How to Conduct an International Internal Investigation

Author:

Donald C. Dowling, Jr.

Littler®

Fueled by ingenuity.
Inspired by you.

Imagine an anonymous worker at a multinational's Egypt factory contacts the global whistleblower hotline and accuses the Cairo plant manager of dumping chemicals into the Nile. Or imagine the manager of a bank's Mexico City branch reports that her secretary's family seems to be trading on inside information. Or imagine an employee of a multinational's Marseilles office complains that one of her co-workers keeps groping her. Or imagine the U.S. Justice Department contacts a multinational's Milwaukee headquarters to ask about some lavish dinners the Middle East sales team hosted for officials in Saudi Arabia.

Any of these incidents, if it actually occurred, would be serious and could be criminal. Obviously a multinational receiving unproven allegations like these needs to find out what really happened. This means launching an internal investigation. Multinationals—particularly those headquartered in the United States—fully appreciate this. They know not to ignore or suppress information about possible wrongdoing. They recognize the value of conducting a thorough inquiry to find out whether what someone claims happened did or did not happen.

Additionally, outside of the United States employment-at-will regime, a thorough internal investigation can be vital because labor judges hold local employers to high burdens of proof. Overseas, an employer that disciplines or fires someone for committing a bad act will need to be able to prove it. An internal investigation can get the employer the proof.

In the last couple of decades, the state of the art for how companies conduct their internal investigations has evolved considerably, particularly in the United States. At multinational organizations, internal investigations often cross national borders, and so investigatory practices become a *cross-border* matter. A U.S.-headquartered multinational looking into suspected wrongdoing in overseas operations tends to want to export its sophisticated made-in-America toolkit of internal investigatory best practices. U.S. management and the U.S. board of directors may insist that a cross-border investigation be thorough enough to satisfy their tough American standards. They will resist backing off, rolling back, watering down or loosening up their good investigatory practices even in the face of an overseas local who protests *"…but you don't understand—that's not how we do things around here."*

But conducting an overseas investigation in the U.S. style can trigger possible legal challenges. And of course, an international investigation has to stay strictly legal—investigators inquiring into possible criminal misconduct cannot afford to be caught breaking the law themselves. In addition to legal compliance, internal investigations should not disrupt an organization's own internal operations, and should avoid causing ancillary cultural (and human resources) problems.

Our discussion here addresses a multinational seeking a way to resolve this conflict, a way to project-manage a cross-border internal investigation to meet headquarters' high standards while also complying with applicable laws and accounting for overseas expectations hostile to American-style investigatory practices. We first set *context* by analyzing four threshold strategic considerations when conducting an international internal investigation. Then we address *process*, detailing four stages and thirty steps for how to conduct an effective and compliant cross-border investigation.

Context: Threshold strategic considerations in an international internal investigation

Before embarking on the specific steps and stages of a given cross-border internal investigation, account for threshold strategic considerations in play. Specifically, think about: (A) the cross-border character of the investigation; (B) the size and scope of the investigation; (C) exporting headquarters' investigatory practices; and (D) the disparate categories of law affecting international investigations.

A. ***Cross-border character of the investigation.*** Most internal investigations are local domestic, with the accuser, the target, the witnesses, the investigators and the alleged incidents all in the same country, and the investigation

triggering issues only under that country's domestic law. Our focus here, however, is on *international* investigations—those that cross national borders. International or cross-border internal investigations may be less routine than local domestic ones, but they are increasingly common in today's interconnected world. And of course they tend to be much more complex, with more serious ramifications.

There are three kinds of international internal investigation. The first, conceptually the simplest, is one we might refer to as a "foreign local investigation": an internal investigation where headquarters in one country investigates an otherwise-local incident of possible wrongdoing in a single foreign country. For example, imagine a multinational's Kansas City headquarters looks into conflict-of-interests charges against the company's country manager in Brazil, or looks into suspected possible embezzlement by a company bookkeeper at a call center in Mumbai, or looks into a bullying charge against the manager of the Lisbon office.

