wgs

The Sedona Conference

Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations

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

January 2025
Public Comment Version
Submit comments by March 6, 2025,
to comments@sedonaconference.org

Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations

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

JANUARY 2025 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief
John E. Davis

Contributing Editors
Lori Baker
Paul Brabant
Walter Delacruz
W. Warren Hamel
Ronald J. Hedges
Wayne Matus
William Marsillo
Mariano Peruzzotti
David Shonka

Steering Committee Liaison
Leeanne Mancari

Staff Editors
David Lumia
Michael Pomarico

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, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the public comment version of The Sedona Conference's *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations* ("*Commentary*"), 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 published 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, intellectual property rights, data security and privacy law, and artificial intelligence. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG6 is to develop principles, guidance, and best practice recommendations for information governance, discovery, and disclosure involving cross-border data transfers related to civil litigation, dispute resolution, and internal and civil regulatory investigations.

The Sedona Conference acknowledges Editor-in-Chief John Davis for his leadership and commitment to the project. We also thank Contributing Editors Lori Baker, Paul Brabant, Walter Delacruz, Warren Hamel, Ron Hedges, Wayne Matus, Bill Marsillo, Mariano Peruzzotti, and David Shonka for their efforts, and Leeanne Mancari for her guidance and input as Steering Committee liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were circulated for feedback from the Working Group membership. Other members provided feedback at WG6 meetings where drafts of this *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by March 6, 2025, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, trade secrets, and artificial intelligence. 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. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Kenneth J. Withers
Executive Director
The Sedona Conference
January 2025

Table of Contents

This *Commentary, Principles, and Best Practices for Addressing Data Risks Associated with Dawn Raids in Cross-Border Investigations* ("*Commentary*") presents and discusses principles and best practices to manage data risks associated with dawn raids in criminal and civil/administrative enforcement investigations that may involve multiple jurisdictions. The *Commentary* seeks to address the unique impacts that dawn raids have on organizations' abilities to comply with data privacy and data protection requirements in cross-border matters.

Part I introduces the issues and describes the scope of the *Commentary*. Part II provides information about the prevalence and risks of dawn raids. Part III sets out eight principles for approaching and managing data risk in dawn raids and is itself divided into two sections. The first section discusses best practices of agencies with respect to achieving their goals while respecting the information rights of those affected by such raids and minimizing the collateral impact of the investigation. The second section considers best practices for organizations to follow when their information is affected by a dawn raid, whether as the subject of the raid or as a third party. Finally, an appendix provides an "Organization Data Checklist in Preparation for Dawn Raids."

I. INTRODUCTION

Government authorities, regulators, and law enforcement agencies are commonly granted extensive powers and resources to support investigations. One of the more distinctive and dramatic powers is to conduct a "dawn raid," whereby authorities—often based on judicial authorization, but sometimes based on administrative process—may, without prior notice, physically or "virtually" enter premises to search for and copy or seize information called for in the investigation.[1] Authorities view such on-site searches, and their surprise nature in particular, as critical to investigating potential misconduct in areas where concealment is expected and the specter of destruction of evidence is ever-present.[2] These raids are increasingly common in both criminal and civil/administrative investigations and may be coordinated among agencies across jurisdictions. They are at once intrusive, disruptive, and potentially threatening to the privacy and confidentiality of an organization's and a third party's seized information. The increased global use of raids coincides with continuing expansion and globalization of data flows and simultaneous surge in data privacy regulations, multiplying the resulting risks and complications. Those risks and uncertainties are compounded by the increasing prevalence of remote working practices.

What makes a dawn raid different from other types of investigative demands? The highly complex nature of multi-jurisdictional investigations causes organizations great uncertainty in preparing for and dealing with dawn raids. Dawn raids are distinct in form and effect from investigative tools that seek information on notice (such as subpoenas, civil investigative demands, requests for information, or self-executing warrants). In concept, a government authority would resort to a dawn raid when it has decided that the notice-based investigative process is insufficient to obtain information believed necessary to carry out an investigation. This decision may rest on any number of factors: e.g., the government may suspect that the organization will not fully comply with a subpoena on notice; the government may conclude that a search will be the best way to get a complete picture of the organization's activities; the evidence may be transient, mobile or threatened with destruction; and/or the agency may wish to emphasize the importance of the inquiry.

Conducting the search without notice provides the raided organization with little control over the scope, review, and use of its seized information. Raids provide fewer opportunities to perform risk assessments tailored to the inquiry, to negotiate with the investigator, and to assert legal challenges prior to disclosure of sensitive information. Organizations are further limited in their ability to control the subsequent use and transfer of protected information seized in the raid. They also are

---

[1] Consistent with practice across varying jurisdictions, this Commentary interchangeably uses the terms dawn raid, raid, search warrant execution, and search and inspection in referencing dawn raids. Similarly, we here use the terms authorities, government authorities, regulators, and agencies interchangeably, unless otherwise indicated.

[2] *See* Case T-439/07, Coats Holdings Ltd. v. European Comm'n (June 27, 2012) ("[I]t is normal for the activities that imply those practices and anti-competitive agreements to take place clandestinely, and for meetings to be held in secret, most frequently in a non-member country, and for the associated documentation to be reduced to a minimum."), cited in INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL ("INDECOPI"), DAWN RAID GUIDELINES, at 7 n.10 (2020), *available at* https://cdn.www.gob.pe/uploads/document/file/2131121/Dawn%20Raids%20Guidelines.pdf.

limited in the legal and practical means of mitigating a range of accompanying data risks, including loss of control, confidentiality, privacy, and privilege. As a practical matter, once the raid has commenced, some effects may be irreversible. Thus, investigating and understanding the risk, business impact, and response options to a dawn raid differs from responding to other types of investigative demands.

Scope: This *Commentary* addresses cross-border, data privacy, data protection, and data security implications of dawn raids in criminal and civil and/or administrative enforcement contexts. Dawn raids are perhaps most notably associated with European enforcement investigations but also are widely used in other jurisdictions, including countries in the Americas and Asia. Accordingly, the topics discussed in the *Commentary* are not intended to be jurisdiction-specific. Rather, they identify and address principles and best practices applicable in a variety of locations.

This *Commentary* primarily focuses on dawn raids occurring in the context of actual or potential criminal proceedings, although in some jurisdictions authorities may also use dawn raids to conduct civil and administrative investigations.[3] Nonetheless, the practices and risks share much in common, and many of the topics discussed in this *Commentary* may be informative to those who are concerned with dawn raids in civil investigations in those jurisdictions where they are allowed. This *Commentary* complements The Sedona Conference's *International Investigations Principles*,[4] which addresses cross-border transfers of data in the context of civil governmental and internal investigations on notice, but pointedly does not delve deeply into dawn raids.

[3] For example, the European Commission ("EC") may on its own decision or based on judicial authorization where required (e.g., where the assistance of police or an enforcement authority is necessary), conduct a dawn raid in EU member-states to follow up on prior information-gathering activities or to resolve incorrect or misleading responses to prior questioning. Council Regulation (EC) No. 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, Art. 20(2), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32003R0001 [hereinafter EU Competition Regulation 1/2003]. National competition authorities in other jurisdictions, such as the UK's Information Commissioner's Office ("ICO") generally have similar powers.

[4] The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018).

II. BACKGROUND: THE FREQUENCY AND RISKS OF DAWN RAIDS

A. Dawn Raids: Growing Use on a Global Scale

The use of dawn raids as an official investigative tool appears to be growing. Agency and public reports indicate that criminal, competition, tax, and enforcement authorities worldwide have increased their use of dawn raids instead of or in addition to using cooperative methods to locate and seize evidence of wrongdoing. There was a brief decline as a result of restrictions relating to the COVID-19 pandemic, but the frequency of raids returned to its prior trajectory once health and safety protocols allowed.[5] Changes in the authorizing laws have also encouraged this increase.[6]

B. Risks Relating to Dawn Raids

Organizations face substantial legal and business risks in connection with dawn raids. Third parties whose information is held by a raided organization share many of these risks. Documents and other materials seized during a raid may be used not only as evidence in enforcement actions by the agencies conducing or sponsoring the raid, but under certain circumstances may also be made available to other authorities and sometimes private litigants in related and unrelated matters. The very occurrence of a raid of an organization's offices may also lead to inquiries by authorities in other jurisdictions, who may seek access to the seized materials. A dawn raid also poses myriad collateral risks to the organization's operations, including the loss of necessary operating equipment and records, adverse publicity, conflicts with business partners and competitors, and the resulting financial implications. As discussed below, once the raid has been conducted, the seized information is out of the organization's control and often may not be easily retrieved, which highlights the need to have strong controls on the conduct of the raid before, during, and after the raid.

1. Investigative and Evidentiary Risk

The most immediate and critical risk of a dawn raid is an organization's involvement in a criminal investigation. An organization must act immediately, generally with legal counsel, to assess and respond to such risk. Lacking prior notice of a raid, organizations have far less ability to understand areas of inquiry, strategize a response, and attempt to influence the governmental actor regarding the scope, timing, method, and uses of information obtained in the raid. This includes a more limited ability to bring legal challenges to seizures. (See Principle 1.)

---

[5] *E.g.,* Emilio De Geiori, *Antitrust in focus - April 2022,*" JDSUPRA (May 4, 2022), https://www.jdsupra.com/legalnews/antitrust-in-focus-april-2022-4697260/.

[6] For example, European competition authorities received more uniform and sometimes broader inspection powers with the 2018 enactment of the ECN Plus Directive. Directive of the European Parliament and of the council to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, 2017/0063 (COD), Art. 6 (Nov. 21, 2018) ("ECN Plus Directive"), http://data.consilium.europa.eu/doc/document/PE-42-2018-INIT/en/pdf, discussed in Maciej Marek, *Focus on antitrust dawn raids in Europe*, DENTONS (Sep. 19, 2019), *available at* https://web.archive.org/web/20190920200435/https://www.jdsupra.com/legalnews/focus-on-antitrust-dawn-raids-in-europe-77155/.

Dawn raids also pose risks with respect to the use of the copied records as evidence in future enforcement actions and even potentially in civil litigation. Such records are, first and foremost, evidence the government can use in an ongoing or future complaint against, or prosecution of, the organization, its employees, and its business partners. That the agency obtains the documents in bulk, typically before review by the organization's lawyers, may undermine the organization's ability to identify the government's priorities and effectively speak with employees about conduct in scope. Even if the material ultimately does not support the government's suspicions, the records may alert the agency to other related or unrelated conduct, which it may choose to share with other criminal or civil enforcement agencies in certain circumstances.

The raid immediately imposes on the organization evidentiary responsibilities as well. To the extent that it did not before, the organization now knows it is involved in an investigation, generally triggering an obligation to take reasonable steps to preserve relevant evidence. This preservation obligation covers not only recorded information seized in the raid but may also include related information left behind and in other locations. It may also cover information under the organization's control but maintained by third parties. Further, the preservation obligation may extend beyond the investigation, in contemplation of related civil and criminal actions in different jurisdictions. Among other actions, the organization generally should consider a deconfliction process, instruct employees to preserve relevant information, and change its document management practices and rules to ensure the data is kept at an IT level. The failure to implement such a "legal hold" can be significant.[7] Spoliation and obstruction concerns have breathed new life into many an investigation that was floundering on the merits.

A dawn raid may open a Pandora's Box of associated dangers. Documents seized in a raid pose elevated risks of disclosure of privileged information, as the organization may not always be able to prescreen the documents, and impromptu screens may be less thorough. A raid in any jurisdiction may sweep up privileged communications in sometimes chaotic circumstances, increasing the chances for disruption, disclosure, and waiver, even where attorneys of the organization are present and seek to quarantine privileged information. Effective screening may be frustrated by any number of factors, including the volume of data, storage medium inaccessibility, incomplete knowledge, and ineffective search terms. Remote working practices, including those affording counsel only "virtual" opportunities to aid in identifying privileged information, can make privilege protection even more difficult. Moreover, the location of the raid may be determinative, as "[p]rotections afforded to documents and information related to a party's communications with counsel and attorney work-product protections vary by jurisdiction."[8] Outside of the U.S., for example, communications between in-

[7] *E.g.*, The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 354, 359–61 (2019).

[8] The Sedona Conference, *Commentary on Cross-Border Privilege Issues*, 23 SEDONA CONF. J. 475, 507 (2022) [hereinafter *Sedona Cross-Border Privilege Commentary*].

house counsel and employees of the organization are often *not* considered privileged.[9] Authorities in some jurisdictions may also demand the waiver of privilege to secure cooperation credit.[10]

Further, "[o]nce information is produced in one jurisdiction, there is a greater likelihood that it will be discoverable in other jurisdictions."[11] Documents seized in connection with an enforcement action may be targeted in follow-on litigation, by way of civil process seeking copies of records "produced" in the search. While there is a strong presumption of secrecy in certain jurisdictions as to documents obtained in raids,[12] that will not prevent a private litigant that learns of the raid from demanding those documents directly from the organization. Alternatively, where a dawn raid is carried out by a civil or administrative authority, such as an EU state competition authority operating under Articles 101 and 102 of the Treaty on the Functioning of the European Union, seized records may be subject to disclosure to third parties in private litigation.[13] Seizures and subsequent transfers may also implicate contract rights held by business partners or trigger an audit demand.

2. Cross-Border Risk

Raids may be conducted simultaneously or sequentially in multiple locations and jurisdictions, with authorities coordinating and sharing seized information. This compounds the risk of information disclosure contrary to legal or contractual restrictions on access, including data privacy, banking or state secrets, International Traffic in Arms Regulations restrictions, employment restrictions, medical information, privileged information, and proprietary information. Moreover, a publicized raid of an organization's offices in one jurisdiction may spark the interest of enforcement agencies in other jurisdictions in which the organization operates. For example, one investigation into a multinational construction conglomerate's alleged bribery of Brazilian government officials reportedly began with an investigation of a money laundering operation at a gas station in Brasília and subsequent raids of

---

[9] *Id.* at 505.

[10] Megan Zwiebel, *In New Guidance, SFO Indicates It Wants Companies to Waive Privilege*, ANTI-CORRUPTION REPORT (Oct. 16, 2019), https://www.anti-corruption.com/4103541/in-new-guidance-sfo-indicates-it-wants-companies-to-waive-privilege.thtml. *But see* The U.S. Justice Manual ("USJM") § 9-28.710 (cooperating organization is not required to waive the attorney-client privilege or attorney work product protection); SEC Enforcement Manual § 4.3 (same).

[11] *Sedona Cross-Border Privilege Commentary*, *supra* note 8, at 507.

[12] For example, where a U.S. dawn raid is conducted in the context of a federal grand jury investigation, the records seized in the raid should be held as confidential by the Department of Justice, either as grand jury materials subject to Rule 6(e) of the Federal Rules of Criminal Procedure, or as exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552, based on exemptions (b)(4) and (b)(7). Thus, a civil litigant seeking access to the seized records from the government is unlikely to obtain such access, although civil process may be brought to force the organization to produce copies itself. Such secrecy is not the rule in all jurisdictions, and it may be overridden in certain circumstances. *See, e.g., In re* Application of the Committee on the Judiciary, U.S. House Of Representatives, for an Order Authorizing the Release of Certain Grand Jury Materials, 414 F. Supp. 3d 129 (D.D.C. 2019) (discussing exceptions to grand jury secrecy rule, including that materials may be shared for judicial proceedings, including congressional impeachment inquiry).

