www.ussc.gov/guidelines/2015-guidelines-manual/2015-chapter-8>.

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, 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 whistleblower 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, the General Data Protection Regulation (GDPR)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

17. GDPR art. 6(f).

18. Previously, the Article 29 Working Party provided guidance on this issue under a parallel provision in the EU Data Protection Directive, Article 7. See 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/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 [Directive] Article 7(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

Although commentators have explored that balance in the context of civil litigation, much of their analysis is inapplicable to Government and Internal Investigations.¹⁹ Determining the appropriate balance requires exploring and weighing a range of public policy issues that are not necessarily 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 that context. In Government Investigations, other important government and public (versus private) considerations are at stake, including the means by which governments enforce national policies (e.g., enforcement of compe-

of the controller, but only subject to the balancing test of [Directive] 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).

19. Close to the time of publication of the *International Investigations Principles*, the Article 29 Working Party provided guidance on transfer derogations under GDPR art. 49 indicating that a derogation may be available for certain investigations. See Article 29 Data Protection Working Party, *Guidelines on Article 49 of Regulation 2016/679* (Feb. 6, 2018), http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614232 [hereinafter WP 262]. Public comments were invited until March 26, 2018). While stressing that derogations must be narrowly construed, this preliminary version of WP 262 notes that the GDPR art. 49(1)(e) derogation for transfers necessary for the establishment, exercise, or defense of legal claims may cover an administrative investigation in a third country including, for example, anti-trust law, corruption, and insider trading investigations; or for obtaining a reduction or waiver of a fine in, for example, an antitrust investigation; or for seeking approval for a merger.

tition 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 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 Organizations 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 Organizations are protected from those who do not share the same values and principles, or are unwilling to abide by them.²⁰

In the case of Internal Investigations, the primary public policy objective is to ensure that corporations 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

20. 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].

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.²¹ Today, it is well accepted in the U.S. and a few other countries, such as the U.K. and the Netherlands, that corporations must have business-conduct policies and associated internal procedures designed to prevent, detect, and remediate employee and corporate misconduct in all aspects of a corporation's global operations: financial, human resources, manufacturing, sales, promotion, and more.²² In contrast, "[i]n Europe, the emphasis

21. See generally RICHARD M. STEINBERG, GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE: IT CAN'T HAPPEN TO US—AVOIDING CORPORATE DISASTER WHILE DRIVING SUCCESS (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).

22. See generally *Responsible Business*, INT'L CHAMBER OF COMM., <https://iccwbo.org/global-issues-trends/responsible-business/> (last visited Apr. 3, 2018) (“[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. 3, 2018) (“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.”²³ Likewise, the scope of potential corporate liability differs in Europe; and the potential for corporations to be held liable for the acts of non-senior management is much lower in Europe than in the U.S.²⁴ Arguably, such differences in

23. *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), http://www.ifc.org/wps/wcm/connect/f515ff804af4fc7da869b9b94e6f4d75/IFC_EUApproach_Final.pdf?MOD=AJPERES.

24. See Clifford Chance LLP, *Corporate Liability in Europe* (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

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 corporations 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 corporation and to identify and remediate inappropriate behaviors.

For example, every FCPA investigation of a multinational Organization necessarily includes a cross-border component requiring collection and review of data from employees in countries alleged to be involved—and these multijurisdictional investigations are increasing.²⁵ As one commentator explains:

With the rollout of a new agency to combat corruption in France and the implementation of anti-corruption 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 anti-corruption legislation. For years they stood alone,

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.

25. Matthew Villmer, *4 Practice Areas Generating Big Billable Hours*, LAW360 (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”).

but now in addition to France and Brazil, a dozen countries are planning to follow suit with their own legislation.²⁶

U.S. regulators often expect Organizations to conduct Internal Investigations and provide the results to the SEC and DOJ in order to earn “cooperation” credit.²⁷ Whether an Organization receives cooperation credit will depend, in part, on its providing authorities with relevant evidence and identifying relevant actors inside and outside of the Organization. This form of cooperation often requires the Processing, transfer, and disclosure of Protected Data.²⁸

26. See Amit Katyal, *Anticorruption Laws Sweeping Across the Globe*, LAW.COM (Feb. 24, 2014), <http://www.law.com/sites/articles/2014/02/24/anti-corruption-laws-sweeping-across-the-globe/> (subscription required).