The second kind of cross-border internal investigation is one we might refer to as the "international problem investigation": an internal investigation into possible wrongdoing that spans a number of countries, but that is not yet threatened to be litigated in any one jurisdiction's courts. For example, imagine a company suspects improper discussions about price-fixing might have happened between its sales teams and competitors in Buenos Aires, Santiago and São Paulo. Or imagine an investigation into a data breach that occurred in Russia and leaked personal data of customers across Europe. Or imagine a sex-harassment charge where the victim is based in Toronto, the alleged harasser works in Miami and the allegedly-inappropriate behavior happened at a sales meeting in Cancun.

The third kind of international investigation—the kind that gets the most attention and that tends to be the most complex—is what we might call a "court/agency charge international investigation": an internal investigation into incidents that are the subject of threatened or pending civil or criminal proceedings in a court or agency of at least one country, but involve evidence or incidents overseas. Examples include internal investigations responding to "extraterritorial" charges under U.S. federal "white collar" criminal laws like prosecutions under the U.S. Foreign Corrupt Practices Act (FCPA) alleging bribery of foreign government officials, or like investigations responding to charges under U.S. securities laws that allege insider trading infractions at overseas offices. Another example is an investigation involving a proceeding by European "competition" (antitrust) authorities with tentacles reaching back into a U.S. company headquarters. Another example is any investigation relating to EU-level court or agency proceedings involving more than one EU member state. Another example is an investigation relating to a civil lawsuit in an American court seeking discovery in, and making allegations implicating, company operations overseas.

Seminars and articles on conducting international investigations tend to focus, sometimes exclusively, on these high-stakes court/agency charge international investigations. But in the real world, the vast majority of international internal investigations are foreign local investigations and international problem investigations. Our discussion here addresses investigations under *all three* scenarios; references here to "international" or "cross-border" investigations include foreign local investigations and international problem investigations *as well as* court/agency charge international investigations.

B. ***Size and scope of the investigation.*** Internal investigations get drawn out, complex and expensive when they look into high-profile criminal allegations and "bet-the-company" claims alleging bribery, sabotage, embezzlement, tax fraud, insider trading, antitrust collusion, workplace violence, environmental crimes, audit/accounting fraud and the like. For example, an American personal care products company once disclosed in an SEC filing that it had spent *$247.3 million* on a single internal investigation. The fact that internal investigations can get so drawn out, complex and expensive has become widely recognized. In one situation, an alleged extortionist is said to have used the high price of internal

investigations as cover to launder an illegal demand: According to CNBC, a 2019 federal "criminal complaint" alleges that Michael "Avenatti offered to refrain from" making public accusations against a company if it would "agre[e] to retain" him "to conduct an internal investigation" that the company "did not request," and as his "investigation" fee, "Avenatti…demanded to be paid, at a minimum, between $15 and $25 million."[1]

While many high-profile internal investigations are expensive, drawn out, and complex, those are exceptional, and for every one of them, companies conduct many quicker, simpler and less expensive inquiries into allegations that would not necessarily constitute serious crimes or bet-the-company exposure. Shorter internal investigations tend to be straightforward, especially if they do not involve outside experts. Many internal investigations (even many *international* ones) are relatively streamlined inquires that look into fairly routine matters like workplace injuries or lower-stakes accusations of petty theft, bullying, harassment, vandalism, expense-account fraud, attendance infractions and conflicts of interests.

Seminars and articles on international investigations often seem to assume these projects are inevitably drawn out, complex and expensive. Our discussion here addresses *all* international internal investigations—large, small and in-between. Even a smaller border-crossing investigation must comply with applicable law and cultural expectations.

C. ***Exporting headquarters' investigatory practices.*** A multinational seeking to conduct cross-border internal investigations that meet headquarters' standards while conforming to overseas laws and cultural expectations should think through how it can strike this balance—how it can adapt its investigatory practices developed at headquarters to very-different environments overseas.

Internal investigations occur around the world. Certainly, conducting thorough investigations has become routine among companies based in common-law jurisdictions. Under law in Australia and New Zealand, for example, investigations need to be thorough to comply with the principle of offering a target "procedural fairness and natural justice." In England, "[i]t is important to carry out necessary investigations of potential disciplinary matters without unreasonable delay to establish the facts of the case."[2] Workplace discrimination investigations are mandatory in Ontario, at least in situations where discrimination is later found to have actually occurred.[3] Similarly, the British Columbia Worker's Compensation Act requires employers launch immediate investigations into workplace accidents that require medical treatment.