[13] Any such disclosures to third parties would be subject to the confidentiality limitations of Art. 6 of Directive 2014/104/EU.

related entities.[14] These investigations eventually involved enforcement actions by Brazil, the U.S., and Switzerland related to the same conduct, culminating in a $3.5 billion multinational settlement. Three years later, the parent organization filed for bankruptcy protection after investigations into unrelated bribery allegations in Argentina, Mexico, Peru, and numerous other countries in the Caribbean and South America.[15]

Cooperation among enforcement agencies has become more regularized with the use of Multinational Legal Assistance Treaties in the U.S. and similar mechanisms in other countries. For example, Switzerland—historically reluctant to share bank and financial records sought by foreign enforcement authorities—has introduced new mechanisms to work with foreign authorities in prosecuting white collar crimes and tracking the proceeds of illicit activities.[16] Another noteworthy instance within the realm of international bribery is the collaboration between the U.S. and enforcement agencies across Europe, South America, and Asia to enter into multiple Foreign Corrupt Practices Act resolutions involving multinational corporations during 2019. A raid conducted under such multilateral arrangements would undoubtedly involve the cross-border exchange of information.

3. Business Implications

Dawn raids may impact an organization's ability to carry on with its daily operations. There may be a police or inspector present onsite during the raid, bringing customer-facing and back-office business to a halt. Even if the raid can be contained in an inconspicuous area, the police or inspector will be occupying a physical space, such as a conference or IT room (or two or three), or server space, that will be unavailable for organization use.

The search team will be occupying and interacting with the office and each search site, as well as targeted systems, including seizing and copying files and equipment that employees depend on to complete day-to-day tasks. In the process, certain system accessibility might be limited, and passwords could potentially be deactivated. If the raid cannot be completed in one day, inspectors may seal premises and commandeer portions of systems pending completion. Inspectors may request to interview certain employees, pulling those individuals away from their desks for hours. Beyond the loss of productivity, an employee being interviewed creates a risk of uncontrolled disclosure of

---

[14] David Segal, *Petrobras Oil Scandal Leaves Brazilians Lamenting a Lost Dream*, N.Y. TIMES (Aug. 7, 2015), https://www.nytimes.com/2015/08/09/business/international/effects-of-petrobras-scandal-leave-brazilians-lamenting-a-lost-dream.html.

[15] Press Release, U.S. Dept. of Justice, Odebrecht and Braskem Plead Guilty and Agree to Pay at Least $3.5 Billion in Global Penalties to Resolve Largest Foreign Bribery Case in History (Dec. 21, 2016), https://www.justice.gov/opa/pr/odebrecht-and-braskem-plead-guilty-and-agree-pay-least-35-billion-global-penalties-resolve; *Brazil's Odebrecht files for bankruptcy protection after years of graft probes*, REUTERS (June 17, 2019), https://www.reuters.com/article/us-odebrecht-bankruptcy/brazils-odebrecht-files-for-bankruptcy-protection-after-years-of-graft-probes-idUSKCN1TI2QM.

[16] Federal Act on International Mutual Assistance in Criminal Matters § 351.1, https://www.admin.ch/opc/en/classified-compilation/19810037/201903010000/351.1.pdf; *see also* Press Release, U.S. Dept. of Justice, United States and Switzerland Issue Joint Statement Regarding Tax Evasion Investigations, https://www.justice.gov/opa/pr/united-states-and-switzerland-issue-joint-statement-regarding-tax-evasion-investigations.

information, which may pose a significant threat to the organization. A dawn raid is a spectacle and tends to undermine productivity even if employees are working remotely or can remain at work and access the tools necessary to do their job.

The business disruptions may continue after the raid has ended. Media coverage is common, and for high-profile raids, an organization will need to devote significant time and attention to public relations. Customers may be reticent to deal with an organization under government investigation. Competitors may potentially use the raid to bolster their legal actions against the subject of the investigation, or they may even have filed complaints to the authorities that triggered the raid in the first place. The public disclosure of a prior dawn raid can also have a significant impact on an organization's chances of participating in or winning a public tender. Public information about the execution of a dawn raid may raise concerns about the organization's integrity, compliance with regulations, ethical standards, and the organization's adherence to legal requirements, including those related to the tendering process itself. For example, procuring entities may view the organization as a higher compliance risk and choose to exclude it from the tendering process.

III. PRINCIPLES AND BEST PRACTICES WITH RESPECT TO DAWN RAIDS

The Principles set out below are intended to guide organizations in planning for and responding to dawn raids and to promote awareness and consistency among government agencies. Principles 1-5 identify data best practices among agencies for planning and conducting dawn raids. Principles 6-8 identify best practices for organizations in preparing for and responding to data implications of dawn raids.

A. Principles and Best Practices for Authorities

This *Commentary* does not purport to minimize the importance and effectiveness of dawn raids or instruct government agencies how they should go about conducting investigations. Rather, the *Commentary* has collected best practices and principles followed by various agencies conducting raids to support their critical missions. Dawn raids present complex and evolving challenges; this *Commentary* is intended to assist authorities by considering the level of process and transparency to be provided *before* obtaining the highly sensitive data often involved in these raids, and the potential collateral data risks that raids may present to third parties and regarding activities outside the scope of the investigation.

***Principle 1*.** **Dawn raids should be conducted based on a process that provides for meaningful pre- and/or post-raid review by an independent authority.**

Comment 1(a). *Right to independent review.* A fundamental principle across jurisdictions is that agency power must be subject to enforceable independent limitations, to provide guidance and guard against overreach.[17] Perhaps the most significant of these limitations is the right to independent review by a qualified tribunal of the authorization and conduct of the raid. As stated by the European Data Protection Supervisor in its Opinion 7/2019 concerning electronic evidence in criminal matters:

> [E]ffective protection of fundamental rights in the process of gathering electronic evidence cross-border requires *greater involvement of judicial authorities in the enforcing Member State*. They should be systematically involved *as early as possible* in this process, have the possibility to review compliance of orders with the Charter and have the obligation to raise grounds for refusal on that basis.[18]

---

[17] Indeed, such limitations are seen as vital in upholding the perception of legitimacy of agency action. One need look no further than scandals in the U.S. relating to asserted agency overreach and failures of oversight, such as the controversy over obtaining FISA warrants. *See, e.g.,* OFFICE OF THE INSPECTOR GENERAL, U.S. DEPT. OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (Dec. 2019) (rev.).

[18] European Data Protection Supervisor ("EDPS"), EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, Executive Summary 3 (Nov. 6, 2019), https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf (emphasis in original) [hereinafter EDPS Opinion 7/2019]. *See* The International Competition Network ("ICN") Guiding Principles for Procedural

Such judicial review helps to promote the existence of clear standards in terms of scope and authorization before an authority may enter premises and seize information, and to create effective and timely means by which impacted organizations and persons can raise legal objections to the raid in its aftermath. While the trend appears to be toward increased and earlier judicial involvement, considerable variation exists among jurisdictions and agencies as to the sequence and level of access to the courts that private parties may have in connection with dawn raids.[19]

Comment 1(b). *No-warrant raids and other judicial means of enforcement.* Whether raids should proceed only upon the issuance of a warrant from an independent judicial authority varies greatly among agencies and jurisdictions and has received considerable attention in the courts.[20] The ability of agencies to decide for themselves whether a raid is appropriate and how it may be conducted raises concerns of accountability and actions that may result in the abrogation of rights before they may be asserted.[21] Some courts have interpreted the laws of their jurisdictions to require judicial warrants and have therefore precluded the use of evidence seized outside of such requirements.[22] Other courts,

---

Fairness in Competition Agency Enforcement, Principle Seven ("Judicial Review/Appeals: Competition agency enforcement proceedings should include the right to seek impartial review by an independent judicial body."), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_GuidingPrinciples_ProFairness.pdf (last visited Dec. 12, 2024).

19 *See generally* EUROPEAN COMPETITION NETWORK, ECN WORKING GROUP COOPERATION ISSUES AND DUE PROCESS: INVESTIGATIVE POWERS REPORT (Oct. 31, 2012) § 2.1, 3.1 (2012) [hereinafter INVESTIGATIVE POWERS REPORT], https://competition-policy.ec.europa.eu/document/download/357ac0f6-92fb-41aa-b1ad-a906fcdd832d_en?filename=investigative_powers_report_en.pdf (discussing EC rights and processes).

20 *See id.* § 2.3.1 at 8–9 (listing 16 jurisdictions that permit competition authorities to make inspection decisions and 14 jurisdictions that require authorization by court warrant).

21 The EC, for example, is authorized to conduct raids of organizational premises without warrants in support of investigations. Warrants are generally required only for unannounced inspections of personal premises. Members of the EU subject to their national laws, in general, have similar powers. So do certain non-EU jurisdictions: the UK's ICO may issue an assessment notice and conduct no-notice inspections of premises, without a warrant, to determine whether a controller or processor of personal information is complying with data protection legislation, such as the GDPR or the UK Data Protection Act of 2018. These inspections can extend to any UK private business that controls or processes personal information. The evidence subject to a privacy raid can be particularly broad, and some laws put the burden on the organization to prove compliance (e.g., the accountability principle of the GDPR and similar legislation).

22 For example, on April 26, 2018, the Belgian Court of Cassation confirmed that competition dawn raids without prior warrant issued by an independent court are unlawful, and that evidence obtained through such unlawful raids was subject to an exclusionary and "fruit of the poisonous tree" rule and must be removed from the case file. This was based on the court's holding that the Belgian Constitution is more protective than Article 8 of the European Convention on Human Rights ("ECHR"), under which a judicial warrant may not always be required. *See Dawn raids without prior judicial warrant are unlawful: Court of Cassation confirms milestone judgment of Brussels Court of Appeal*, EUBELIUS (June 15, 2018), https://www.eubelius.com/en/news/dawn-raids-without-prior-judicial-warrant-are-unlawful-court-of-cassation-confirms-milestone. And in the U.S., consistent with the Fourth Amendment to the U.S. Constitution, which protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures," raids in support of criminal inquiries typically require a sufficiently supported judicial warrant, including a showing of "probable cause" a crime has been committed and "a fair probability that contraband or evidence of a crime will be found in a particular place" specified in the search warrant. U.S. CONST. amend. IV; Illinois v. Gates, 462 U.S. 213, 238, 283 (1983).

sometimes pointing to efficiency and exigency concerns, have upheld the right of agencies to act without a warrant so long as there is a meaningful and timely post-raid recourse to an impartial tribunal in order to retrieve seized data and restrict its use, including the ability to appeal warrants or post-raid judgments on issues of law and fact.[23] In June 2024, the European Union Court of Justice Advocate General issued an advisory opinion that allowing competition authorities to conduct email searches without a warrant during dawn raids is consistent with Article 7 of the Charter of Fundamental Rights of the European Union, so long as there is a legal framework with adequate safeguards against abuse such as ex post facto judicial review.[24]

Comment 1(c). *The scope of seizure should not exceed the needs of the inspection.* Clear and particularized notice of the scope of search, justified by its legitimate and articulated purposes, should be submitted to the authorizing entity in advance of the raid and later may be shared with the subject of the raid to promote transparency. While the timing of disclosure varies, it should take place in time to permit meaningful review of the actions. The authorizing entity, consistent with law enforcement imperatives and practicalities as well as familiar privacy law principles of minimization,[25] should actively work to limit the scope of raids to avoid overreach and "fishing expeditions," which present heightened risks of impact to the data rights of raid subject and third-parties.[26] The use of other investigative tools to obtain information, such as demands for production on notice, should be considered as alternatives.[27]

Comment 1(d). *Post-raid challenges to seizures of information.* Organizations impacted by raids should be permitted meaningful and timely opportunities to bring legal challenges— including to seizures and

---

[23] In 2015, the ECHR held that dawn raids by the French competition authority violated both the rights of defense and the right to privacy, because there were insufficient means to judicially challenge the authorization of the raid and scope of information seized. ECHR, 5th Sect., Apr. 2, 2015, n°63629/10, n°60567/10, Vinci Construction and GTM Génie civil and Services v/. France**,** cited in *Antitrust Alert: Dawn Raids by French Competition Watchdog Trampled on Fundamental Rights,* JONES DAY (Apr. 21, 2015) https://www.jonesday.com/en/insights/2015/04/antitrust-alert—dawn-raids-by-french-competition-watchdog-trampled-on-fundamental-rights.

[24] Imagens Médicas Integradas et al. v. Autoridade da Concorrência, Cases C-258/23 to C-260/23 (responding to 2023 Portuguese Constitutional Court ruling that searching emails solely on the authorization of the Public Prosecutor's Office without prior judicial authorization based on Art. 21 of the EU Law on Competition, violated Portugal's Constitution), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=287318&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1. The opinion further stated that member-states may nevertheless impose warrant-type requirements based on national law where that would not "undermine the effectiveness of the prevention of anticompetitive practices within the European Union."

[25] *E.g.,* Brazilian General Data Protection Law, Art. 6; Ecuadorian Personal Data Protection Law, Art. 10.

[26] In Nexans France SAS and Nexans SA v. European Commission, Case T-135/09 judgement of Nov. 14, 2012, *available at* https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2012.399.01.0016.01.ENG, for example, the EU General Court annulled parts of the inspection decision because it was imprecise in its delimitation of the products concerned, which applicants claimed permitted an overly broad examination of the entirety of the organization's business in violation of general principles of EU law against arbitrary or disproportionate intervention in the sphere of private activities.

[27] *E.g.*, INT'L COMPETITION NETWORK, ANTI-CARTEL ENFORCEMENT MANUAL*,* Chapter 1, § 3.1.

subsequent uses of information— before impartial tribunals. This post-raid forum is critical to protecting the rights of the subject and third parties and ensuring fair and equitable conduct by authorities. Justice delayed may be justice denied, and the right to challenge must be sufficiently proximate so as not to frustrate the exercise of the right. For example, a process that limits post-review challenges of the conduct of the raid (as opposed to the determination to conduct the raid) until after the final decision on the merits of a matter has been found to provide insufficient immediate protection of rights, although there is no clear consensus in the courts on this principle.[28]

Moreover, opportunities for challenges to vindicate threatened rights must be aligned with incentives to do so. A process that permits only third parties in possession of potentially restricted information (e.g., a cloud service provider holding customer data) the right to challenge a raid or subsequent transfers, rather than the data subject, may provide insufficient protections. This concern is elevated in cases where the party in possession of the restricted information may not have standing to assert all of the rights available to the data subject, and may be prohibited from providing notice of the raid to the owner of the information.

Comment 1(e). *Exclusionary remedies.* In appropriate circumstances, courts should be empowered to issue "exclusionary" remedies under which evidence seized in violation of rights and processes must be returned, cannot be further transferred, and must not be used by agencies or others.[29] While a full treatment of this issue is outside of the scope of this *Commentary*, jurisdictions including the U.S. have well-developed bodies of law regarding such exclusionary rules (and exceptions), including "fruit of the poisonous tree" provisions that provide not only that evidence improperly seized cannot be used, but also that the investigators may not use other information obtained through the use of improperly obtained evidence.[30]

Although exclusionary rules can be an effective tool to impose accountability on agencies and ensure that they follow legal requirements surrounding dawn raids, there are societal costs that may be

---

[28] *E.g.,* Delta Pekárny AS v Czech Republic, App 97/11, ECHR 279, Oct. 2, 2014 judgment (NYR). *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.7 (generally discussing rights to judicial review of inspection actions of competition authorities of the EU and European Competition Network). *But see* Deutsche Bahn AG and Others v. European Commission (Case C-583/13 P) (ECJ 2015) (rejecting a challenge to a no-warrant raid based on unavailability of judicial review until after conclusion of the investigation; finding sufficient protections for fundamental rights in the EC's obligations in making decisions, various legal limitations on EC during inspection, the need for the EC to involve national authorities when force is required, and the subject's (eventual) right to review of the inspection by the European courts), *available at* https://curia.europa.eu/juris/liste.jsf?num=C-583/13&language=EN.