27. 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).

28. *Id.*

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

From the perspective of Investigating Authorities, the foremost consideration for government-initiated civil investigations is to ensure that the government gains access to information needed to exercise regulatory responsibilities;²⁹ they will object if Organizations appear to use Data Protection Laws to stone-wall investigations.³⁰ Investigating Authorities prefer to obtain

29. The *International Investigations Principles* addresses only those situations in which an Investigating Authority requires the Organization to provide information and documents, and the Organization must determine how best to cooperate while still complying with relevant Data Protection Laws. Consequently, the *International Investigations Principles* does not address how an Organization should respond to a search warrant or a dawn raid, Mutual Legal Assistance Treaty (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." 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. For example, China's State Secrets Law was invoked in an attempt to block the SEC from obtaining documents in a securities fraud investigation

Organization cooperation and not to resort to other means of obtaining relevant information. U.S. regulators' requests for information and documents are initiated by agencies pursuant to their statutory authority.³¹ Investigating Authorities 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 al-

of the Chinese affiliates of BDO and the "Big Four" accounting firms—Ernst & 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), <https://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), <https://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.).

31. *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 "compelled" to provide information, but is forbidden from taking certain actions unless it provides whatever information may be required. *Id.* at 3–5.

lowed to respond may be significantly compressed in the Government Investigation context. And some Organizations accordingly believe that regulators do not understand the conflicting obligations placed on Organizations when regulators issue broad requests for information, including Protected Data, “wherever it may be.”

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.³² To support collection of evidence in that context, EU investigators may rely on legal authorities that are not available either to the Organization under investigation or to foreign investigators.³³

32. 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&context-Data=\(sc.Default\)&firstPage=true&bhcp=1&ignorebhwarn=IgnoreWarns](https://uk.practicallaw.thomsonreuters.com/6-380-1599?__lrTS=20170427190502429&transitionType=Default&context-Data=(sc.Default)&firstPage=true&bhcp=1&ignorebhwarn=IgnoreWarns) (last visited May 15, 2018) (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).

33. Regulation (EC), No. 45/2001, which has to be adapted to Article 2(2)(b) and 2(3) of the GDPR, governs data protection by EU institutions that does not fall under Chapter 2 of Title V of the Treaty on European Union (TEU). GDPR, art. 2(2)(b) and 2(3).

Organizations accordingly must develop protocols that address their production of information to government agencies within reasonable timeframes and mitigate the privacy impact on affected Data Subjects. 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.³⁴ In addition, rules of procedure provide for the sealing of personal and other confidential information.³⁵
- Government Investigations often are not confined to conduct that occurred within one nation's 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.
- Because Investigating Authorities are typically not required to set out a specific claim or legal theory when

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

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

they request data, it may be difficult for an Organization to assess the relative importance 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. For example, 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.³⁶ Further, the CID statutes require that documents be described with “such definiteness and certainty as to permit such material to be fairly identified.”³⁷

- 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.³⁸ 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

36. 15 U.S.C. §§ 57b-1(c)(2), 1312(b)(1); *see* 16 C.F.R. § 2.6.

37. 15 U.S.C. §§ 57b-1(c)(3)(A), 1312(b)(2)(A); *see* 16 C.F.R. § 2.7(b).

38. 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>.

court.³⁹ However, regulatory demands are not always self-enforcing; and if an Organization refuses to comply with an agency request (except when statutory or automatic penalties attach to noncompliance), the Investigating Authority must seek judicial intervention to enforce its requests. Only at that point might a court provide even limited oversight.

- Investigating Authorities may assess cooperation credit based on an Organization's willingness to provide information and identify employees and others involved in the matter under investigation.
- Investigating Authorities may use a combination of police powers and civil information requests to gather evidence.

Courts are not always available to assist Organizations 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 Organizations they regulate, and judicial supervision of agency requests is very limited. Investigating Authorities 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."⁴⁰ For example, in assessing a challenge to an FTC administrative subpoena, U.S. courts have observed that "[a]lthough the court's function

39. See 16 C.F.R. § 2.7. Under Commission Rule 2.7, a party may raise objections to an FTC 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.