In some common law countries, an employer that fails to conduct a thorough investigation faces significant exposure; for example, a court in Australia awarded AUS$1.5 million in a workplace bullying claim, in large part because the employer had failed to follow up on the victim's complaints.[4]

Also, conducing a good internal investigation is important beyond the common-law world, and in many civil-law jurisdictions an internal investigation is actually *mandatory*. Austria's Supreme Court requires employers investigate sex harassment complaints,[5] as does a May 2018 amendment to employment law in Korea, and as do statutes in Chile, Costa Rica, India, Japan, Venezuela and elsewhere (including South Africa, which is common law). A proposed 2019 European Union directive to take effect in May 2021 would require investigating ("diligent follow up to") whistleblower complaints received over "internal reporting channels."[6]

1 Dan Mangan and Kevin Breuninger, *CNBC* news report, Mar. 25, 2019.

2 U.K. Advisory, Conciliation & Arbitration Service [ACAS] *Code of Practice on Disciplinary and Grievance Procedures*, Mar. 2015 at ¶5.

3 *Scaduto v. Ins. Search Bureau*, Human Rights Tribunal of Ontario [HRTO] Feb. 24, 2014 at ¶¶ 78, 79, 82; *Sears v. Honda of Canada*, HRTO Jan. 13, 2014 at ¶161; *Morgan v. Herman Miller Canada*, HRTO Apr. 18, 2013 at ¶ 95; *Ibrahim v. Hilton Toronto*, HRTO Apr. 22, 2013 ¶¶ 111,113.

4 *Robinson v. State of Queensland* [2017] QSC 165 (Sup. Ct. Q'land Aug 2017).

5 Austria Supreme Court decision 9 ObA 131/11x, Nov. 26, 2012.

6 EU dir. 2018/218 at art. 5(1)(c).

However, while internal investigations are virtually universal, how an employer conducts an investigation varies greatly from country to country. Not surprisingly, the United States stands at the robust end of this spectrum. In the United States, lawyers (often former federal prosecutors), consultants, private investigators, forensic accountants and other professionals specialize in conducting thorough—sometimes multi-million-dollar—investigations using high-tech procedures. The uniquely American environment of employment-at-will plus the lack of a comprehensive federal data protection law leave U.S. employers largely free to investigate staff wrongdoing broadly.

At the other end of this spectrum, though, are all the countries where an employer investigation tends to be cursory—by American standards, inadequate. In some parts of Continental Europe, Asia, Latin America and Africa, prevailing cultural and human resources norms assume an internal investigation will not rock the boat, will comply with restrictive employment and data privacy laws, and will respect the local company hierarchy, even if that means the investigation leaves some stones unturned. There are even some jurisdictions where formal investigations are deemed a police matter outside the province of companies, where an internal company inquiry needs to fly beneath the "radar" of local police.

This means American multinationals exporting American investigatory toolkits run into problems. One commentator has noted, "some countries are not used to the 'American style' of investigations. They are quite interested in protecting their privacy and employment rules of the workplace."[7] An in-house lawyer at a major American multinational once told an American Bar Association conference (Atlanta, November 1, 2012): "One of the biggest mistakes an investigator can bring to a foreign investigation is an American mindset." One London solicitor addressing American lawyers about investigations outside the United States explained:

> Most corporations that have faced a significant [international] investigation will be familiar with the need to balance the thoroughness of the investigation with the need to respect the [overseas] suspect's and the informant's data protection rights. Increasingly we are seeing [overseas employee] suspects and their advisors seek to exercise these rights to slow down or halt an investigation [outside the United States]. In at least one case where I have been involved, injunction proceedings were threatened [to stop the U.S.-driven internal investigation].[8]

Any multinational conducting investigations abroad needs to confront the differences and strike its own particular balance. Americans, understandably, want to do investigations right; they are reluctant to put aside tough investigatory tools and frustrated about tampering with proven investigation strategies and well-honed practices. At the same time, no organization means to send out investigators who burst into overseas workplaces, breaking local laws and disrupting local operations.