[29] *See Belgian Supreme Court confirms illegality of dawn raids due to the lack of a warrant*, STIBBE (June 1, 2018), https://www.stibbe.com/en/news/2018/june/belgian-supreme-court-confirms-illegality-of-dawn-raids-due-to-the-lack-of-a-warrant (discussing 2018 decision of the Belgian Supreme Court that dawn raids in the travel sector had been conducted illegally, given that protection offered by the Belgian Constitution is wider than Article 8 of the ECHR, and requiring information unlawfully obtained to be removed from the case file).

[30] In Spain, the National Court in 2015 annulled fines of €61 million imposed by the Spanish competition authority on five electricity companies and their industry association, which had been based on evidence seized in a raid with inadequately defined scope. *Antitrust Alert, supra* note 23.

suffered by suppressing evidence of criminality based on prosecutorial mistakes and misconduct, and it is largely a disfavored remedy. Indeed, seeking suppression in U.S. courts of evidence gathered by law enforcement outside of the U.S. and shared via intergovernmental agreement typically is an uphill battle with only very limited grounds for objection.[31]

***Principle 2*. The dawn raid procedures that authorities follow should be in writing, readily available, and consistently applied, and should inform private parties of their rights and the processes available to them for protecting those rights.**

Comment 2(a). *Transparency of subject legal rights and redressability of injury.* Legal rights are more sustainable when they are known, clear, and exist within a system permitting meaningful redress.[32] As a best practice, there should be a written and readily available statement of subjects' rights and the remedies available in connection with information seizures in a dawn raid. Such rights and remedies may include the right to review the authorizing instrument during the raid, to be present for the raid, to call counsel to be present for the raid, to have privileged and confidential information of subjects and impacted third parties protected pending review, and to timely seek judicial review.[33]

The following rights are consistent with the above principle.

1. **To review the authorizing instrument.**

2. **To require that the search be confined to the scope authorized in the writing, and accordingly, to be able to object to any excesses.**

---

[31] *See* United States v. Getto, 729 F.3d 221, 230–31 (2d Cir. 2013) (rejecting defendant's Fourth Amendment challenge to evidence received from Israeli National Police via Multinational Legal Assistance Treaty ("MLAT") because exclusionary rule applies only to foreign evidence where there is U.S. control or direction of the foreign investigation, an intent to evade the U.S. Constitution, or where the foreign agency's actions "shock the judicial conscience"), citing United States v. Lee, 723 F.3d 134, 139, n. 3 (2d Cir. 2013) (under the "international silver platter doctrine" the Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country).

[32] Certain authorities, including the EC and the Peruvian Competition authority (Indecopi), have issued detailed written standards and guidelines for raids which they make available publicly—although the guidance may not be considered binding in the courts. *See* Explanatory note on Commission inspections pursuant to Article 20(4) of EU Competition Regulation No 1/2003, European Commission, https://competition-policy.ec.europa.eu/antitrust-and-cartels_en; DAWN RAID GUIDELINES, INDECOPI, *available at* https://cdn.www.gob.pe/uploads/document/file/2131121/Dawn%20Raids%20Guidelines.pdf (last visited Dec. 12, 2024). *See also* AUSTRIAN FEDERAL COMPETITION AUTHORITY, GUIDANCE ON DAWN RAIDS (Oct. 2017), *available at* https://www.bwb.gv.at/fileadmin/user_upload/Englische_PDFs/Standpoints%20and%20Handbooks/Guidance_on_dawn_raids_final.pdf. *See generally* Annabel, Cédric & Jorge, *Safe-raids? Meaningful judicial review of dawn raids on business premises*," EU LAW ENFORCEMENT, https://eulawenforcement.com/?p=1495 (surveying dawn raid procedures of the Commission and 9 Member States along with their prior safeguards).

[33] In Argentina, for example, these rights find support in Article 18 of the Federal Constitution (right to due process and defense), the Criminal Procedure Code and other regulations such as Resolution 535-E/2017 of the Ministry of Security.

3. **Generally, to be present at the raid, and to have counsel present at the raid.**

4. **Generally, to decline to be interviewed to avoid providing potentially self-incriminating answers; to request that counsel be present if the interview occurs; and to have counsel if involved persons are arrested or detained and questioned off-site.**

5. **To request that privileged information (as defined in that jurisdiction) not be taken or reviewed, or if the claim of privilege is disputed, that potentially privileged information be segregated until a court determines entitlement.**

6. **To obtain an index to, and/or copy of, the information copied/seized.**

7. **To timely review investigative minutes to ensure accuracy, including the recording of objections raised.**

8. **To timely challenge the determination and conduct of the raid before an independent tribunal without obstructing agency action (although this may not necessarily prevent the raid from occurring).**

***Principle 3*. Dawn raids should be conducted in a manner narrowly tailored and proportionate to the circumstances and purpose of the action, so that the data rights of impacted persons are preserved and respected.**

Comment 3(a). *Raids should be proportional and tailored to legitimate purposes.* The use of dawn raids should be proportionate to the investigative need. Dawn raids in general should be used only where demands for information on notice would frustrate law enforcement purposes (as where there otherwise is a credible risk of spoliation of evidence or evasion of the demand), the inspection is appropriately and narrowly restricted to the subject matter and articulated purpose of the inspection, and the raid is conducted in a manner that preserves the information rights at issue (e.g., so that privileged information is not reviewed by inspectors outside of the privilege challenge process).

Comment 3(b). *Considerations to Promote Proportionality.* Heightened attention should be paid to ensuring that other less intrusive and less cooperative means of compelling disclosure to the agency are not available or would unacceptably undermine the investigative purpose.[34] Best practices may be promoted by asking:

---

[34] Proportionality principles are generally applied in structuring and limiting data transfers in international investigation and disclosure efforts. *See generally* The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557, 612 (2018) (Principle 4, cmt. 4d, citing GDPR art. 5(b)–(d)) ; *see also In re* Bard IVC Filters Prods. Liability Litig., 317 F.R.D. 562 (D. Ariz. 2016) (rejecting on proportionality grounds discovery request for marginally relevant document located in EU where most of the relevant materials were also in the U.S.); Principle 2 cmt. (citing FED. R. CIV. P. 26(b)(1) (scope of discoverable information restricted by proportionality; listing factors in proportionality determination).

- Can the evidence be obtained through other (less intrusive) means?
- Would a demand for information on notice frustrate law enforcement purposes? Is there a credible risk of spoliation of evidence absent the raid?
- Is a dawn raid appropriate for the level of offense being investigated?
- Are the rights of impacted persons adequately preserved through the warrant process and/or via post-raid challenge?
- Is the examination appropriately restricted to the subject matter and articulated purpose of the inspection?
- Is collection appropriately targeted (e.g., through use of data screening, filtering, and other minimization techniques) to mitigate risks to subject and third-party rights?
- What rules will be followed by the investigative team to ensure these principles are met, and that the raid is conducted in a manner to preserve the right to review?
- How is privilege to be protected?[35]

Comment 3(c). *Special considerations should apply to attorney and law office searches.* The risks to privileged and other protected information posed by raids of law offices are especially pronounced. Typically, special procedures must be followed and specific showings made to initiate such a raid, and special processes are put in place to protect privileged information. However, the nature and consistency of such protections vary widely across jurisdictions, as does the definition of protected information and who may enforce such protections.[36]

---

[35] Many agencies maintain such internal procedures. For example, in its Regulatory Action Policy, the ICO sets out its enforcement policy under the Data Protection Act of 2018. In general, it reserves dawn raids and other of its most intrusive enforcement powers for high-impact, intentional, willful, neglectful, and repeated breaches of data protection law. Further, in order to obtain such a warrant, the ICO will need to satisfy the court of the reasons for urgent access to the premises, and that providing notice would frustrate the purpose of the inspection, e.g., that evidence would be destroyed if notice was provided. INFORMATION COMM'RS OFFICE, REGULATORY ACTION POLICY (2018) at 12, *available at* https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf; DPA Section 149(2). *See also* COMPETITION & MARKETS AUTHORITY, COMPETITION ACT 1998: CMA GUIDANCE AND RULES OF PROCEDURE FOR INVESTIGATION PROCEDURES UNDER THE COMPETITION ACT 1998 (Mar. 2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288738/CMA8resp_CA98_CMA_Guidance_and_Rules_of_Procedure_SoR.pdf.

See also ICN ANTI-CARTEL ENFORCEMENT MANUAL, *supra* note 27, Ch. 1, § 3.1 (certain agencies will conduct a search only if other investigative tools would not be effective; setting out "needs" test asking "whether there are other reasonable and less intrusive means to obtain the information sought").

[36] *See generally* USJM, *supra* note 10, § 9-13.420 (Searches of Premises of Subject Attorneys), https://www.justice.gov/jm/jm-9-13000-obtaining-evidence. *See also* Klitzman, Klitzman, and Gallagher v. Krut, 744 F.2d 955 (3d Cir. 1984)

These problems and the difficulties of adequately protecting privilege were on display in the raid conducted in September 2015 by German prosecutors of the Munich law offices of outside counsel for Volkswagen. This was in connection with a criminal investigation of emissions fraud by its subsidiary, Audi. The raid was authorized by court order but lacked sufficient safeguards to recognize and preserve privilege, and post-raid efforts to protect the privilege were largely unsuccessful. In July 2018, Germany's high court rejected a challenge to the raid brought by Volkswagen and the law firm. The court held that the raid did not impermissibly permit the review of privileged documents because, under German law, the seized communications were not privileged—the law firm was engaged only by the parent organization, not the subsidiary that was the target of the Munich prosecutors. Further, the Munich offices of the law firm were found to have no constitutional right to bring a challenge because the firm was headquartered in the U.S. The court stated that a contrary ruling invited important evidence being "purposefully stored with lawyers or only selectively published."[37]

Comment 3(d). *Organizational planning issues.* This principle implies corresponding best practices for organizations that have information seized in dawn raids. Relevant issues for the private parties to address include:

- *The location of data can be determinative (including to what extent it is accessible across borders).* Local law of privilege, including whether corporate group members are protected under representation, varies tremendously and may provide traps for organizations that are not mindful of what has been seized. Organizations in their dawn raid planning should identify where sensitive documents are held and from where they are accessible, as well as what remedial measures may mitigate risks. (See Principle 7.)

(requiring courts to "scrutinize carefully the particularity and breadth of the warrant authorizing the search, the nature and scope of the search, and any resulting seizure"; finding warrants overbroad because they permitted seizure "without regard to whether the materials had any connection to particular alleged crimes or to [subject matter] in general").

[37] *See* Tom Fox, *Raid on Jones Day German office clouds FCPA investigations,* FCPA BLOG (Mar. 17, 2017), https://www.fcpablog.com/blog/2017/3/17/tom-fox-raid-on-jones-day-german-office-clouds-fcpa-investig.html, citing https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2018/bvg18-057.html (in German); Ana Reyes and Matthew Heins, *Jones Day Case Highlights Questions Of Atty Privilege Abroad,* LAW360 (July 27, 2018), https://www.law360.com/articles/1067688/jones-day-case-highlights-questions-of-atty-privilege-abroad. Other courts, albeit a minority, have expressed suspicion of dawn raids executed on attorney offices or law firms, because of the risk of violating attorney-client privilege and attorney work-product protections. *See* Cohen v. United States, No. 1:18-mj-03161, 2018 WL 1772209 (S.D.N.Y April 13, 2018), ECF No. 30 (April 27, 2018) (barring government team from accessing materials seized in search warrant executed at offices of attorney Michael Cohen and appointing a special master to review seized materials for relevance and privilege, including an opportunity for defense counsel to challenge the special master's determinations, prior to production of materials to government prosecutors); *see also In re* Search Warrant Dated June 13, 2019, 942 F.3d 159 (4th Cir. 2019) (in granting preliminary injunction against government, halting review of records seized in search warrant of a law firm, court observes: "Federal agents and prosecutors rummaging through law firm materials that are protected by attorney-client privilege and the work-product doctrine is at odds with the appearance of justice."). *Cf.* Harbor Healthcare Systems, L.P. v. United States, 5 F.4th 593 (5th Cir. 2021) (per curiam) (criticizing prosecutors' refusal to destroy or return to the organization's privileged information obtained in raid of corporate offices, in case later use desired). *But see In re* Sealed Search Warrant, 11 F.4th 1235 (11th Cir. 2021) (per curiam) (broadly rejecting contention that use of governmental "taint teams" to self-screen for privileged material seized from targets of criminal investigations is inappropriate; citing cases).

- *The extent to which privileged communications can be protected in law offices headquartered outside of the location of the raid.* Dawn raid planning should include an assessment of attorney-created documentation and attorney-client communications—what is privileged, and who is a client, under local law and regional law (which may be superseding). Documents prepared by in-house lawyers, for example, are likely not privileged in a European Commission ("EC") investigation even if they are considered privileged under the member-state laws of many EU countries. In addition, the EC may determine that EU law applies when it seeks documents created under privilege in the U.S. and shared with non-U.S. entities, squarely setting up a conflict with U.S. privilege law. To illustrate the point, in the Volkswagen investigation, the attorney engagement letters did not support the assertion of privilege under local law, which had a far-reaching impact on the organization's ability to protect that sensitive information from disclosure.

- *The extent that exposure of privileged documents in one jurisdiction controls the privilege status of the documents in another jurisdiction.* Following the Volkswagen raid discussed above, plaintiffs in a German civil action filed a petition in U.S. courts under 28 U.S.C. § 1782 (which permits discovery in aid of foreign proceedings) to obtain the internal investigation documents held by the law firm. The court applied U.S. law to hold that an attorney-client relationship broadly existed between the law firm and Volkswagen, protecting those documents from use in the civil action.[38] However, other courts have found that documents were discoverable in a U.S. court proceeding when the documents would have been privileged under U.S. law but were not considered privileged under foreign law.[39]

***Principle 4*. Dawn raids should be conducted with due respect for the data privacy, protection, and localization laws of sovereigns whose citizens and residents are affected by the raids, as well as the rights and interests of persons who are subject to such laws.**

Comment 4(a). *Dawn raids may lead to cross-border conflicts of law.* Authorities in dawn raids commonly seize electronically stored information ("ESI") from the raided premises.[40] Moreover, authorities increasingly reach for ESI that is accessible from the premises but located remotely, including ESI that

---

[38] *In re* financialright GmbH, No. 17-mc-105, 2017 WL 2879696 (S.D.N.Y. June 22, 2017), citing *In re* Parmalat Securities Litigation, No. 04-MD-1653, 2006 WL 3592936, at *5-6 (S.D.N.Y. Dec. 1, 2006).

[39] Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479, 492–93, 495–96 (S.D.N.Y. 2013). *See also* United States v. Getto, 729 F.3d 221, 227–28 (2d Cir. 2013) (MLATs permit U.S. authorities to obtain and rely upon data seized by foreign authorities even where the same such seizure would have been unconstitutional if conducted in the U.S.).