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

is ‘neither minor nor ministerial,’”⁴¹ it is “strictly limited”⁴² to determining whether the FTC 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.⁴³

Not only is government authority broad and court review limited, but it also may not serve an Organization’s interest to seek judicial supervision over production disputes with Investigating Authorities. From a defense point of view, government investigative requests are often challenging. Timing may be crucial. The Organization may not want to force the Investigating Authority to turn to a court when an impasse appears because the Organization may not want to irritate the authority with a legal challenge to its request. Any party that pushes the agency into court to seek judicial enforcement runs the risk of damaging its working relationship with the authority and reducing any cooperation credit it might otherwise receive. It also runs the risk of adverse publicity from not cooperating with a Government 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, may provide protections regarding the use and disclosure of information provided to the government.⁴⁴

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

42. *See id.* at 872.

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

44. *See* ANTITRUST GUIDELINES, *supra* note 20, 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).

Further, when disputes arise over what information and documents the Organization should provide in response to a government request, the government may be in a particularly strong negotiating position. For example, in a merger-related second request, Organizations have a strong incentive to “get the deal done.” Similarly, if the Organization faces potential criminal exposure because of employee misconduct, the consequences of complying with Investigating Authority requests may be more important to the Organization than they would be in private litigation. There may be a sense of greater seriousness, with the Organization wanting to ensure that it does the right thing (in terms of both compliance and public perception). Tactical considerations often shape the response to a government request.

In some jurisdictions, particularly the U.S., Organizations may be able to engage in arm’s length, candid discussions with the Investigating Authority seeking to focus the investigation and limit productions to only the most necessary and relevant data and information, especially as the Organization may be concerned that produced materials may be disclosed in subsequent civil lawsuits (e.g., a damages suit following an antitrust investigation).⁴⁵ Statutory time limits, limited budgets, and heavy workloads also create incentives for Investigating Authorities to respond to legitimate, reasoned, and well-supported requests to limit an investigation. Despite these incentives, authorities are not obligated to cooperate. Further, one might think that if an Organization is being investigated by a U.S. authority and wants to cooperate, it should obtain the cooperation of a Data Protection Authority in the relevant country. However, some fear that such cooperation during an ongoing investigation might come at the price of triggering an investigation in

45. See Shonka, *supra* note 31, at 8–9.

that country for the same conduct under investigation in the U.S., or may otherwise compromise the confidentiality that often surrounds such investigations or trigger a separate investigation relating to violation of Data Protection Laws in connection with complying with the U.S. investigation.

Conversely, some Investigating Authorities have expressed concern about the potential for tactical abuse of Data Protection Laws in Government Investigations. Investigating Authorities may be concerned that an Organization may be more inclined to use Data Protection Laws as a defense to production in the government context. An Organization's tactical decisions about whether—and to what extent—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 producing data to the Investigating Authority. 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, such as rights to access, correction, and deletion, those laws may potentially give Data Subjects the ability to prevent or at least delay the ability of their employers or an Investigating Authority to obtain relevant but incriminating or embarrassing documents. An employee may attempt

to use these laws to subvert or delay justified adverse employment action or even criminal prosecution.⁴⁶ Such attempts interfere with the ability of Organizations to cooperate with the government in detecting and ending wrongdoing, and ultimately harm the Organization, consumers, and society.

Organizations responding to agency requests for information must also consider the potential for obstruction of justice charges. Such cases are usually 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 against the Organization or its lawyers—even if the Organization maintains a good-faith belief that the information can be legally withheld.⁴⁷ Of course, this

46. 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. See David C. Shonka, *Producing Information from the EU to U.S. Government Agencies*, DIGITAL DISCOVERY & E-EVIDENCE (December 21, 2017) [hereinafter *Producing Information*].

47. For example, a corporate 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 (last updated May 6, 2018), <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 locates incriminating documents as part of an internal FCPA investigation but decide not to disclose

presents a dilemma for an Organization if the mere preservation of data is considered to be “Processing” within the meaning of applicable Data Protection Laws.