D. ***Disparate categories of law affecting international investigations.*** We have seen that legal compliance in conducting an internal investigation is crucial—investigators looking into someone else's possible wrongdoing cannot afford to draw misconduct allegations onto themselves; indeed, shortcomings in the investigatory process are susceptible to being exploited for leverage, because the target may have a keen incentive to shift blame, play the victim and accuse investigators of wrongdoing. Of course, to comply with the laws that apply to an investigation, investigators must first identify all those laws.

7 S. Russell-Kraft, "How to Avoid Botching Your Internal Investigations," Law 360, May 22, 2014).

8 J.P. Armstrong, "Anti-Corruption and Bribery Compliance: The U.K. Perspective," *NY State Bar Int'l Chapter News*, Fall 2012 at 5, 9-10.

American investigators can be at a disadvantage in identifying which laws apply to internal investigations because domestic American law leaves internal investigations largely unregulated (*Upjohn* warnings[9] and W*eingarten* rights[10] aside), due to employment-at-will, the absence of any comprehensive federal data protection statute and the fact that American constitutional due process protections do not reach non-government actors. By contrast, in many other countries, private companies' internal investigations must comply with a web of employment law, privacy law and criminal procedure-type rules that protect investigations' targets and confer due process protections.

Identifying the universe of laws that regulate an international investigation is a big task, for two reasons. First is the cross-border hurdle—in an international investigation, more than one jurisdiction's laws inevitably come into play, so investigators must identify and reconcile laws of more than one country. Second is the hurdle of identifying which laws within a given jurisdiction reach an internal investigation. This part can be tricky because disparate legal concepts become relevant. "Internal investigation law" is not some discrete, confined area of law unto itself (like, say, patent law or tax law or workers' compensation law). Rather, within any one jurisdiction, an internal investigation might trigger issues across a range of substantive legal areas. Specifically:

- **Laws directly regulating internal investigations:** A few legal doctrines are specific to non-government organizations' internal investigations. For example, some jurisdictions require giving investigatory witnesses certain notices before an interview ("*Upjohn* warnings," in the United States). And witnesses in internal investigations may enjoy a legal right to bring a representative into certain investigatory interviews ("*Weingarten* rights" in the United States). Some countries require non-government organizations bring in a court or government officer when taking certain investigatory steps—in France, for example, when an employer reads employee emails, and in Switzerland, when an interrogator administers an oath to a witness. Also, in some jurisdictions in some contexts there are sector-specific laws that relate to internal investigations, such as investigation mandates in the financial services sector. And some substantive laws impose some specific rules on investigating certain infractions of those particular laws, like regulation of antitrust investigation responses in the U.S.

  In all, though, only relatively few discrete legal doctrines explicitly regulate how a non-government organization must conduct its internal investigations. The much bigger challenge is identifying the doctrines under *other* substantive areas of law that can spring up in the context of an in-house investigation.

- **Attorney/client privilege and work-product law:** Internal investigators need to understand, up front, which documents, emails, notes, interview tapes and the like can be shielded (withheld from disclosure) under an enforceable privilege. In the U.S., internal investigators stay vigilant about which documents and testimony fall under attorney/client privilege and the work-product doctrine, but these concepts get fuzzy in other countries, particularly outside the common-law world. In jurisdictions like Germany, China, and many others, a U.S.-style attorney/client privilege simply does not exist,[11] or at most, what is called the "privilege" amounts to little more than a requirement or expectation of attorney confidentiality. Countries like France and Hungary may recognize a limited privilege for documents produced by law firm lawyers, but not for in-house counsel, who in some countries are not enrolled members of the bar. There is no European-wide in-house counsel privilege.[12] And countries that offer a local attorney/client privilege may not necessarily extend it to foreign—say, American—lawyers who are not enrolled with their local bar.

9 *Upjohn v. U.S.*, 449 U.S. 383 (1981).

10 *NLRB v. Weingarten, Inc.*, 420 U.S. 251 (1975).

11 *See Wultz v. Bank of China,* 979 F. Supp. 2d 479 (S.D.N.Y. 2013)(stating that Chinese law does not recognize an attorney/client privilege).

12 *Akzo-Nobel*, Eur. Ct. Justice case c-550/07P, Sept. 14, 2010.