[40] *E.g.,* Section 27(5)(b) of the UK Competition Act 1998 (authorizing Competition & Markets Authority officers to require any relevant ESI that is accessible from the searched premises to be produced for seizure, preserved, and to prevent interference with such steps).

is in the cloud or held by employees working remotely.[41] Potential conflicts with foreign data privacy and protection laws and export restrictions arise where such ESI is drawn from outside of the country. This sort of compelled cross-border transfer raises concerns of the foreign sovereign and those whose data are subject to its laws and potentially requires the organization to violate such foreign laws in enabling the transfer instruction. Yet refusing to enable the transfer places the organization at risk of being labeled obstructive, with accompanying penalties, negative inferences, and other consequences. (See Principle 6.)[42] Authorities should recognize those concerns and, when enforcement priorities allow, consider adopting policies and practices to minimize these types of conflict.

Comment 4(a)(i). *"E-Raids."* Reflecting the way that organizations conduct and document their business, the great bulk of evidence sought and acquired in dawn raids is in digital form. Such data is often stored on cloud-based systems that may be accessed remotely. Investigators conducting an "E-raid" may in place of, or in conjunction with, the raid of the physical premises, schedule a video conference and extract passwords and access to organization and employee systems and devices. The investigator may then review and/or remotely copy data (often with organization representatives permitted to monitor the process). Such attendees, systems, and devices may be in locations outside of the jurisdiction of the investigating agency.

E-raids may also reach outside of the office. There is a long-term trend toward remote work, at home or other locations outside of the organization office (including in different jurisdictions). Employees are doing business and otherwise creating records of interest with their personal devices and providers (including messaging apps like WeChat or WhatsApp, and cloud-based third party services and repositories like Google Drive and Box). Agencies have responded by requiring employees to come into the office and bring their devices for inspection and by going to employees' residences to

---

[41] The EC has long asserted the right to access all information that is accessible to the inspected entity. *See* Directive (EU) 2019/1 of the European Parliament and of the Council of 11 December 2018 to empower the competition authorities of the Member States to be more effective enforces and to ensure the proper functioning of the internal market, Art. 6 (EC inspectors have the right to access all information accessible to the inspected entity, making no exception for location), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001. The validity and contours of this "access principle" have not been squarely tested in a court of law. *See* Organisation for Economic Co-operation and Development (OECD), Directorate for Financial and Enterprise Affairs Competition Committee, Investigative powers in practice – Unannounced Inspections in the Digital Age and Due Process in relation to Evidence Gathering, at 2, https://one.oecd.org/document/DAF/COMP/GF/WD(2018)25/en/pdf. The EC's approach is not the only one, however. Other agencies adopt a "Location approach," where they look purely at where the digital information is stored as described in the authorizing order; to look beyond that location, the agency must obtain another order. See ICN ANTI-CARTEL ENFORCEMENT MANUAL, *supra* note 27, Chapter on Digital Evidence Gathering § 8.4 (noting that where new sources of data outside of the jurisdiction are identified, steps may be taken to immediately arrange for preservation of such data including through the 24/7 Network, pending legal process).

[42] The Sedona Conference's *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders*, 21 SEDONA CONF. J. 393 (2020), provides an excellent discussion of conflicts-of-law risks and factors involved in cross-border data transfers.

collect data. Home raids with collections of data from personal devices and nonorganization repositories raise significant privacy concerns.[43]

Yet further challenges can occur when the organization does not participate in the raid at all. Some have expressed concern about cybersecurity and national intelligence laws providing authorities extrajurisdictional access to data hosted by service providers without cooperation of the host country, much less the owners of the information.[44] Agencies use strategies (what the FBI calls "Network Investigative Techniques" or "NIT") to surreptitiously gain remote access to, and seize, electronic information. These seizures reportedly have taken place across international borders.[45] Moreover, under the "access principle,"[46] the boundaries of an electronic seizure need not necessarily be articulated in a legal order authorizing the search; the investigator may simply follow access points to their conclusion. Subjects of such investigations would be unable to influence the course of the raid by scrutinizing the authorizing instruments, raising objections in real time (or, in some cases, at all), or to advocate for special procedures to identify and secure privileged, sensitive, and protected information. Subjects who do not learn of the raids until after the seizure is complete (if at all) may further struggle to understand even what was taken, hampering their ability to investigate the circumstances, take remedial action, or to mount a defense.[47]

These concerns also exist in the case of "remote warrants," which enable investigators in the U.S. to search media located outside of their jurisdiction. In 2016, the U.S. adopted changes to the Federal Rules of Criminal Procedure ("FRCrP") that loosened restrictions for government agents executing a remote search warrant."[48] These changes authorize the government to search computers located

---

[43] For this reason, home raids in the EU typically require a judicial warrant from a national court, although the line between work and home is becoming blurred. *See supra* n.21. Companies should prepare their employees for the possibility of such actions. In October 2021, the UK Financial Conduct Authority (FCA) issued guidance on the implications of remote work, noting: "It's important that firms are prepared and take responsibility to ensure employees understand that the FCA has powers to visit any location where work is performed, business is carried out and employees are based (including residential addresses) for any regulatory purposes. This includes supervisory and enforcement visits." *Remote or hybrid working: FCA expectations for firms*, FCA (last updated Feb. 13, 2023), https://www.fca.org.uk/firms/remote-hybrid-working-expectations.

[44] European Commission, Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data (Feb. 29, 2020), at 9, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[45] Jeff Welty; *Search Warrants Authorizing Law Enforcement Computer Hacking and Malware*, NORTH CAROLINA CRIMINAL LAW (Jul. 23, 2018), https://nccriminallaw.sog.unc.edu/search-warrants-authorizing-law-enforcement-computer-hacking-and-malware/.

[46] *See supra* n.41.

[47] Agencies including the U.S. Department of Justice ("DOJ") may seek "warrants that excuse agents from having to notify at the time of the search the person whose premises are searched." U.S. DEPT. OF JUSTICE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, at 83, *available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

[48] FED. R. CRIM. P. 41(b)(2)-(5).

outside the jurisdiction of the magistrate judge issuing the warrant. These searches—like the NIT searches described above—were developed to deal with increasingly sophisticated cybercriminals who deploy obfuscation technology to evade law enforcement. Prior to the changes, the government could only issue search warrants outside of their districts in limited circumstances, such as when a tracking device was installed within the district and moved outside of the district, or in cases of terrorism investigations.[49] The 2016 changes to FRCrP Rule 41, however, allow the government to remotely access a suspect's computer when the suspect has obscured the location by using anonymizing technology such as a proxy server or a Virtual Private Network.[50] The amended Rule 41 therefore allows the government to execute a search warrant that requires accessing a computer network outside the district where the warrant was issued.

While many of the early and more aggressive applications of these remote search warrants stemmed from investigations involving child pornography, the statute does not so limit their use. For organizations that do business around the world, this tactic increases the chances that an organization network or device could be swept up in an investigation where the organization or an employee is merely tangentially related. Organizations should consider such risks in determining what content is permitted to pass through their servers.[51]

Comment 4(b). *Intergovernmental comity considerations.* Consistent with comity principles, authorities conducting dawn raids generally should not unilaterally access data located in a foreign jurisdiction. Instead, the investigating authority should gain the permission or enlist the assistance of the resident foreign authority through an agreed upon procedure, a bilateral/multilateral agreement, or other intergovernmental cooperation mechanism.[52] The foreign authority may then evaluate the request and

---

[49] *Id.,* advisory committee's note to 2016 amendment.

[50] *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches,* U.S. DEPT. OF JUSTICE (June 20, 2016), https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[51] By contrast, self-executing warrants enable law enforcement to send a warrant to an organization instructing it to conduct a search. *See, e.g.,* United States v. Bach, 310 F.3d 1063, 1067 (8th Cir. 2002) (upholding use of search warrant faxed to internet communication company asking it to conduct the search for records, finding that the "Fourth Amendment does not explicitly require official presence during a warrant's execution," and that "[c]ivilian searches are sometimes more reasonable than searches by officers."), citing cases. For example, a self-executing search warrant reviewed by the authors of this article was signed by a magistrate judge and served on an organization and includes instructions as to how to execute the warrant in addition to the description of items to be "seized" by the "government," or in this case, the recipient. The recipient is "ordered to disclose the [requested] information to the government within 14 days of the issuance of this warrant." The self-executing warrant is not a dawn raid but functions more in the nature of a subpoena in its execution and so abides by judicial warrant requirements and generally provides the recipient far more opportunities to shape and respond to the government's demands than would a traditional raid.

[52] *See* Principle 1 of The Sedona Conference's *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Jan. 2017), at 9 ("in a U.S. legal proceeding, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws"), *available at* https://thesedonaconference.org/publication/International_Litigation_Principles. *Cf.* EDPS Opinion 7/2019, *supra* note 18 (noting that involvement of member state is needed to enforce data subject rights, which may differ across jurisdictions).

obtain the data in its jurisdiction in conformity with its own laws and process. That may include first screening such information for restricted information or providing the holder the opportunity to influence and challenge the seizure and process in advance of the requested acquisition and transfer, and appropriately remediating the data set before transfer.

This restraint is consistent with rules, laws, and guidelines of many authorities that require consideration of such deferential processes in acquiring data stored outside of the jurisdiction.[53] The U.S. Cloud Act, while outside of the scope of this *Commentary*, is a recent example of a statutory scheme that promotes deference to foreign jurisdictions when obtaining extraterritorial data.[54]

Comment 4(c). *Procedures to promote comity.* Authorities should put in place procedures to avoid or minimize conflicts with foreign data protection requirements for seized information. For example, U.S. courts will employ comity considerations when evaluating whether foreign data protections should be enforced as an evidentiary privilege in the U.S. Similarly, U.S. courts generally recognize the attorney-client privilege when a U.S. lawyer advises a foreign organization on U.S. law, even if that privilege would not be recognized under the foreign law.[55]

---

[53] For example, the DOJ, often with the FBI or other agencies, may work with authorities outside of the U.S. via intergovernmental MLATs and other mechanisms to conduct coordinated raids at a foreign organization location. (USJM, *supra* note 10, § 9-13.500-525). When considering issues of obtaining evidence abroad, the Justice Manual requires consideration of the appropriate method to gain that country's assistance. *See id.,* § 9-13.510, Obtaining Evidence Abroad—General Considerations ("Every nation enacts laws to protect its sovereignty and can react adversely to American law enforcement efforts to gather evidence within its borders without authorization. Such efforts can constitute a violation of that nation's sovereignty or criminal law. You should contact the Office of International Affairs, Criminal Division, as soon as you become aware that you may need evidence located in another country to determine methods for securing assistance from abroad and to select an appropriate one."). *See also* Article 22(1) of EU Competition Regulation 1/2003, *supra* note 3, Art. 22(1) (competition authority from one EU member-state may carry out an inspection on behalf and for a competition authority from another member-state).

[54] The Clarifying Lawful Overseas Use of Data Act (Cloud Act), 18 U.S.C.A. § 2523 (2018), in brief, authorizes warrants issued on certain U.S. electronic communications and cloud providers under the 1986 Stored Communications Act ("SCA") to reach communications stored outside of the U.S. Such warrants may be quashed if (a) the disclosure would cause the provider to violate foreign laws; (b) "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and" (c) "the customer . . . is not a United States person and does not reside in the United States." A court hearing a challenge to the Cloud Act warrant will perform a comity analysis and consider "the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure" and "the interests of the qualifying foreign government in preventing any prohibited disclosure." This solution—while not directly permitting challenge by the data subject—tends to mitigate providers' fears that complying with SCA warrants for extraterritorial data would require violation of foreign law. The Cloud Act also authorizes reciprocal rights to non-U.S. jurisdictions that, in entering into a bilateral agreement with the U.S., prequalify to make requests directly to U.S. service providers for SCA information maintained in the U.S., rather than proceeding via an MLAT. *See also* discussion of proposed EC E-Evidence Directive, *E-evidence – cross-border access to electronic evidence*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (last visited Dec. 13, 2024).

[55] *See* The Sedona Conference, *Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders,* 21 SEDONA CONF. J. 393 (2020); Wultz v. Bank of China Ltd., 979 F. Supp. 2d 479, 492–93, 495–96 (S.D.N.Y. 2013). *Cf.* Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. Commission of European Communities, (Joined Cases T-125/03 and T-253/03 (2007) (in-house counsel are not "independent" and so their communications are not

Comment 4(d). *Considerations when intergovernmental cooperation is lacking.* It is a reality that certain countries will not always cooperate in foreign agency investigations, frustrating the efforts of law enforcement. Some objections may be principled—a country may deny a request for assistance in obtaining data to investigate something that is not illegal in the country where the data is located (e.g., criticisms of a government are likely protected activity in the U.S., although they may be a crime in other jurisdictions). Some objections, however, may be parochial or even corrupt.

When the agency seeks to go it alone on this basis, the various interests may best be weighed through a pre-raid submission, similar to a warrant, that permits a court to apply comity principles. An authority determined to engage in "self-help," in contrast, may face a stiffer burden in a post-raid challenge to the seizure, when hindsight reigns and it may be unable to take affirmative steps to help justify its actions. The U.S. Supreme Court in *Société Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, set forth the following five factors to consider in determining whether a foreign data restriction must be complied with: (1) the importance to the litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the U.S.; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interests of the U.S., or compliance with the request would undermine the important interests of the state where the information is located.[56] Some courts have also considered the negative impact of the producing party being out of compliance with the foreign law.[57]

***Principle 5*. There should be meaningful restrictions on the immediate access by authorities to privileged and protected information during a raid, and on the review, use, disclosure, and ultimate disposition of such information.**

Comment 5(a). *Special procedures for protected information.* As is feasible, seizures should be restricted to information within the scope of the authorizing instrument, which should be narrowly tailored. (See Principle 3.) Moreover, investigators should not seize or review information where there are reasonable grounds to believe the material is unreviewable on the ground of privilege. For ESI in particular, it may be easy and tempting for authorities to scoop up information that is out of scope or

---

privileged; legal professional privilege covers internal documents drafted solely to seek advice from external lawyers). Reportedly, the legal advice of inside counsel relied upon by the EC in finding that John Deere & Co. knowingly violated EU anticompetition law had been provided by counsel to organization management in the U.S. and Germany in a memo that was seized in a dawn raid on European offices. Case L-35/38, John Deere & Co. v. N.V. Cofabel, 14 December 1984 O.J.L. 35, 2 C.M.L.R. 554. I, at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1985:035:FULL:EN:PDF at 61, discussed in *European Court of Justice Finds In-House Legal Advice Not Protected by Legal Professional Privilege,* SIMPSON THACHER (Sept. 17, 2010), https://www.stblaw.com/docs/default-source/cold-fusion-existing-content/publications/pub1061.pdf.

[56] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522, 539–40, 544 (1987) (quoting RESTATEMENT OF FOREIGN RELATIONS LAW (REVISED) (1986)).

[57] Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (citing *Aérospatiale*, 482 U.S. at 543–44. n.28).

protected, then sort and analyze later.[58] In contrast to the use of investigative tools based upon notice, raided companies are in a poor position to clarify legitimate scope, tailor the response, or identify and segregate for special treatment information that should not first be reviewed by the authority.

Authorities should develop special procedures to protect privileged or otherwise protected information in dawn raids, to isolate such information without betraying the privilege,[59] and to provide organizations the ability to assist in its identification and sequestration before exposure.[60] As discussed below, authorities have developed several different practices that may be effective in a given situation.