Complicating matters further, multiple countries’ Investigating Authorities may be involved in an area of investigation. Unlike discovery in the U.S. court or administrative litigation context, where the typical pattern involves cross-border transfers to the U.S., Government Investigations may involve reciprocal sharing amongst countries, each with different laws governing such exchanges. When one government becomes interested, others may follow.⁴⁸ This often appears in the context of antitrust review of mergers, as well as in the context of other antitrust and anticorruption investigations. Such matters require the subject Organization to manage cross-border, document-transfer issues in multiple jurisdictions and thus raise complex and challenging issues of case management, document Processing, review, transfer, and coordination. Indeed, an Organization may find itself in the awkward position of submitting different sets of documents to different Investigating Authorities in order to comply with different countries’ Data Protection 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 Organization’s ability to collect (and use in its defense) the very

them to the DOJ/SEC because of relevant Data Protection Laws. The Organization (and its counsel) are thus in a worse position as a result of attempting to cooperate.

48. An interesting example of international cooperation is the provision in the U.S. SAFE WEB Act, 15 U.S.C. § 46(j) that 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).

documents that Investigating Authorities have already obtained may be hindered, or even defeated.

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 are important to global business operations and compliance functions.

C. Specific Considerations: Internal Investigations

As set out previously, Organizations 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, Organizations place great weight on “finding and fixing” compliance-related issues. U.S. hotline reports, whistleblower allegations, and the SEC’s Dodd-Frank rules require prompt investigations to permit Organizations to manage their compliance obligations. In addition, various U.S. whistleblowing, labor, employment, and civil rights laws protect employees’ rights in the workplace and require employers to protect those rights. Similarly, other countries also have “leniency programs” for Organizations that self-report violations of laws, including laws protecting workers’, and other, rights. Programs like these provide Organizations strong incentives 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 corporations 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 the Organization or counsel advising the Organization. The Organization or its counsel may be prevented from conducting a thorough, meaningful Internal Investigation or from providing full and meaningful advice to management. For example, it makes no sense to give notice to an employee before investigating potential wrongdoing by that employee. Conceivably, counsel could be exposed to a malpractice suit by a client Organization if he or she does not conduct a thorough Internal Investigation or provides inappropriate advice based on an incomplete investigation.⁴⁹ Accordingly:

- Organization investigators generally seek to maintain secrecy regarding the subject matter of an Internal Investigation to prevent interference with the investigation or destruction of evidence, or when required by law;
- it may be prudent for Organization investigators to issue broad preservation notices in order to accomplish preservation without alerting alleged bad actors to the nature and targets of the Internal Investigation;

49. 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.

- it might be in the interest of the Organization 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 destruction of evidence;
- notice may not be given at all or may be delayed until the moment of collection because an employee may destroy evidence or confer with other involved employees in an attempt to initiate a cover-up;⁵⁰
- employees may object upon receiving notice 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 Organization may need to disclose the investigation and its results as part of a self-report to an Investigating Authority in order to obtain cooperation credit for the Organization;
- because the Organization will not know what the investigation may uncover, the Organization may be unable to tell employees how the information will be used or how long it will be retained; and

50. For all the reasons given with respect to Government Investigations, consent is not a viable option in Internal Investigations. Moreover, 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.

- 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 conclusion, cross-border transfers of data in Government Investigations and Internal Investigations may require an approach that differs from that taken in litigation.

II. STATEMENT OF PRINCIPLES FOR ADDRESSING DATA PROTECTION IN CROSS-BORDER CIVIL GOVERNMENT AND INTERNAL INVESTIGATIONS

Principle 1

Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, 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 a specific 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, customer, or other personal data. Having in place appropriate policies can help an Organization 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 the assets of the Organization. In certain countries, labor laws require employee body representatives to

be involved in the drafting and approval of 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 Data Protection Authority. 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. Nevertheless, policies should allow for flexibility in individual matters, particularly when specific decisions are documented and are accordingly considered in light of facts and circumstances known at the time.

Comment 1b: An Organization may be able to earn good will with an Investigating Authority 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 an Organization to come forward, meet, and discuss issues with the Investigating Authority promptly. In order to be in this position, Organizations 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 Organization and Investigating Authority to detect wrongful conduct. Preparing such a framework or guidelines in advance of Government Investigations 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 Organization 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 and understands its business and legal interests and priorities.⁵¹

Comment 1c: In developing a framework or guidelines for Internal Investigations, an Organization should anticipate potential disclosure to third parties. Most Internal Investigations conclude as purely internal matters without third-party involvement. Stakes for data protection in this context are comparatively low as Data Protection Law exceptions may apply and any third-party involvement and cross-border data transfer is under the Organization'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 the Organization must anticipate broader data preservation obligations, cross-border data transfers, and third-party disclosures, all of which raise heightened data protection concerns.