All this said, outside the U.S., discovery in civil litigation tends to be far less extensive and so *attacks* on the attorney/client privilege can be rare. Even in international investigations, as a practical matter the privilege analysis may be most relevant to the scenario of someone seeking investigatory files in a U.S. forum.[13] But that said, there are some important overseas contexts where a company may be asked to turn over assertedly privileged documents—data privacy law "access requests," for example, and so-called "dawn raids" by government authorities such as antitrust or tax enforcers.

- **Criminal procedure law:** We mentioned that outside the United States, a private company's internal investigation might actually trigger certain criminal procedure laws even though the company is not a "state actor." For example, certain Eastern European and other countries purport to ban or restrict criminal investigations by non-government investigators. Some internal investigations can trigger laws that require investigators have a government license, and so a non-licensed investigator investigating might be a crime. Some jurisdictions require reporting evidence of a crime over to the police as soon as a private party gets the information, well before the close of its investigation. Some jurisdictions blur or dispense with the concept of "state action," extending into the non-government sector criminal suspects' substantive rights, like the right to be represented by a lawyer in an investigatory interview and the right to remain silent.

- **Employment law:** Outside of the U.S. employment-at-will environment, employment laws can regulate how an employer looks into employees' activities. Indeed, in much of the world the fundamental American investigatory tactic of instructing employees they "must cooperate" in an investigation misstates applicable law: Employees do not actually have to cooperate with an employer's investigation in jurisdictions where a witness's refusal to speak to investigators or turn over documents is not an infraction that supports good cause for discipline.

- **Collective labor law:** In the United States, labor unions tend not to see internal investigatory practices as a mandatory subject of bargaining. Further, *Weingarten* rights aside, American labor unions tend not to have much leverage to impede a specific internal investigation. By contrast, in some countries (particularly in Continental Europe), works councils and other collective labor bodies demand a right to "consult" in advance over the employer's investigatory practices. And labor law in Finland, France and other jurisdictions gives worker representatives leverage to insist on advance information as to how investigators will conduct a slate of interviews, even giving labor representatives a voice in the interview process.

- **Data privacy and state secrets laws:** The United States has a patchwork of data privacy laws, but—other than "wiretap" and stored communications regulations regarding telephone calls and intercepting electronic communications (Electronic Communications Privacy Act, 18 U.S.C. § 2510, and state laws)—few American data protection laws regulate how an employer must conduct an internal investigation, assuming the employer had issued the usual boilerplate statements that extinguish reasonable employee expectations of privacy in company computer systems, files and work spaces.

  By contrast, comprehensive data protection laws overseas like the EU General Data Protection Regulation (GDPR) have profound effects on internal investigations, regulating issues from reading employee emails to reviewing internet search histories to retaining investigatory files to responding to "data subject access requests" that seek investigatory files and interview notes—and also restricting "exporting" personal data back to headquarters, even for internal investigation purposes. And overseas data protection laws can curtail proactive investigatory tactics like searching desks and workspaces, recording, photographing, video monitoring and phone call monitoring.

13 *E.g. Wultz, supra* note 11 (analyzing reach of U.S. attorney/client privilege to documents in China, where there is no privilege, as to discoverability in a U.S. forum).

Further, some countries—China and Russia, in particular—impose tough "state secret" laws that flatly prohibit exporting politically important information, regardless of whether it is personal data.

Complying with data protection (and state secret) laws in cross-border investigations is particularly complex and raises a wide range of legal issues.[14] And the comprehensive data protection laws imposing these restrictions go well beyond Europe. In recent years, many countries the world over have implemented similarly broad data laws; examples include Argentina, Brazil, Canada, Costa Rica, Hong Kong, Israel, Japan, Korea, Mexico, the Philippines, Singapore, South Africa, Taiwan, Uruguay and others.

- **Substantive law of the infraction investigated:** Some internal investigations look into whether an employee merely breached an internal rule, but many (maybe most) investigations look into allegations that might constitute a breach of law. In these cases, investigators must understand nuances of the underlying law allegedly breached. For example, anti-harassment laws in many countries (Australia, Brazil, France and many others) prohibit routine non-discriminatory bullying that would be perfectly legal stateside. As another example, an American company investigating an allegation of bribery overseas needs to understand not only the U.S. FCPA, but also the host country's local domestic bribery law.