Comment 5(b). *The use of "taint teams" to protect privilege.* One such procedure is to sequester privileged information from the investigative team before an independent determination of privilege. This may be done by isolating the documents in a neutral manner (e.g., through technology) and

---

[58] UK ATT'Y GEN.'S OFFICE, ATT'Y GEN.'S GUIDELINES ON DISCLOSURE - FOR INVESTIGATORS, PROSECUTORS AND DEFENCE PRACTITIONERS, at 24-25 (Dec. 2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf (authorizing retention of irrelevant information "inextricably linked" to relevant information, and cautioning investigators not to be overly quick in disregarding such irrelevant information due to potential for case requirements later). Such overcollection and retention may cause considerable downstream problems in controlling information and investigation risk and may be the focus of time-consuming efforts to retrieve out-of-scope data.

[59] For example, EC officials generally are prohibited from reviewing or seizing documents that are, or are asserted to be, protected by a legal privilege. *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.5 (discussing variations of process for protecting legal professional privilege during raids); OECD, Directorate for Financial and Enterprise Affairs Competition Committee, Summary of discussion of the roundtable on the treatment of legally privileged information in competition proceedings [hereinafter OECD LPP Report] (discussing "sealed envelope procedure" where investigator may physically seize or copy documents and family members for later determination of privilege by Directorate-General for Competition's Hearing Officer, which acts as an independent arbiter regarding procedural disputes between targets/third parties and EC investigators), https://one.oecd.org/document/DAF/COMP/GF/WD(2018)25/en/pdf. *See generally* Wouter P. J. Wils, *Legal Professional Privilege in EU Antitrust Enforcement: Law, Policy & Procedure*, WORLD COMPETITION L. & ECON. REV., Vol. 42, No. 1 (March 2019), at 21–42. In addition, the DOJ has developed guidelines for obtaining, protecting, and further transferring protected information, including information subject to foreign laws, and potentially privileged information. *See* USJM, *supra* note 10, §§ 9-13.400-.512.

[60] Such guidelines of conduct are embraced by regulators as well as subjects of raids. The ICN has commented directly on such procedural transparency and inclusiveness, and the need to address confidentiality and privilege concerns arising from inspections and enforcement actions. *See* International Competition Network (ICN) Guiding Principles for Procedural Fairness in Competition Agency Enforcement ("Meaningful Engagement: Competition agencies should seek and take into account relevant information and views from parties and third parties to inform their consideration of enforcement matters. Agencies should offer meaningful communication with parties on significant factual, legal, economic, and procedural issues at key points during enforcement . . . .") ("Confidentiality Protections: Competition agency enforcement proceedings should include a process for appropriate identification and protection of confidential business information and recognition of privileged information. The decision to disclose confidential information should include consideration of the confidentiality claims, rights of defense, rights of third parties, incentives to provide information, effects on competition, and transparency to the public."), *available at* https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/09/AEWG_GuidingPrinciples_ProFairness.pdf.

then either permitting counsel for the subject to first review the seized data for privilege or routing such documents to a special review team with independence from the investigative team.

Authorities may arrange for the creation of a "taint team" composed of persons working for the investigating agency who are walled off from the investigative team, or, in circumstances where a court has been engaged, a special master or independent counsel to review the seized materials for privileged documents and communications. In theory, privileged information may thus be excluded from review by the investigators, who will not be "tainted" by the information.[61]

Variations of such procedures are common. For example, the Netherlands Authority for Consumers and Markets, upon assertion that data to be inspected contains privileged correspondence, will take a "cursory look" at the data and either set it aside or, if not convinced that it is privileged, will route the data to an uninvolved Legal Professional Privilege officer for further review.[62]

Beyond using different personnel, additional steps may be taken to protect the rights of the data owners and subjects. The review team should consist of people who are knowledgeable about the subject matters of the investigation, are well-versed in the nuances of relevant privilege laws, and are operationally independent of the investigators. Investigators should not review any materials in scope before the taint team clears them for investigative review and analysis. Authorities should consider consulting with counsel for the data owners and subjects to better identify the subject information, consistent with counsel's obligation to protect client confidentiality. Further, counsel should receive access to the seized materials as soon as practicable and be given a meaningful opportunity to object to further use by the investigators of any document that has been released to them.

The use of taint teams composed of prosecutors and other persons who may appear to lack independence from the investigative agency, as well as the "cursory look" practice, are controversial. These practices may raise the specters of conflicts, create greater incentives to construe privilege narrowly, increase the risk of leakage of privileged and irrelevant information (either to the investigating team or for unrelated matters), and have an adverse impact on principles underpinning the privilege, such as the free flow of information between attorney and client. While generally accepted, some U.S. courts have rejected the idea that review of privilege information by other prosecutors—even if procedurally walled off—is acceptable and have required the appointment of an independent reviewer in situations where privilege risks are pronounced, such as searches of law offices.[63] At least

---

[61] The U.S. Justice Manual provides for the use of a "privilege team" "to protect the attorney-client privilege and to ensure that the investigation is not compromised by exposure to privileged material." USJM, *supra* note 10, § 9-13.420(e). The DOJ considers this an internal process that creates no rights in the event the guidelines are not followed.

[62] *See* The Netherlands Authority for Consumers and Markets, 2014 ACM Procedure regarding the legal professional privilege of lawyers, *available at* https://www.acm.nl/sites/default/files/old_publication/publicaties/12771_2014-acm-procedure-regarding-the-legal-professional-privilege-of-lawyers-2014-02-06.pdf.

[63] *See, e.g.,* United States v. Gallego, No. 4:18-cr-01537-001-TUC-RM (BPV), 2018 WL 4257967, at *3 (D. Ariz. Sept. 6, 2018) (ordering special master be appointed instead of DOJ taint team), quoting United States v. SDI Future Health, Inc., 464 F. Supp. 2d, 1027, 1037 (D. Nev. 2006) ("federal courts have generally 'taken a skeptical view of the

one appellate court has found such practices to violate fundamental U.S. principles of separation of powers due to judicial functions being arrogated by the executive.[64] In other instances, courts have held that judicial approval of an intra-agency taint team should not be granted in ex parte proceedings, given the risks of irreparable harm to privilege and the adversary system implicated by law office searches.[65]

Comment 5(c). *Additional Screening Procedures and Artificial Intelligence (AI).* Additional measures may be needed to appropriately address owner and subject data property and privacy rights. Design of these measures should take into account the nature of the data and the means to isolate the sensitive information and may require a team knowledgeable about the technical solutions available to facilitate such a process.

Even where a taint team is used, authorities should consider screening mechanisms to identify potentially privileged information in a seized dataset that minimize risk to privilege. Investigators may bring in counsel for data owners and subjects to identify privileged information. Where there is disagreement as to an objection to disclosure, interested parties may be given an opportunity to have their objections considered by an impartial neutral party.[66]

Government's use of 'taint teams' as an appropriate method for determining whether seized or subpoenaed records are protected by the attorney-client privilege.'").

[64] This was the conclusion of the Fourth Circuit Court of Appeals in *In re* Search Warrant Issued June 13, 2019, 942 F.3d 159 (4th Cir. 2019). The Court found that the ex parte order of the special master authorizing the use of a "filter team" of federal agents, prosecutors, and forensic examiners to review a criminal defense law firm's records seized under warrant violates separation of powers and fails to effectively protect privilege. *Id.* at 182–83 ("It would be difficult for reasonable members of the public to believe that Filter Team AUSAs would disregard information in Lawyer A's emails that might be relevant to other criminal inquiries in Maryland."). The Court enjoined the taint team review and ordered the records to be provided to a special master to perform that function. *See id.* at 178 ("In sum, the Filter Protocol improperly delegated judicial functions to the Filter Team . . . which left the government's fox in charge of guarding the Law Firm's henhouse."). *See supra* n.63 (discussing case law). The Court of First Instance of the EU similarly disapproved of the EC's "cursory look" practice where there is any doubt or dispute about whether a document is protected by the legal professional privilege. *Akzo Nobel Chemicals Ltd. and Akcros Chemicals Ltd. v. Commission of European Communities,* (Joined Cases T-125/03 and T-253/03 (2007).

[65] *In re Search Warrant Issued June 13, 2019,* 942 F.3d at 179 (citing adversarial hearings conducted concerning the DOJ's proposed use of filter team in the Michael Cohen matter, referenced *infra* Cmt. 8(c).

[66] The UK Serious Fraud Office ("SFO") takes this approach, involving cooperation with organization counsel and review of search term responsive documents by independent counsel. R. (on the application of McKenzie) v. Director of the Serious Fraud Office, 2106 EWHC 102, 2016 WL 312261 (Admin) (Divisional Court, Jan. 27, 2016) (discussing procedures). Courts have criticized broad collections of privilege-rich ESI as is likely in a search of attorney files for their potential to irreparably damage the data rights of clients and of attorneys, as well as stressing the boundaries of probable cause needed in U.S. systems to support a judicial search warrant. In *In re Search Warrant Issued June 13, 2019*, the Fourth Circuit called out the government for the overbreadth of seizing entire mailboxes of attorneys without effort to restrict the seizure just to the client at issue; ultimately, 99.8 percent of the 52,000 seized emails did not make any reference to the single client under scrutiny. 942 F.3d at 178. The Court rejected the assertion that review of such irrelevant material is required for "context" in making privilege determinations, as no probable cause exists to seize such documents. *Id.* (citing United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1172 (9th Cir. 2010) (en banc) (criticizing

Screening of ESI may be conducted using computerized (often domain, name, or keyword) searches on-site in the collection process, or if the data is seized more broadly and is taken from the premises, screening may be performed by a third-party vendor or by agency staff with appropriate safeguards. The efficacy of these searches may be aided by input from the owner of the claimed privilege.[67]

Artificial-intelligence-driven technology may also aid in identifying and mitigating the risk of exposure of privileged information seized in a raid. Prosecutors who executed the search warrant of U.S. President Donald Trump's then-personal attorney, Michael Cohen, proposed that the ESI seized be assessed using Technology-Assisted Review software to identify potentially privileged documents, which would then be removed from the mass of data seized and separately reviewed by a special master. In this way, the burden on the review team and the risk of exposure to the prosecutors would be reduced. While the court hearing challenges to the seizure elected to proceed with a more traditional special-master procedure, it is foreseeable that the privilege screening process may be automated to a great extent as technology improves and stakeholders become more comfortable with the process.[68]

Comment 5(d). *Privilege holders should take diligent steps to protect privilege across borders.* This principle also recommends vigilance on the part of those who have privilege claims to assert. While many jurisdictions (including the EU) will not impute a waiver to privileged advice seized during an inspection,[69]

---

government "overreach" in seizure of electronic data unsupported by probable cause), abrogated on other grounds by Hamer v. Neighborhood Hous. Servs. of Chi., 138 S. Ct. 13, 16-17 (2017).

[67] *McKenzie, supra* note 66 (in upholding SFO process of in-house technical staff isolating protected material, noting the "vast difference between the task of identifying a document as potentially attracting privilege and determining whether it was protected, a process which involved close consideration of the content and context.").

[68] Letter of Department of Justice to Hon. Kimba M. Wood (Apr. 26, 2018) (Case l:18-mj-03161-KMW) (S.D.N.Y.), *available at* https://archive.org/stream/Michael-Cohen-Court-Documents/2018-04-26-Cohen-28_djvu.txt. *See* FED. R. EVID. 502 explanatory note ("Depending on the circumstances, a party that uses advanced analytical software and linguistic tools in screening for privilege and work product may be found to have taken 'reasonable steps' to prevent inadvertent disclosure."). *But see* EDRM/DUKE LAW, TECHNOLOGY ASSISTED REVIEW (TAR) GUIDELINES (Jan. 2019) at 32 ("Privilege review is one area where existing permutations of TAR face significant challenges that may make them less valuable to clients and counsel.").

[69] In general, the concept of waiver properly should not include involuntary or forced disclosures. *See* Facebook Interim Order, recital 103: "It should be noted in that regard that the applicant itself indicates, referring to the case-law of the United States courts (United States v. American Tel. and Tel. Co., 642 F.2d 1285, 1299 (D. C. Cir. 1980)), that such disclosure could only be characterized as a waiver in the case of a 'voluntary disclosure' of the documents at issue." Order of the President of the General Court in Case T-451/20 R, Facebook Ireland v Commission, EU:T:2020:515, at para. 62, *available at* https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=D128683786B502FF27F2D433DF9CA36A?docid=233082&text=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=4350801. Defining what is "voluntary", however, may sometimes lead to debate, including whether reasonable steps were taken to protect such information from a raid. This lack of certainty is exacerbated in cross-border situations. Certain jurisdictions provide statutory and case-law protections. For example, Federal Rule of Evidence 502 limits the scope and effect of waivers associated with unintentional (involuntary) disclosures in certain U.S. proceedings, and even provides protections as to *intentional* disclosures in some circumstances. *See* FED. R. EVID. 502(d) (authorizing federal court to "order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court . . . [or] any other federal or state proceeding."); *id.* FED. R. EVID 502 explanatory note (protections available for "quick peek"

this is not universal. Accordingly, privilege holders should aggressively seek to protect privileged information, even where such privilege is not always respected or clear.[70] As noted, documents seized in a raid and found not privileged in the home jurisdiction often make their way to jurisdictions like the U.S. with broader conceptions of privilege. (See Comment 6(d).) Among the factors a U.S. court will consider in evaluating whether such documents retain their privileged status in the U.S. are the efforts made by the organization to preserve the privilege, to object to each disclosure, and to retrieve the documents.[71]

Comment 5(e). *Protecting Privacy.* Digital assets and communication systems continue to proliferate, increasing the likelihood that personal data will be stored on an organization's systems, employee computers, and mobile devices seized by the authorities.

Authorities should therefore consider means to exclude irrelevant data identified as personal, particularly where employees designate data as such or make a request. The authorities may weigh several factors to help determine which safeguards for personal data are appropriate under the circumstances, including the investigative need, comity, and the privacy interests of implicated jurisdictions, subjects, and third parties. For example, if data has been seized from an organization in France, French employees' concerns might be given decisive weight if they have had no, or only peripheral, involvement in the subject matter of the inquiry. Conversely, if the investigation focuses on an individual's personal actions, the interests of conducting a thorough investigation might weigh in favor of including such content.

In many situations, the search can take a different approach when confronted with a directory that an employee has designated as containing personal content, or messages with indicative terms such as "PERSONAL" or "PRIVATE" in the header. Rather than blindly trusting such self-designations, authorities could search for agreed-to terms provided by the employee that can identify the specific content that should be excluded from the investigation; conversely, authorities could search a folder designated as "PERSONAL" for terms that would indicate only relevant (and nonpersonal) data. As

---

situations where privileged information is provided to adversary, subject to retrieval). Parties subject to a dawn raid or collateral compelled disclosures may also consider requesting that the overseeing authority issue an order with findings of fact that the disclosure is not voluntary and does not waive any privilege or protection in any proceeding—although such order and findings would have uncertain impact outside of the authority's jurisdiction. A full discussion of the many ways that privilege information may be waived in interactions with authorities, and strategies to manage such risk, is beyond the scope of this *Commentary*.