Comment 1d: When an Internal Investigation reaches a point where the need for third-party disclosure becomes likely, the Organization should consider the potential need to demonstrate the reasonableness and good faith of its decision-making processes in the event they are challenged. The Organization should also position itself to explain data protection issues to the Investigating Authority and to propose limitations and alternative sources of data. The Organization is in the best position to determine the appropriate scope of its initial investigation; whether, when, and how to escalate the investigation; and

51. The GDPR's requirements of data protection by design and by default (GDPR art. 25) facilitate this further.

what measures to take to maximize compliance with Data Protection Laws throughout this process.

Comment 1e: Organizations that regularly conduct business in certain jurisdictions—and thus may face Government 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 an Organization with a clear plan of action instead of having to start anew for each matter. An Organization 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: An Organization addressing a specific cross-border investigation should begin by identifying relevant jurisdictions and relevant Data Protection Laws governing the Processing and cross-border transfer of information, and identifying a resource skilled in applying such laws. It is probably impractical for Organizations to retain legal counsel in every jurisdiction but, if faced with an investigation, Organizations 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 Investigating Authorities. 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.”⁵² In addition to this broad,

52. 5 U.S.C. § 552(b)(7)(C).

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.⁵³ Similar protections are provided under the False Claims Act,⁵⁴ Hart Scott Rodino Act,⁵⁵ 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.⁵⁶ These types of confidentiality protections should be referenced in cover letters accompanying productions, production agreements, and if possible 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

Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.

Comment 2a: Organizations have legal, regulatory, and governance duties that may at times conflict with data protection obligations. When such interests conflict, an Organization may

53. 15 U.S.C. § 1313(c)(3).

54. 31 U.S.C. § 3733(i)(2)(C).

55. 15 U.S.C. § 18a(h).

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

need to balance the rights of Data Subjects against the Organization's legitimate interests in complying with those duties. In assessing an Organization's conduct, Data Protection Authorities and those who implement and enforce Data Protection Laws should recognize these competing imperatives.

Comment 2b: This Principle applies where a Data Protection Authority is evaluating whether an Organization 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 civil regulatory enforcement and corporate governance. Both seek to detect, appropriately punish or discipline, and prevent unlawful conduct and promote lawful conduct. Organizations 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.⁵⁷

This Principle describes a standard that Data Protection Authorities, Investigating Authorities, and works councils may use to determine whether Organizations are responding appropriately to Investigating Authorities' requests or in conducting Internal Investigations. Courts and Data Protection Authorities should consider good faith, reasonableness, and proportionality in judging either an Organization's Internal Investigations or its

57. 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 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>.

responses to Government Investigations. And in judging an Organization's responses to Government Investigations—particularly in the U.S.—best practices should recognize that Investigating Authorities 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 Organizations respond to them with limited recourse to court intervention prior to the government's filing of a court action against the Organization. During a Government Investigation, determining whether an Organization's response to an information request is sufficient rests primarily in the hands of the Investigating Authority 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 on behalf of the Organization.

Comment 2c: Data Protection Authorities and other stakeholders should be mindful of an Organization's self-governance needs, recognizing the societal and economic benefits that accrue from an Organization 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 conduct often causes widespread and long-term damage, harming Organizations, innocent employees, customers, and societies and economies as a whole. Undetected malfeasance sometimes spans years or even decades. Maintaining lawful conduct and detecting and eliminating unlawful conduct benefits Organizations, their customers, their employees, and society, and is generally a common international public interest. Conversely, undetected and unpunished malfeasance often multiplies and replicates when employees escape detection and then recruit co-workers and

competitors into their schemes and carry their unlawful conduct to new jobs in the same or different industries.⁵⁸

Principle 3

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

Comment 3a: Every investigation that requires data to move across borders implicates the interests of multiple parties and countries. At a national level, the country conducting an investigation has a vital interest in securing the information it needs to protect its societal and economic interests. The country in which the information sought is located has, at a minimum, an interest in asserting its authority over the data located there and, to the extent the data relates to Data Subjects within its jurisdiction, it also has an interest in ensuring that those Data Subjects are treated fairly and consistently under its laws. The country

58. 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[.]”).

from which the data originated also has an interest in helping to uncover unlawful conduct committed by entities within its borders; ensuring that Organizations residing within it are responsible corporate citizens; and ensuring that employees of Organizations residing within it are obeying the law.