While understanding and identifying all these areas of law relating to international investigations is a big task, an international investigation team should streamline its work by putting aside legal issues *unrelated* to the investigatory process itself. Isolate tangential legal matters that do not regulate the investigatory process, even if those matters involve pre- or post-investigatory issues. Specifically, internal investigators frequently brush up against matters of discipline, dismissal, and whistleblowing—but these legal issues tend not to comprise part of an internal investigation and are usually best put aside to address apart from the investigation:

- **Discipline and dismissal law:** Aside from one exception discussed below, procedures and laws regulating firings tend to become relevant immediately *after*, not during, an internal investigation (if the investigation leads to the employer's imposing post-investigatory discipline). Within an organization, often the person administering discipline or doing a dismissal will be someone who was not on the international investigation team.

- **Whistleblowing laws regulating whistleblower hotlines and prohibiting whistleblower retaliation:** Unless an internal investigation happens to be looking into an allegation of whistleblower retaliation, whistleblowing laws have little to say about the internal investigatory process. Whistleblowers' allegations, sometimes submitted via a hotline, *trigger* many internal investigations. But then the investigation digs back into the underlying infraction alleged, not into matters concerning the whistleblowing channel or process itself. And as long as the investigation team avoids being accused of harassing a whistleblower during the investigation (be careful there), the whistleblower retaliation issue tends to become relevant immediately *after* an investigation, as the employer considers imposing post-investigatory discipline and deals with the whistleblower going forward.

With so many legal issues in play in an internal investigation, having a lawyer on (or advising) an international investigation team is a real asset. Unfortunately, though, one lone lawyer may not be enough, unless that lawyer is positioned to field all the varied legal questions likely to arise. For example, a local overseas lawyer may be vital to counsel on an internal investigation in the foreign country, but would not be positioned to advise on, say, the scope of U.S. attorney/client privilege or the U.S. FCPA. As another example, an American white-collar criminal lawyer is

14 *See* "The Sedona Conference Int'l Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices," 19 SEDONA CONF. J. 557 (2018); U.S. Library of Congress, "China: New Implementing Regulations of Law on State Secrets" (Mar. 31, 2014) (*available on* www.loc.gov).

essential when investigating allegations related to a pending or possible U.S. federal criminal prosecution, but might not be positioned to advise on (or even spot issues under) foreign countries' employment, collective labor, and data privacy laws.

Among all the legal issues possibly in play in an international investigation, one constant is that almost every internal investigation outside the United States triggers tricky issues of host country *employment* law. Therefore, most international investigation teams need foreign employment law expertise. This may be less obvious to American headquarters, because in the employment-at-will United States, employment law plays only a peripheral or marginal role in the investigatory process (as distinct from the post-investigatory *disciplinary* process). Sometimes, U.S. investigators see substantive employment law as relevant to investigations into employment law allegations—say, investigations into alleged bullying, harassment, discrimination, equal pay violations, payroll irregularities or immigration/I-9 compliance—but not relevant to investigations into infractions unrelated to the law of the workplace—for example, investigations into alleged insider trading, price-fixing, embezzlement, tax fraud, environmental wrongdoing or data breaches. By contrast, in most countries outside the United States, even an internal investigation into a financial crime or other allegation completely unrelated to employment law triggers nuanced employment law issues *as to the investigatory process itself*, and may also trigger issues of collective labor law and employee-context data privacy law.

Process: The stages and steps for conducting an effective and legally compliant cross-border internal investigation

Having addressed threshold strategic considerations for conducting an international investigation, we turn now to process—the mechanics, stages and steps involved in project-managing a cross-border internal investigation that will meet headquarters standards while complying with applicable laws and accounting for expectations overseas that may be hostile to American-style investigatory practices.