[70] The need for good-faith vigilance is heightened by the potential for prospective expansion or clarification of the scope of the attorney-client or legal-professional privilege by the courts. This was seen recently in the European Union Court of Justice's decision in Judgment of December 8, 2022, Orde van Vlaamse Balies, IG, Belgian Association of Tax Lawyers, CD, JU v. Vlaamse Regering, C-694/20, EU:C:2022:963, which clarified that the Legal Professional Privilege falls under the right to the protection of private communications, and so extends to attorney-client communications regarding legal advice beyond just those related to "rights of defense" in litigation.

[71] *See In re* Parmalat Sec. Litig., No. 04-MD-1653, 2006 WL 3592936 at *5–6 (S.D.N.Y. Dec. 1, 2006) (denying plaintiffs' effort to use organization documents seized by Italian authorities from the organization's offices in Italy, even though the authorities broadly disclosed the documents, where the organization zealously and consistently asserted the privilege, judicially preserved its claims, and objected to disclosure).

stated previously, input from technical experts should be considered, and advances in technology hold promise for further automating this process.

Subjects of raids may advance this process considerably by taking appropriate steps to minimize their holdings of personal information.[72] This is becoming increasingly difficult given the central role that electronic communication tools play in many employees' work life. Organizations may also wish to review their use policies—consistent with applicable law—to ensure they are clear as to how employees may use organization equipment/systems for nonbusiness purposes, and to note that companies may be required to disclose personal information to agencies without notice or direct remedial action.

Comment 5(f). *Protecting Sensitive Commercial Information and Trade Secrets.* Seized information transferred across borders and between agencies may include highly sensitive commercial information and trade secrets. The disclosure of such information may result in competitive harm or other harm to the subject in a manner that is not directly tied to the purpose of the investigation. Indeed, the investigation may have been precipitated by a competitor's complaint. In order not to inflict, even inadvertently, such collateral competitive harm or other harm on the subject of the investigation, transferring authorities should take reasonable steps to troubleshoot and protect the confidentiality and integrity of trade secrets against disclosures that may cause unfair competitive damage.

Similarly, even within the confines of a single jurisdiction, law enforcement agencies may have overlapping authority, and there may be requests, or even requirements, to share information gathered in a law enforcement investigation. In some circumstances, such recipient cooperating agencies may themselves be subject to requests to share information with their foreign counterparts. All such agencies in the originating country should take reasonable precautions within the scope of their authorities to ensure that any recipient of transferred information will protect sensitive commercial information and trade secrets from inappropriate disclosure.

Such restrictions in interagency transfers may include restrictive covenants appropriate for the nature of the transfer. Additional reasonable safeguards should be considered where such covenants are expected to be less reliable, for example, where political considerations are a factor or when transferring information to a foreign agency. In these situations, technical measures can be implemented to further protect the information. For example, the receiving agency can be invited to access the information through a secure online portal that provides the ability to access, search, and read documents, but restricts other functions such as printing or copying the information. Alternatively, the information can be protected with digital rights management tools, whereby documents are delivered but made accessible in a framework that blocks usage or transfer of the information and blocks access after an agreed period of time.

---

[72] *See generally* The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95, 107, 129 (2019).

Finally, law enforcement agencies may themselves be subject to oversight, audits, and reviews by other authorities within their own nation. For example, within the U.S., the conduct of federal agencies, including (or especially) law enforcement agencies, are commonly subject to inquiries by various Congressional committees, the Government Accountability Office, the Office of Management and Budget, and Inspectors General, among others. Where those oversight bodies assert an absolute right to have access to all information in an agency's possession, those oversight authorities should use extreme diligence before disclosing their collected information, whether directly or in their "Final Reports," that may inflict collateral damage on private parties or investigative targets, domestically or internationally.

Comment 5(g). *Out-of-Scope Uses of Protected Information*. Where information subject to foreign data protection laws has been obtained in a raid through agreement or cooperation of the locality, the information should be used only for permitted purposes, as discussed under Principle 6. While agreement on this issue should be established between the governments in advance of the transfer, to the extent it is unaddressed, the authority in possession should seek additional agreement of the foreign sovereign before transferring the information onward or using the information for uses other than its authorized purpose.[73]

Comment 5(h). *Handling of Documents at the Close of an Investigation.* Like every other organization, law enforcement agencies need to record their actions and maintain records of their decision-making. Such requirements, even when they are not imposed by laws such as the Federal Records Act in the U.S., are well-grounded in practical necessity. Law enforcement agencies need to have an "institutional memory" of their actions; they need to be able to identify and learn from their past experiences; and they need to be able to account for their actions with their own supervisory authorities.

When investigations end, law enforcement agencies are not always able to return or destroy all the information they have collected. It may also be assumed that information that is not needed for any purpose other than record keeping may be subject to loss, theft, misuse, inadvertent disclosure, and other mishaps. Each of those outcomes can cause direct and immediate harm to the subject of the investigation and to disinterested third parties that may have been brought into the investigation for one purpose or another.

To mitigate these risks, authorities therefore should take reasonable steps to return or destroy all collected information and related materials that reflect the contents of such documents, except to the extent they are required to keep them for mandatory record keeping purposes and for the on-going operations of the authority. To the extent any such remaining records are not subject to mandatory

---

[73] *See* USJM, *supra* note 10, § 9-13.512 (Intended Use of the Evidence) ("When a country provides evidence pursuant to a request for legal assistance, such as an MLAT, letter rogatory, or letter of request, contact OIA [Office of International Affairs] before using or disclosing it for a purpose other than that specified in the legal assistance request. (Examples of such use or disclosure include Freedom of Information Act requests, or requests to use the evidence in a parallel civil or administrative proceeding.) OIA will work with the USAO [U.S. Attorney's Office] to determine whether the evidence can be used for a different purpose without the express permission of the country that provided it and, if not, for guidance in securing such permission.").

disposition schedules, they should be reviewed at periodic intervals with the goal of disposing of all materials that the agency no longer needs. The agency should not wait until the end of the case to return seized materials deemed unreviewable on the ground of privilege; such data should be returned at the first opportunity after such determination (as well as kept in a secure environment in the meantime). An agency should also be receptive to requests of the former holders/owners of the data for an updated inventory or accounting of what data is being retained, and the basis for continued retention.

Many agencies now keep their records in the cloud, which in theory makes disposal easier. However, special note should be made of backup systems and other redundant copies of documents and related information, such as office or personal "convenience" copies that investigators may have kept. Although it may be impractical to suggest that backup tapes should be systematically opened and reviewed at the end of each investigation, this *Commentary* suggests that they be kept on a strict disposition schedule that allows for their destruction at a time when "more recent" backups would be sufficient to reconstruct agency activities in the event of any disastrous loss or other operational need. Similarly, individual investigators should be encouraged, or required, to periodically (at least annually) review their files and dispose of all unneeded materials.

B. Principles and Best Practices for those Subject to Dawn Raids

***Principle 6*. Organizations and third parties subject to a dawn raid should cooperate in the raid and should not obstruct or otherwise impede its conduct. On the other hand, the mere assertion of rights and attempt to exercise those rights should not be considered lack of cooperation or obstruction.**

Comment 6(a). *Cooperation with authorities and lawful instructions.* Organizations and individuals involved in raids should—and generally are obligated to do so by law[74]—cooperate, avoid obstructing, and comply with authorized and reasonable requirements of inspectors conducting the raid. Cooperation, moreover, can be effective strategy in minimizing damage and mitigating risk of such raids.

Comment 6(b). *Consequences for lack of cooperation.* The potential consequences of the failure to cooperate are severe. First, the authority may levy significant fines or bring or make a referral for criminal charges against the organization/actors for obstruction of the investigation. For example, the EC is empowered to issue a fine of up to 1 percent of the total turnover in the preceding business year for noncooperation and incomplete cooperation, and up to 5 percent of the average daily turnover in the preceding business year for each day that an organization does not permit inspection.[75] Obstruction may also be considered an aggravating circumstance in issuing sanctions for violating EU rules of competition[76] and separately may be considered a criminal act.

Comment 6(c). *Conduct constituting obstruction.* Determining what conduct crosses the line for failure to submit to inspection is highly fact-specific, but certain actions will create risk. One of the first things that inspectors look for is the deletion or failure to take appropriate steps to preserve data during the pendency of the investigation. Cooperation should always include preserving information

---

[74] For example, the UK Competition Act 1998 Sec. 70 makes it an offence to hinder, oppose, obstruct, or unduly influence any person exercising a power or carrying out a duty in terms of the UK Competition Act, https://www.legislation.gov.uk/ukpga/1998/41/contents.

[75] The UK Competition Act, *id.*, Sec. 28; EU Competition Regulation 1/2003, *supra* note 3, Arts. 23 and 24. *See also* Directive (EU) 2019/1 of The European Parliament and of the Council of December 11, 2018 to empower the competition authorities of the Member States to be more effective enforcers and to ensure the proper functioning of the internal market, Art. 16 (The ECN Plus Directive requires the imposition of "effective, proportionate and dissuasive fines" for hindering a raid), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0001.

[76] *E.g., Dawn Raid Derailment—A Cautionary Tale,* JONES DAY (Oct. 16, 2018), https://www.jonesday.com/en/insights/2018/10/dawn-raid-derailmenta-cautionary-tale (cataloging fines: in 2018, EC administrative finding of obstruction against Slovakia's state-owned railway ZSSK for hiding, and then overwriting, data on a laptop requested by officials during inspection; in 2015, the General Court of the European Union ("GCEU") upheld an EC fine of 2.5M euros against Energeticky and its subsidiary for circumventing inspector-required IT lockouts of employees to email accounts and diverting additional email from inspectors' attention; in 2012, a GCEU ruling affirmed a 10 percent increase in fine on Koninklijke Wegenbouw Stevin ("KWS"), which refused access to Commission officials until KWS's attorneys arrived almost an hour later and refused temporarily to provide access to a director's office based on the assertion it contained no relevant information).

within the scope of the authorizing instrument. Critical first steps include suspending any auto-delete programs and notifying personnel of the need to preserve relevant documents and data. The organization should also consult with legal counsel as to the extent of its additional preservation obligations relevant to the investigation and update the scope of preservation based on subsequent developments, including the results of further interactions with the authorities and the organization's own investigation.

Once premises are sealed by inspectors, breaking the seal is subject to criminal penalties, including incarceration and significant monetary fines.[77] The failure to comply with inspector instructions regarding access to information may also be viewed as lack of cooperation. Examples include: the failure to provide passwords (including failing to cooperate in providing biometric identifiers) and to decrypt data; taking steps to divert relevant incoming information; and failing to provide remote (including cloud) access. One live issue is whether and under what circumstances inspectors may demand access to information maintained in a foreign jurisdiction. (See Comments 7(a)-(b).) For example, in 2019, the Turkish Competition Authority issued obstruction fines to Unilever and Siemens purely for not giving access to cloud storage. No data was lost, and granting access would likely have violated the European Union's General Data Protection Regulation (GDPR), suggesting that organizations may want to consider whether their systems should be designed to provide only limited access in order to shield data residing in other jurisdictions.

Comment 6(d). *Additional factors in cooperation.* The manner in which an organization responds to a dawn raid may also have an impact on the authority's perception of the subject. The U.S. Department of Justice, for example, may consider conduct deemed uncooperative as evidence for separate charges of obstruction as well as a factor in determining cooperation credit in sentencing.[78] Certainly, prosecutors have a way of making life harder for organizations perceived to be hindering an investigation.

Comment 6(e). *Cooperation obligations of third parties.* A third party on site in a dawn raid shares obligations of the subject to cooperate and not impede the execution of the raid. To the extent that the third party is under the control of the subject, moreover, any obstruction or failure to cooperate may be attributed to the subject. The subject organization should make sure to educate such third parties under its control about raids and their rights and obligations. For example, a third party may have

---

[77] Under EU rules, the EC may "seal any business premises and books or records for the period and to the extent necessary for the inspection," EU Competition Regulation 1/2003, *supra* note 3, Art. 20(2)(d). "The Commission may by decision impose on undertakings . . . fines not exceeding 1% of the total turnover in the preceding business year where, intentionally or negligently . . ., seals affixed . . . by officials or other accompanying persons authorized by the Commission have been broken." *Id.,* Art. 23(1)(e). In 2010, the GCEU affirmed the EC's decision to impose a €38 million fine on the German energy provider, E.ON, for breaching an area sealed during a dawn raid. *Antitrust: Commission welcomes General Court ruling on E.ON breach of seals case* (Dec. 15, 2010) https://ec.europa.eu/commission/presscorner/detail/de/memo_10_686.

[78] John Davis and Tom Hanusik, *New DOJ Policies Relieve "Catch-22" Pressure on Companies Conducting Cross-Border Investigations*, CROWELL & MORING (Dec. 14, 2018), https://www.crowell.com/en/insights/client-alerts/new-doj-policies-relieve-catch-22-pressure-on-companies-conducting-cross-border-investigations.

been engaged by the organization to manage its IT resources and may be asked to provide access to systems or even sit for interview. Another scenario may involve an independent third party (such as a customer) who is onsite during the raid, or whose information or property is caught up in the raid. Such independent third parties would be well counseled to not impede the execution of the raid, although their affirmative obligations are unclear.

Comment 6(f). *Legitimate assertions of rights should not be the basis for a finding of non-cooperation.* For example, there should be a process where the target of a raid may in good faith challenge the request of an EC investigator to take a "cursory look" at files to which a privilege claim is asserted. This process would allow for verification of the basis of the privilege assertion by an objective reviewer before the harm of even "cursory" disclosure occurs. Under this process, the agency should not rely upon such assertion of rights as a basis to fine or otherwise penalize the target, even where such objection is subsequently determined to lack merit. Moreover, consistent with Principle 1, any such determination should be made by an independent authority, and not the authority that is seeking the disclosure. Note, however, that some authorities may view perceived abuse of such challenges as obstructive behavior.

***Principle 7*. Organizations should assess the risk of dawn raid occurrence, including to the business, contracts, and protected information, and take reasonable steps to prepare for and mitigate such risks.**

Comment 7(a). *Organizational steps to assess and mitigate data risk.* To properly manage a dawn raid, organizations should take appropriate steps to assess their risk and impact, understand the organization's rights and obligations, and use that information to prepare for their occurrence and mitigate their effects. First steps include:

- developing and implementing written dawn raid procedures with clear allocation of responsibilities;
- practicing responding to raids to minimize impact on the organization and impacted information; and
- taking steps to safeguard information at risk of unauthorized access and disclosure (e.g., storing privileged information in clearly labeled, secure areas).

Annexed hereto is a checklist of best practices that may be used by organizations in preparing for and responding to data privacy and cross-border issues in dawn raids. The following discussion of issues provides a framework for considering and implementing the checklist of best practices:

Comment 7(b). *Data protection.* Information at risk of a raid may be subject to a variety of protections based on access, location, content, or usage. It is therefore necessary to evaluate the nature of

the data that may be seized and the protections that could apply. This can be assessed by answering the following questions:

- What jurisdictions' laws apply?
- Do those laws apply to this data?
- What do the laws restrict?
- Do any exceptions apply?
- What measures should be taken to comply with the law?
- Which offices or operations of the organization need access to this data?
- Should steps be taken to limit access to certain data in certain countries?

Organizations should address these issues in advance of a raid, given the difficulty of attempting to do so in the moment.