At the sub-national level, every Data Subject whose information is sought has a significant interest in having his or her information protected from misuse, as well as in having unlawful conduct committed against him or her uncovered and punished. Similarly, the Organization that is the subject of the investigation not only has a critical legal interest in the outcome of the investigation, but it also has a significant economic interest—even if not always legally cognizable⁵⁹—in minimizing its costs and burden in producing information, in minimizing any resulting penalties, 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 information produced in one investigation is 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, as would happen if responding to a Government Investigation triggered an inquiry by Data Protection Authorities in another jurisdiction.

Each of these varied interests might best be balanced if all interested courts and Investigating Authorities recognize both

59. 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.

the potential conflicts that may result from variance in legal regimens and the common interests that may result from convergent public policies.

Comment 3b: Due regard for conflicting interests is especially warranted when the Organization is cooperating with the Investigating Authority and demonstrating a good-faith effort to produce relevant information in a timely manner. Although Investigating Authorities 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-faith conduct by working with the Organization to find workable solutions to problems encountered because of conflicting legal obligations. Such cooperation on the part of the Investigating Authority may ultimately facilitate production of requested information and hasten the investigation while minimizing the Organization’s expense and burden of compliance. More importantly, a record of working with Organizations that manifest good faith and cooperate in investigations will encourage other parties to cooperate in future investigations.

Comment 3c: One way in which Government Investigations differ fundamentally from private litigation is that Government Investigations focus on events, acts, or practices and the Investigating Authority’s theories and perceptions may change as it gathers more information. Accordingly, the scope of an investigation may expand over time or become more focused. Moreover, a Government Investigation does not end until the Investigating Authority determines not to pursue the matter further, or initiates a formal challenge.

As a consequence, when the country hosting relevant information has strict Data Protection Laws, issues of data Processing (including preservation) present one of the most vexing problems for Investigating Authorities and Organizations

whose information is requested in cross-border investigations. This is so for Investigating Authorities because they may be unable to “release” an Organization from its data preservation obligations until they know with certainty that they no longer need certain information. It is so for the subject Organizations 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 Investigating Authorities and subject Organizations in this regard can best be addressed through a dialogue in which the Organization is mindful of the Investigating Authority’s legitimate need for information and the Investigating Authority is mindful of the legal obligations of the Organization and the interests of Data Subjects whose information may be implicated in the investigators’ requests. In many instances, the Investigating Authority should consider whether its needs might be met through alternative mechanisms, such as phased productions, or receipt of aggregated or redacted/anonymized/pseudonymized information. Nevertheless, an Investigating Authority should demonstrate due regard by releasing an Organization from its data preservation obligations once it can appropriately do so.

Comment 3d: Investigating Authorities should retain Protected Data only so long as they are legally obliged to do so. In this regard, there generally is no difference in best practice between a litigation context and investigation context, except that in the context of investigations it may not be as clear to parties when a legal obligation to retain Protected Data preserved for the investigation 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 Investigating Authorities

to determine the status of an investigation.⁶⁰ In responding to inquiries about the status of an investigation, Investigating Authorities should bear in mind the interests and policies of the host country and those of any Data Subjects. One objective should be to “release” parties from their preservation obligations as soon as possible, consistent with the needs of the investigation.⁶¹

Principle 4

Where the laws and practices of the country conducting an investigation allow it, the Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority 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.

Comment 4a: U.S. experience has shown that there is real value in early and frequent engagement between the Investigating Authority and the party being requested to produce information. When the parties are candid and forthright with investigators, and investigators are willing to listen and engage with

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

61. 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).

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 court-ordered data protection), an Organization should look for opportunities to proactively alert Investigating Authorities to potential legal conflicts and propose measures designed to protect data. In jurisdictions where Investigating Authorities will entertain it, early discussions regarding scope may allow the Organization 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 Investigating Authorities 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.⁶²

Comment 4c: The issues under investigation may evolve over time as leads are followed and threads of information are developed more fully until resolved—favorably or unfavorably. Investigating Authorities must be able to go where the evidence leads. In many ways, these needs are antithetical to the trans-