Protections that may come into play include those regarding banking information (e.g., Swiss Banking Act Art. 47) and other protections that may apply if the authority is foreign to the targeted organization, such as sovereign protection or "blocking" statutes (e.g., Swiss Penal Code Articles 271 and 273) and state secrets laws (e.g., China State Secrets Act).[79] While the GDPR[80] would not limit the powers of an investigating agency, the organization should be mindful of personal information covered by the GDPR and take steps to safeguard against *any* sort of unauthorized disclosure.

---

[79] *See also* French Law no. 68-678 of July 26, 1968, relating to the Communication of Economic, Commercial, Industrial, Financial or Technical Documents and Information to Foreign Individuals or Legal Entities, as modified by French Law no. 80-538 dated July 16, 1980, Art. 1 ("Subject to treaties or international agreements it is prohibited for any individual of French nationality or who usually resides on French territory and for any officer, representative, agent or employee of an entity having a head office or establishment in France to communicate to foreign public authorities, in writing, orally or by any other means, anywhere, documents or information relating to economic, commercial, industrial, financial or technical matters, the communication of which is capable of harming the sovereignty, security or essential economic interests of France or contravening public policy, specified by the administrative authorities as necessary [emphasis added]."); *id.* at Art. 1b ("Subject to any treaties or international agreements and the laws and regulations in force, it is prohibited for any person to request, to investigate or to communicate in writing, orally or by any other means, documents or information relating to economic, commercial, industrial, financial or technical matters leading to the establishment of proof in light of foreign administrative or judicial proceedings or as a part of such proceedings."); *id.* (permitting foreign disclosures conducted under international agreements or treaties); French Law no. 2016-1691 (Sapin II Law) (requiring the Agence française anticorruption to ensure compliance with blocking statute by organizations, under investigation by foreign authorities, that have entered into agreements requiring the appointment of a corporate monitor).

[80] In general, privacy protections will not preclude authorities' access to information seized in a raid. That does not, however, end the headaches that may ensue for organizations dealing with the aftermath of a raid.

Comment 7(c). *Legal Privilege.* It is outside of the scope of this *Commentary* to survey global privilege law,[81] but it is clear that protections for legal privilege vary significantly across jurisdictions. For example, as a general proposition, the attorney-client privilege may be strong in the U.S., less so in the UK, and largely inapplicable in many other nations. Organizations should educate themselves as to privilege rules applicable to their information, as well as the procedures in place that authorities apply to privileged information in dawn raids.[82] Organizations should also put in place a protocol to determine how to manage privileged content, particularly when data is removed from the organization. Further, organizations should proactively engage with regulators to understand and influence the process. This should take the form of advising the regulatory agency of the names of all in-house and outside counsel, as well as law firm names, and to the extent known, particular issues and areas that counsel has been consulted on and that may be privileged.

In addition to the process afforded by the authority, organizations should conduct their own privilege examination of seized information. An organization's failure to be diligent in reviewing its own files and promptly raising privilege objections may be seen in some jurisdictions as a lack of concern about authorities' use of the privileged information and lead to negative outcomes. (See Comment 8(d).)

Comment 7(d). *Confidentiality.* Organizations similarly should seek to have a protocol put in place to manage confidential information for the whole lifecycle of the investigation. The protocol should specify the conditions under which a document will be deemed confidential, and the requirements for preserving confidentiality.

Comment 7(e). *Security.* Although security often is assumed when a governmental body seizes data, organizations must familiarize themselves with security conditions during and after the raid. As noted, organizations should implement security protocols for the whole lifecycle of the investigation, enable a secure investigation environment, and confirm encryption for data in transit. Among the ways to promote security are to: ensure that the search is consistent with the scope of the warrant; consider objecting to disproportionate searches (such as wholesale collections and forensic images of laptops); and follow up on data return/destruction at the appropriate time.

Comment 7(f). *Third-party rights.* Third parties' protected and sensitive information and property may be caught up in a raid in the same manner as those of the subject. While authorities are generally bound to confidentiality and may return seized data following completion of the investigation, they may also share seized information with other regulators in certain circumstances.

---

[81] *See generally Sedona Cross-Border Privilege Commentary*, *supra* note 8 An interesting overview of the Legal Professional Privilege before EU Courts in competition proceedings is set out in the OECD LPP Report, *supra* note 59.

[82] *See* INVESTIGATIVE POWERS REPORT, *supra* note 19, § 2.5 (discussing variations of process for protecting legal professional privilege during raids).

Third parties should consider the legal and contractual obligations of the data controller to their information, including to notify the third party of a seizure and to cooperate in ensuring that appropriate steps are taken to obtain an accounting and to protect such information.

Notice requirements vary according to jurisdiction, parties, and subject matter. In general, authorities have no obligation to notify data owners of seizures. Similarly, it is likely that a transfer of protected information to an authority in a dawn raid or through subsequent legal means would not constitute a breach of data protection regulations or require notice by the organization. For example, there is no requirement under the GDPR that organizations notify persons whose personal information was seized by the EC or EU authorities in a dawn raid, although non-EC/EU authorities are outside of this safe harbor.[83] There may, moreover, be contractual or prudential reasons for notice.[84] Organizations, however, are cautioned to consider coordinating any such notice with authorities, as giving notice may be viewed as interfering with the investigation by tipping off other suspects. As previously noted, obstructive conduct has reinvigorated many an investigation that had already gone stale on the merits.

***Principle 8*. Organizations should assess their response to a raid and consider any mitigation and remediation steps appropriate to protect their data rights and those of third parties that are affected by the raid, and to improve future responses.**

---

[83] *See* Letter of EDPS assistant supervisor Wojciech Rafal Wiewiorowski, Subject: Investigative activities of EU institutions and GDPR (Oct. 22, 2018), https://edps.europa.eu/sites/edp/files/publication/18-10-30_letter_investigative_activities_eui_gdpr_en.pdf (while GDPR Article 14(1)(e) requires controllers to inform data subjects about the "recipients or categories of recipients" of their personal data, GDPR Article 4(9) specifies that "public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients," and so no notice is required).

[84] Further question as to governmental authorization and notification is raised when evidence is seized by nonstate actors with judicial authorization to conduct forced, no-notice inspections similar to dawn raids. One example is a counterfeit search and seizure action (*saisie contrefaçon*) initiated through an ex parte request of a court by the owner of an intellectual property right. Upon a sufficient showing, a court may authorize an independent expert or supervising solicitor (sometimes backed by locksmith, police, party solicitors, and technicians) to conduct an unannounced inspection on the infringing party to obtain evidence confirming the infringement. *See* Jan-Diederik Lindemans, *Transatlantic "Hide and Seek": Proving Infringement of Intellectual Property Rights through Pre- Trial Proceedings for Taking Evidence in the United States and the European Union*, E.I.P.R., Issue 8 pp. 455-62 (2013), https://fordhamipinstitute.com/wp-content/uploads/2015/11/Sunrise-III-2-Lindemans-Jan-Diederick.pdf. While not a dawn raid, similar private remedies may raise similar data privacy and protection issues and are available in a variety of jurisdictions, including the UK and other common law countries (*e.g.*, Anton Pillar orders, which more closely resemble contempt proceedings), other EU nations, and the U.S. (*e.g., D*irective 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Art. 7*,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004L0048R%2801%29; 17 U.S.C. § 503(a); *see also* 18 U.S.C. §1836(b)(2)(A)(ii) (authorizing court under the Defend Trade Secrets Act to issue an ex parte order enabling the seizure from defendants of "property" containing plaintiffs' trade secret information; utilizing law enforcement to take possession of data, documents, and repositories identified in the order as containing such information; and the appointment of neutral technical experts to facilitate such seizure).

Comment 8(a). *Post-Raid Challenges to Actions*. Issues with the authorization, scope, conduct, and implications of the raid may be evident from the beginning. The organization should be familiar with the grounds to challenge such raids in court, including to move to block follow-on raids and require protections and restrictions on the use of the information obtained. Organizations may have an advantage if they strategically deploy knowledgeable counsel to shadow investigators, understand investigators' search strategies and how they conform to scope as defined in the inspection decision, and ensure that investigators follow procedure and respect privilege. While authorizing instruments are often so high-level and broad as to frustrate efforts to rein in overbroad search and seizures, it is critical to assert objections in real time and insist that they are recorded in the minutes of the raid.[85] As discussed below, further investigation may also uncover additional support for or reason to assert such challenges.

Comment 8(b). *Post-Raid Assessment: Initiate an Internal Investigation.* At its earliest opportunity, the organization will want to understand the scope and purpose of the investigation, and the underlying facts. The first step is to determine what records and data have been seized and undertake an internal investigation into the underlying conduct. The goals of the internal investigation are two-fold: first, to understand the organization's exposure and options, including whether it has an obligation to self-report or may want to come forward for purposes of earning cooperation credit; and second, what, if any, obligations and rights the organization has in relation to the seized records and data.

As to the first goal, the internal investigation should be conducted in order to understand substantive and other risks to the organization from the agency conducting the raid, from other regulators with whom the authority may share its information, and from competitors who may have filed a complaint to spur the raid or were alerted to the raid or the investigation. For instance, it is possible the agency conducting the raid may share information seized with other agencies in its own government or with foreign governments if the investigation is a multistate investigation. The internal investigation will often proceed beyond the information seized. For raids conducted by a competition authority, the organization will urgently want to reach a conclusion about the potential for an application for leniency. Success may be measured in days, hours, or even minutes, where credit is granted to early actors.

As to the second goal, to the extent that the investigation identifies data from third parties that has been seized in the raid, the organization will need to assess its obligations to those parties. Those obligations may include giving notice and an opportunity to intervene, consistent with confidentiality requirements, if any, that may apply under the circumstances of the raid and the larger investigation.

Comment 8(c). *Maintaining Privilege.* Typically, the organization should engage experienced outside counsel to conduct the investigation, thus maximizing the extent that the investigation is covered by

---

[85] The European Court of Justice's decision in *Deutsche Bahn AG and Others v. European Commission* (Case C-583/13 P) (ECJ 2015) illustrated the utility of such practice. Among the factors that the court looked at in determining whether out-of-scope evidence was seized in a raid through a permissible "accidental" discovery or an impermissible "targeted search" are the contemporaneous minutes of the search. A subject's after-the-fact reconstruction of what occurred may be viewed as less credible.

lawful privilege (noting that privilege protections may vary from jurisdiction to jurisdiction). While the organization may ultimately decide to waive any privilege to present results of the investigation in return for leniency, without proper planning, there may be nothing to waive. Additionally, government agencies may disfavor an investigation conducted solely by the internal resources of the organization that is under investigation, as they may be perceived to lack independence. Thus, this *Commentary* recommends engaging outside counsel, and more specifically, outside counsel without substantial other business with the organization, such that the investigation, and its work product, will be viewed as independent and objective.

Outside counsel should consider hiring an independent forensic IT consultant to conduct the on-the-ground investigation as to what data and records were seized. Again, this puts an objective outside expert in the position to record and assess what was seized, what remains, and to what extent other relevant materials are available and may need to be produced. As discussed above, it is critical to expedite this review by compiling a comprehensive record of all data and devices seized during the raid and retaining copies when possible.

Comment 8(d). "*Clean-Up" Subpoenas*. In the U.S., the government team executing the search warrant will often serve a grand jury subpoena in connection with the dawn raid as insurance for obtaining all relevant data and records, including records and data that the team may have missed in the search. If the government agency does serve a subpoena or civil investigative demand in connection with or after the raid, it becomes even more important to determine through an internal investigation what materials have been seized and whether materials that have not been seized are nonetheless subject to production to the government under the subpoena. The timeframe for a response will typically be very short. In order to fully comply with the subpoena, the internal investigator may have to examine laptops and mobile phones of employees who were not present during the raid or who work remotely, backup servers, cloud-based data, and other data sources that were not subject to search. Even absent a subpoena or investigative demand, the organization should authorize the investigative team to fully explore potentially relevant sources of documents and data in order to have a complete understanding of the organization's potential exposure.

Comment 8(e). *Notification and Dawn Raid Plan for Other Facilities/Locations.* The organization should also consider the possibility of further raids—for the instant investigation and any later investigations—and how best to respond to make such raids less disruptive and risky to the organization. Such response must be consistent with legal obligations, including cooperation and preservation obligations in relation to the investigation.

If the organization does not already have a dawn-raid policy in place, it should consider creating and implementing such a policy as quickly as possible and distributing it to other facilities and locations. Elements of a dawn-raid policy are set out in the Appendix hereto. The organization, working in concert with outside counsel, should analyze whether there are obvious facilities and locations for a follow-on raid, and, to the extent possible, pre-position legal assets on location to be prepared to respond. For example, some organizations should make sure to have in place several high-volume portable storage devices to make a contemporaneous copy of all data transferred to the authority.

The organization should also consider the following proactive data control steps:

- organizing information in a manner more conducive to cooperation so that any additional search will be less disruptive to the organization;
- understanding and evaluating the extent, use cases, and limitations on cross-border access to information in protected jurisdictions;
- strengthening access controls and need-to-know policies;
- implementing encryption and digital rights management software;
- limiting proliferation of information across locations/jurisdictions; and
- maintaining encryption keys locally, so that seizure or point of access in one location does not compromise security elsewhere.[86]

Comment 8(f). *Advice to Employees—Potential Approach by Investigators.* A critical part of the organization's response is to prepare its employees for the possibility that they may be contacted by government authorities as part of the post-raid investigation. The best practice is to instruct employees how to conduct themselves before a dawn raid occurs; mock dawn raids and practice dry runs may help. Employees should be advised of their rights and responsibilities, both in terms of the substance of the investigation and any requests government agents might make for records or data within the employee's care, custody, or control. The investigating agency may even move to execute searches at the homes of individuals, including employees, owners, directors, and, in some cases, legal counsel.

In general, employees that are approached by investigators have the following rights and responsibilities. **Organizations should confirm consistency with local governing law.**

- The employee has the right to know that there is an investigation that relates to particular issues as described.
- The employee has the right to speak with an investigator.

---

[86] The organization must ensure that any such steps are consistent with its cooperation obligations, including to not inappropriately hinder an investigation and to preserve data sought and of relevance to the investigation. *See supra* Cmt. 1(c). Switching to ephemeral messaging in the midst of an investigation with ongoing preservation obligations, for example, will likely be viewed negatively through the prosecutorial lens. *See, e.g.*, FTC v. Noland, No. CV-20-00047-PHX-DWL, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021) (sanctioning defendants that, the day after learning of government investigation, switched to the Signal ephemeral messaging platform and set all messages to "auto-delete," finding they intentionally deprived agency of relevant documents); Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 WL2870106 (W.D. Ark. July 3, 2019) (finding that use and "necessity of manually configuring [the messaging app] Signal to delete text communications" by plaintiffs was "intentional and done in bad faith").

- The employee has the right not to speak with an investigator to avoid providing potentially self-incriminating answers.[87]

- The employee has the right to speak with the investigator with counsel present.

- The employee should be courteous and professional at all times.

- If the employee speaks with an investigator, the employee should tell the truth in all respects and should not guess or speculate as to any matters.

- The employee should not take any action to destroy, delete, edit, or modify any records or data in the care, custody, or control of the employee.

- If the employee is asked to provide organization documents or data or is asked to provide access to organization IT platforms, the employee should not refuse the directive but may request that the investigator instead direct the inquiry to counsel for the organization.

- If the employee does have relevant records or data in its care, custody, or control, the employee should notify organization counsel or the investigation team immediately.

- If an employee is approached by an investigator, the employee should notify the organization's counsel or the investigation team of the contact immediately.

Of course, nothing in the advice to employees should suggest in any way that the employee may obstruct or impede the investigation. That said, the organization *normally* is entitled to notify its employees that the investigation is ongoing and to advise employees of their rights and responsibilities. In appropriate circumstances the organization might consider offering to provide independent, individual counsel for some or all of its employees. There may, however, be particular investigations where disclosure is forbidden (e.g., relating to national security) or discouraged (e.g., where prosecutors wish not to tip off persons).[88]

---

[87] *See* Judgment of 2 February 2021, DB v Commissione Nazionale per le Società e la Borsa (Consob), C-481/19, ECLI:EU:C:2021:84. (recognizing that the EU Charter of Fundamental Rights provides for a right to remain silent for natural persons in administrative investigations; precluding penalties for persons who refuse to provide potentially self-incriminating answers to investigating authorities under EU Directive No 2003/63 and EU Regulation No. 596/2014.4).

[88] Indeed, authorities may view paying for counsel for employees to be evidence of noncooperation or obstruction if the payment appears conditioned on adherence to facts that the authority believes all involved know to be false. The DOJ previously took an even more extreme position on this. In the now-withdrawn "Holder memo," the DOJ indicated that in some circumstances "a corporation's promise of support to culpable employees and agents, either through the advancing of attorney's fees, [or] through retaining the employees without sanction for their misconduct . . . may be considered by the prosecutor in weighing the extent and value of a corporation's cooperation." Memorandum from Eric Holder, Deputy Att'y Gen., to all U.S.D.O.J. Component Heads and U.S. Att'ys (June 16, 1999), *available at* https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2010/04/11/charging-corps.PDF. The DOJ now

Comment 8(g). *Remediation*. The internal review following a raid may uncover issues that the organization wishes to address independent of the underlying investigation, e.g., violations of legal, contractual, and organization requirements; inefficiencies; failures to follow best practices; difficulties in responding to the raid; compliance weaknesses; IT weaknesses; and information management gaps. The internal review may provide the necessary information for the organization to both proactively address data and records issues highlighted by the dawn raid and confront the underlying matters that are the subject of the investigation.

Comment 8(h). *Disclosures*. Some of the most complicated issues that arise in the aftermath of a dawn raid are whether and how to disclose the fact of the raid, the larger investigation and remediation, and what data was collected. The post-raid review should be the starting point for these issues.

Potential disclosure targets include insurers, auditors, other regulators, contract parties, and the market, as well as third parties whose proprietary, restricted, or personal information has been seized during the raid. Authorities conducting dawn raids are generally operating under appropriate exceptions as to transfer and processing of personal/restricted information. However, there may be contractual and other obligations, as well as business imperatives, to notify customers and other third parties whose information has been seized or implicated in the investigation. One difficult determination is how to approach making disclosures to stakeholders whose data may have been collected by the investigating body. Especially in a climate of increased sensitivity regarding data privacy, there may be reasons to consider telling customers that their personal data was seized by the government during a raid.

Further, if the organization were to determine after the fact that personally identifiable information that was nonresponsive to a subpoena was collected, the organization could work with the government to seek appropriate redactions or, if necessary, challenge the storage and review of the material. These efforts are often unsuccessful in criminal investigations, especially in the U.S.,[89] but could lend credibility to rebuttals of any possible future allegations that the organization failed to take adequate steps to safeguard personal information, as well as bolster corporate efforts to demonstrate concern for customer privacy.

expressly disclaims reliance on whether an organization is paying its investigated employees' attorney fees or providing them counsel, while still holding that "[i]f the payment of attorney fees were used in a manner that would otherwise constitute criminal obstruction of justice—for example, if fees were advanced on the condition that an employee adhere to a version of the facts that the corporation and the employee knew to be false—these Principles would not (and could not) render inapplicable such criminal prohibitions." USJM, *supra* note 10, § 9-28.730.

[89] *See, e.g.,* United States v. Davis, 767 F.2d 1025, 1033–34 (2d Cir. 1985) (siding with the DOJ in a challenge to a criminal investigation on comity grounds).

APPENDIX: ORGANIZATION CHECKLIST IN PREPARATION FOR DAWN RAIDS

While a chronological structure can be effective, ensuring that the response is functional under the pressure of a dawn raid is paramount, and preparation could be structured as follows:

- Pre-Raid Preparation: Sections on introduction, roles and responsibilities, legal rights and obligations, and training and rehearsals. This part focuses on the groundwork and readiness before any raid occurs.

- During the Raid: Starting with immediate actions upon the arrival of investigators, followed by detailed procedures for document handling and communications. This part is structured around the sequence of events typically occurring during a raid.

- Post-Raid Follow-Up: Focused on the aftermath of the raid, detailing the debriefing process, legal follow-up, and any necessary adjustments to the plan based on lessons learned.

When preparing, keep the following checklist in mind:

1. Policies

a) A formal, written policy should be developed for dealing with dawn raids and customized to the location in advance.

b) That policy should include at minimum:

1) Detail immediate tasks to be undertaken during a dawn raid.

2) Identify responsible persons (e.g., reception, head of building or plant, IT, head of communications, and in-house counsel).

3) Identify pre-engaged outside counsel and IT, electronic discovery, and/or forensic vendors.

4) Provide detailed actionable material (e.g., a Dawn Raid Plan) that is rolled out and available at all times.

5) Document procedures on data preservation and collection, including privacy and legal-hold notifications.

6) Ensure updating and enforcement of data retention, hygiene, access, and usage policies.

7) Ensure updating and circulation of email/communications channel usage policies (including those regarding marking, storing, and sharing privileged documents) and use/privacy notifications.

8) Evaluate heavily regulated and highest risk operations, as well as high-risk jurisdictions and location.

2. Actionable Materials – Dawn Raid Plan

A dawn raid plan should contain:

a) Detailed instructions and be tailored to each member of the dawn raid team.

b) Up-to-date contact information of all responsible persons, including designated dawn raid team members responsible for coverage of a certain location.

c) Up-to-date contact information for all outside counsel and IT, electronic discovery, or forensic vendors, and which location they are servicing.

d) Detailed instruction at reception at all relevant locations, including the relevant contact information for that location, along with a communication and action protocol in place that describes exactly what information the receptionist should provide and what actions the receptionist should take.

e) IT capabilities that include a computer with controlled access to needed systems.

3. Dawn Raid Team Roles and Responsibilities

Create a designated dawn raid team. Members should be the first responders in the event of a dawn raid. In larger or international organizations with many locations, it is advisable to establish local teams as well as a central directing team. The following roles are typically needed during a dawn raid and should be established in advance:

a) Team leader: One person should be the team leader. The leader is the face of the organization to the authorities, and, preferably, the decision maker for all actions taken during the dawn raid. He or she instructs all team members. Often the team leader is an in-house counsel or executive working with advice of outside counsel.

b) In-house counsel: In-house counsel must be educated as to the rights and limitations of the actions of authorities and the organization's options to object, as well as be responsible for managing the process and challenging inspector actions. They should study the subpoena/warrant or operative document and set limits regarding the inspection based upon the rights of the inspector and the documents. Legal objections should be lodged if appropriate.

Questions should be asked in real time when the inspectors' actions appear to exceed scope or threaten privilege/protection (e.g., collection requests or search terms overbroad in context).

c) Outside counsel: Ideally, outside counsel will be preselected and engaged in relation to the type of inspection (e.g., antitrust) and data issues involved, and

available on call and able to service a specific location within a reasonable time. Outside counsel will generally have the same function as in-house counsel, including specific expertise and experience with dawn raids.

d) Communications lead: One person should be the face of the organization to the news media. The communications lead should rely on predrafted statements and communicate only in consultation with in-house and/or outside counsel. Consider whether a public relations consultant should be engaged.

e) Additional team members: Typically, additional team members are compliance officers, data security officers, or other trained personnel from the organization who will accompany inspectors as they fan out. They will document all actions, including documents viewed or taken, persons questioned, questions asked, etc. Team members will frequently inform and align with the team leader.

f) IT expert: An IT expert (e.g., someone with a background in operations, electronic discovery, and/or forensics and is experienced in working with counsel on legal matters) and at least one designee are needed to ensure that the inspector's questions regarding the organization's data storage practices and policies can be answered (including directing inspectors to required data stores and noting where and how privileged/restricted items are kept).

The IT expert plays a crucial role in scoping data collection and should be knowledgeable enough to make educated suggestions on how to accurately guide the inspector's requests. It is critical that the IT expert can identify, preserve, and ultimately collect required data to make it available to the inspectors and to document and retain a copy of all data provided for the organization (remote support may be required).

This goal may be achieved in several ways, such as:

1) Large-capacity hard drives can be filled with data that is subject to seizure by the inspectors, so the inspectors may take a copy and the team may also keep a copy of exactly what was taken. If there is no ability to keep a copy of what the inspectors seizes, consider asking the court to resolve the issue.

2) Other systems may allow for preservation in place or require longer time to collect, giving the organization time to deliver the required data after the dawn raid. The IT expert should be ready to discuss options of how to deliver data to inspectors in the days after the dawn raid.

g) Forensic specialist: This team member, whether internal or external, should be preselected to assist as needed.

h) Receptionist: Receptionists are typically the first contact and should obtain a copy of the warrant and check its legitimacy and the inspector's identification. Receptionists play a critical role in greeting the government team, timely informing the organization's dawn raid team, especially outside counsel on call, and guiding inspectors to a designated area.

i) Plant security and/or facility management: Plant security may shield off inspectors from regular operations and reroute employees and customers. Plant security will provide access for inspectors under the dawn raid team's supervision while maintaining overall security and confidentiality. Plant security may also be helpful in providing support and supplies as needed (e.g., additional office space, office supplies, chargers, food and water, keeping the facility open after hours as needed, etc.).

4. Training

a) The dawn raid team and additional key people should be trained to ensure they:

1) Understand the objective of a dawn raid.

2) Are aware of the authority's rights and process.

3) Understand the penalties involved in noncompliance.

4) Are prepared to handle the raid as it unfolds and know their roles and responsibilities during a dawn raid.

5) Understand how to ask and answer questions and provide information.

6) Anticipate the steps to be taken after the raid is completed, including the various teams to be involved, as outlined below.

b) In particular, relevant persons should be trained to:

1) Ask for a copy of the search warrant or authorizing instrument.

2) Ask authorities to wait for in-house or outside counsel.

3) Provide a room for the government to wait comfortably (such meeting rooms should be predesignated, adequately sized, and out of view, with access to restrooms; a separate meeting room for the organization's dawn raid team should be in proximity).

4) Be calm and friendly. Do not volunteer information.

5) Understand that, *consistent with local law*, it is their individual choice whether or not to give a statement to the government agents; that they have a right to have counsel present for any interview; that they

may also decline to make any statement; and if they make a statement, it must be truthful.

6) Be aware that privacy and other data protection laws apply, including as to home inspections.

7) Avoid giving passwords without consultation with organization counsel.

8) Avoid giving unsupervised access to systems, and protest if demanded, unless otherwise directed by in-house or outside counsel.

9) Keep notes and document important aspects during the dawn raid, such as questions asked and documents inspected and taken.

10) Take reasonable steps to ensure material questions, requests, objections, and protests are recorded in the investigative minutes and contemporaneously in organization minutes.

c) The dawn raid team and additional key people should practice and be trained with mock exercises.

5. Safety and Security

a) In certain jurisdictions, inspectors or respective police support may be carrying firearms. The dawn raid team should make a positive determination of whether entrants will be armed, take this additional hazard into consideration, and warn organization personnel if appropriate.

b) If t firearms or other weapons are on the premises, the inspectors should be alerted to the type of weapons and their location.

c) Organizations may be responsible for any unauthorized persons on the premises. Confirm the credentials and authorizing documentation of any persons seeking access under assertion of a dawn raid.

6. Data

a) Prepare a data map in advance that identifies and enables understanding of what sort of data is stored, where, and how. The data map may include information on typical data sources that will be requested during a dawn raid and how to preserve and collect it. It may be helpful to make use of existing electronic discovery procedures and tools. This will help in identifying and strategizing about the proper handling of protected, privileged, and sensitive information; in enabling the organization's response to any dawn raid (including minimization of data acquisitions and targeted data acquisitions by authorities); and in helping to understand the organization's exposure from seized information and equipment.

b) Include employee personal/mobile devices and repositories in the assessment and indicate how employees maintain information of the organization. Mobile devices are fair game for seizure in many raids.

c) Identify access points for restricted information, including information maintained outside of the jurisdiction.

7. Technology Support

a) A forensic or electronic discovery technology and services consultant should be identified in advance to help assist with the response to a dawn raid and should possess the necessary equipment to cooperate and protect the organization's interests (e.g., sufficient hard drives to make two copies of whatever data the inspectors copy from organization repositories, without delaying government access).

b) Such a service may also be relevant for immediate analysis and review of seized data to deal with the legal follow-up.

8. Evidence Protection

a) If possible, copies should be made of everything seized, and the organization should make every effort to ensure that original documents are not taken from the premises.

b) Inspectors may, however, take materials without affording the opportunity for copying. To the extent possible, responsible persons should record how information was inspected and taken, what was taken, and obtain copies through post-inspection processes. Log files of searches on accessible systems should be secured.

1) For instance, U.S. federal law enforcement typically will schedule time at a later date when counsel for the organization can come into the federal building with a copier and make copies of certain critical files or files otherwise afforded access.

c) Reasonable efforts should be made to identify sensitive materials, including personal information, trade secrets, and confidential information, and make this known to the government regulators.

d) If what is searched and taken is excessive, a qualified person (generally counsel) should lodge a protest and request that the authorities preserve but not review until a court can hear the issue.

9. Documentation and Debriefing

a) Once the search is complete, government investigators are required to leave a copy of the search warrant or the document authorizing the raid, along with

a receipt of items seized. The receipt should provide a reasonably detailed description of data, documents, and other materials seized by the investigators.

b) Separately, the organization should prepare its own inventory of data, documents, and materials seized, and ask the government investigators to sign it, indicating what they have taken and what they agreed or did not agree to do. Although the government may decline to sign the organization's inventory, if done properly, it will be a critical contemporaneous record of the search and seizure.

c) The organization should hold a debriefing meeting with all members of the dawn raid team and conduct a postmortem of the raid in order to get a firm understanding of all actions that occurred, especially where in the facilities the inspectors went, who was interviewed, and what was accessed and copied or seized.

d) In-house or outside counsel should prepare a report of the raid, consolidating all notes taken by the dawn raid team, including all property and information taken, all information copied, all persons interviewed, all questions asked by investigators as well as answers given, and the authorizing documentation.

e) To the extent possible, identify and correct any inaccurate information provided to investigators.

f) The organization should follow up on unanswered questions or incomplete answers.

g) Management and employees should be instructed not to speak to the news media and to refer media inquiries to the designated contact.

h) Depending on the authorizing instrument, once government investigators have completed the raid and leave the premises, they are not allowed back, absent exigent circumstances, unless they obtain consent or obtain a new search warrant.

However, should the raid not be completed in one day, and the inspectors/agents indicate that the search will continue into another day, inspectors may return and seize additional evidence, including data, and may even seal the relevant portion of the premises pending completion.

Management and employees should be made aware and instructed accordingly.

i) The fact that a dawn raid has occurred at the 'organization's premises will likely become public knowledge through media reports. The organization should consider immediately preparing a press statement, which would be made available in response to media inquiries. The statement should be reviewed and approved by counsel for the organization before issuance.