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

parent, 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 accuracy and proportionality,⁶³ 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 GDPR Articles 24(1), 25, and 28(1), appropriate technical and organizational measures must be adopted to ensure the security and confidentiality of the processed data. In-country evaluation by a local entity versus immediate cross-border transfer and disclosure should be considered.⁶⁴ Notice should be given to the Data Subject as soon as practicably and appropriately possible, recognizing that providing notice can, for instance, undermine an investigation and may have to be delayed.⁶⁵

Comment 4e: In disclosing information about global operations and educating Investigating Authorities regarding potential data protection issues, Organizations should be prepared to

63. See, e.g., GDPR art. 5(b)–(d).

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

65. Note that exceptions are provided in GDPR art. 14(5)(b) where providing notice would “seriously impair” the objective of the Processing; see also Article 29 Data Protection Working Party, *Guidelines on Transparency under Regulation 2016/679*, at 28, 17/EN/WP260 (Dec. 12, 2017), available at http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=50057.

Moreover, there are limits on how far an Investigating Authority will go (or can be expected to go) in protecting the rights of Data Subjects. See *Producing Information*, *supra* note 46.

explain how proposed measures to limit and channel disclosure meant to minimize Data Protection Law conflicts are compatible with, and not intended to impede, investigation objectives.

Principle 5

Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.

Comment 5a: To encourage and facilitate cooperation in Government Investigations and voluntary compliance with requests for information by Investigating Authorities, governments sometimes enact laws that limit 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 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. SAFE WEB Act.⁶⁶ That law allows the FTC to share information with non-U.S. agencies in consumer protection cases upon request if: (1)

66. 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.*

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.⁶⁷

Despite the limitations on their ability to share information, governments often investigate conduct or transactions that cross borders or even span the globe.⁶⁸ Some matters may pique the interests of other nations. Examples of non-criminal matters include mergers involving large international Organizations or other competition cases involving monopolistic or other anti-competitive practices that cross international borders. Although Investigating Authorities 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 authorities to generalized discussions about legal theories and investigative strategies because authorization statutes preclude sharing actual information about the entities and subject matter of investigations.

Comment 5b: The inability of Investigating Authorities to share information has consequences for Organizations subject to investigation by more than one government for conduct involving common facts or transactions. Such Organizations 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

67. See 15 U.S.C. § 46(j)(1)–(4).

68. Investigations into the manipulation of London Interbank Offered Rate (LIBOR) and currency exchange rates are a good example: see, e.g., DOJ Division Update Spring 2016, <https://www.justice.gov/atr/division-operations/division-update-2016/> (noting international enforcement cooperation across multiple jurisdictions in foreign currency exchange manipulation investigations).

others. At the conclusion, Organizations 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 Organization 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, Organizations may be able to coordinate the timing of investigations and lessen their burden of producing information to multiple Investigating Authorities. Most importantly, by encouraging coordination and cooperation among Investigating Authorities, the Organization 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 Government Investigation that an Organization can best control. In many instances, only the Organization can authorize governments to share information that they otherwise could not share.⁶⁹ Also, in some instances the Organization 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 or related investigation in another country. In such situations, the Organization should consider whether its interest may, consistent with applicable Data Protections Laws (*see* Comment 5e, *infra*), best be served by granting waivers to encourage and facilitate cooperation and coordination among Investigating Authorities. An important factor for the Organization to consider is that once enforcement actions in one jurisdiction are filed against a mul-

69. The Organization's ability to authorize such further disclosure may, however, be subject to obtaining appropriate Data Subject input.

tinational Organization, 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 Organization has proactively granted a waiver and cooperated with other jurisdictions, its cooperation has the potential to reduce penalties.

Comment 5d: Assuming an Organization decides to grant waivers that allow countries to share information, it should carefully consider the scope of any waiver it grants, and especially whether it will allow Investigating Authorities to share information protected by a legally-recognized privilege or applicable blocking statute. In this regard, U.S. law generally recognizes that communications between an Organization's managers and in-house attorneys, as well as communications between the Organization's managers and other select employees, may be privileged. Not all countries recognize such privileges. Accordingly, when granting waivers to Investigating Authorities, Organizations 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.⁷⁰ Similarly, by their very nature, dawn raids may result in the capture of more information than the Investigating Authorities need for their investigation. Indeed, dawn raids may result in the acquisition of information that is wholly irrelevant to the matter or beyond the scope of the investigation. In those cases, assuming the subject of the investigation has a chance to allow sharing among multinational investigators, the Organization

70. 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>.

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 Organization 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 Organization 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

Investigating Authorities 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 Investigating Authorities may, consistent with Data Protection Laws, 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 authorities to enter into Memoranda of Understanding and other cooperative arrangements with their foreign counterparts. Authorities 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.⁷¹

Comment 6b: Given the potential benefits, Investigating 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 Organizations that manifest good-faith efforts to cooperate in an investigation offer to facilitate the flow of information between governments. By acceding to such offers, Investigating Authorities may help reduce the subject's costs of compliance with investigative demands and thereby encourage cooperation by other subjects in future investigations. A more immediate benefit is that all concerned Investigating Authorities 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

71. See ANTITRUST GUIDELINES, *supra* note 20, at ¶¶ 5.1.3, 5.1.4.

should reach results that are approximately consistent, if not identical.

Principle 7

Courts and Data Protection 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.”⁷² 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.”⁷³ As noted earlier, Government and Internal Investigations implicate the law enforcement interests of foreign sovereigns, and may involve the specter of significant corporate exposure. Accordingly, the stakes may be high for both the country conducting the investigation and the Organization that is the subject of the investigation (the public interest and the collateral consequences of civil law enforcement proceedings can be far reaching). The Organization’s decisions of whether and how intensely to assert any conflicts-of-laws may be difficult. An interesting question is how courts and Data Protection Authorities 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, as

72. 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)).

73. *Id.* at 10.

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.⁷⁴ 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.⁷⁵

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 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

74. *Id.* at 10 n.30.

75. See ANTITRUST GUIDELINES, *supra* note 20, at ¶ 4.1; Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party at 15, *In re Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation* (No. 17-2), 2017 WL 6383224, https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf [hereinafter EU Microsoft Amicus].

where the information is located and any potential consequences for [its] foreign relations.”⁷⁶ 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.”⁷⁷ 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.”⁷⁸ 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 Data to that which they truly need.⁷⁹

76. 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)).

77. *Id.* at *12–13.

78. *Id.* at *13.

79. See EU Microsoft Amicus at 12–16, *supra* note 73.

Principle 8

A party's conduct in undertaking Internal Investigations and complying with Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, 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 addresses the standard governments should apply when considering the legitimate governance needs of Organizations 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 Data Protection Authorities, Investigating Authorities, and courts that may be required to evaluate the parties' actions. In these situations, a standard of good faith and reasonableness should apply, particularly when guidance is unavailable, vague, or inconsistent. Data Protection Authorities assessing the conduct of an Internal Investigation should recognize the substantial benefits that accrue to the Organization and to society when Organizations detect, stop, prevent, and punish illegal conduct by their employees. When conflicts of law do arise, Organizations should make good-faith and reasonable efforts to mitigate risk, recognizing that full compliance with conflicting obligations may not be possible. Conversely, when called upon to evaluate party actions and responses, Data Protection Authorities, Investigating Authorities, and courts should consider the conflicting obligations and base their judgments on consideration of the Organization'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 and what data is actually protected. Depending on which country's law applies and the specific circumstances of the matter under investigation, factors including the Protected Data's country of origin and the relevant Data Subject's residency or nationality may also be considered in assessing how to proceed. The Data Controller must ultimately make decisions about how to effectuate Processing and potential transfer and disclosure 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 Investigating Authorities or Data Protection Authorities. 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.⁸⁰

Comment 8b: There may be situations in which courts, Data Protection Authorities, or others may be called upon to evaluate an Organization's compliance efforts in a Government Investigation that the host country finds do not adequately support its

80. 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.").

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 Organization'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, in light of the competing if not conflicting demands, and governed by a good-faith and reasonableness standard.

Comment 8c: Organizations can—even when acting in good faith and reasonably—still make mistakes in the view of the Data Protection Authority or Investigating Authority. Investigating Authorities should view these perceived shortcomings in light of overall efforts of complying with conflicting regulatory schemes. Good faith and reasonableness includes a range of interpretations and judgments of how to comply with Data Protection Laws. Thus, two Organizations may approach the same inquiry differently but still reasonably. There is no one-size-fits-all assessment, and the same Organization may respond to regulatory inquiries differently but still reasonably and in good faith. Across cases, the outcome of the legal analysis of complying with Data Protection Laws may differ for valid reasons.