There are any number of ways to break down or unpack the international investigatory process. Because every investigation is different, some components central to one investigation will not be present in others. One helpful way to separate out the issues is to detail the main stages of an international investigation, and then to break those stages down into their component steps. Here is a 30-step checklist for a multinational seeking to project-manage a cross-border internal investigation, grouped into four stages:

1. Take Preparatory Steps *before* the International Investigation
2. Respond Initially to a Suspicion or Allegation Arising Abroad
3. Interview Witnesses Abroad
4. Impose Discipline, Take Remedial Measures and Issue Communications *after* the International Investigation

Stage 1: Take Preparatory Steps *before* the International Investigation

In America, an organization does not necessarily need to take any specific steps before launching an internal investigation. Tapping experienced investigators is a great idea, but otherwise, even a start-up company's first-ever domestic U.S. investigation might come off perfectly well, even if the company had not done anything in advance to pave the way or prime the pump.

Not so abroad. Outside U.S. employment-at-will—particularly in Europe and other jurisdictions with comprehensive data protection laws—an organization needs to clear some preparatory hurdles before it launches an internal investigation into a specific allegation or suspicion of wrongdoing. Overseas, *neglecting* to take these pre-investigatory steps may complicate an internal investigation, and may even make it non-compliant and possibly compromised. Consider taking the following steps outside the United States even before getting a specific allegation or suspicion of wrong doing to investigate.

1. **Implement a Robust Code of Conduct:** A fundamental tool for multinationals that will conduct international investigations is a well-thought-out, properly-launched global code of conduct or business ethics (or package of global policies) that applies to affiliates' employees worldwide. The code should expressly forbid all acts the organization has a compelling business reason to prohibit—insider trading, environmental crimes, bribery/improper payments, antitrust violations, intellectual property infractions, audit/accounting impropriety, conflicts of interests, mishandling data, discrimination, harassment, bullying and the rest.

   The code should be particularly clear on topics that tend *not* to be illegal under most countries' laws—topics like conflicts of interests, supervisor/subordinate sexual relationships and inappropriate conduct on social media. Outside of U.S. employment-at-will, whenever alleged or suspected wrongdoing is not per se illegal, the code of conduct or other work rule becomes central to an investigation, because even if a target is guilty as charged, without a specific code or rule prohibiting the misbehavior, there will be nothing to investigate, as there will be no grounds for discipline. Would-be wrongdoers will point out they did nothing illegal and nothing to break any internal company rule.

   That said, a global code of conduct should also specifically prohibit acts that *are* otherwise illegal. Outside U.S. employment-at-will, where there is no code of conduct or work rule, employee lawbreakers sometimes argue that even a legal infraction is not good cause for discipline or dismissal, especially when the employee broke a law to get the job done, help the employer, or "go the extra mile." Think of, for example, an employee who bribed an obstreperous official who was blocking an important company project, or a sales executive colluding with competitors to raise prices and boost profits, or a plant manager pouring hazardous waste down a drain to save expensive environmental remediation costs.

2. **Launch a Compliant Whistleblower Hotline:** From an American point of view, an effective whistleblower hotline is a strongly recommended practice, both to uncover compliance problems and to provide evidence for investigators. Hotlines exist to elicit allegations, complaints and denunciations for the organization to investigate and then, as necessary, remedy (keep in mind, though, that not all internal investigations start with a hotline tip—many investigations look into allegations that surface "off-hotline"). Without a hotline, wrongdoing is more likely to get covered up and violations are more likely to proliferate. Further, America's Dodd-Frank government whistleblower bounty program motivates employers to launch robust in-house hotlines to lure in whistleblower denunciations that otherwise might go straight to U.S. government enforcers.

   Whistleblower hotlines have become so common in the United States that a mini-industry has emerged of outsourced hotline providers. Indeed, a whistleblower hotline is more than just a strategy—one can be required. Publicly traded American companies and "foreign private issuers" must make report "procedures" available for the "confidential, anonymous submission by employees" of their "complaints and concerns regarding questionable accounting or auditing matters."[15] New York State guidance addressing the financial services sector urges

15 Sarbanes-Oxley Act of 2002, Pub.L. No. 107-204, at §301 (1).

"establish[ing] procedures for ensuring appropriate follow-up to valid [whistleblower] complaints."[16] A recent French law called "Sapin II" requires whistleblower hotlines at employers with more than 50 employees, and in early 2019 the EU proposed a directive to become effective May 2021 that also mandates in-house hotlines—"internal reporting channels" at employers of over 50 employees.[17]

But overseas, especially in parts of Europe, whistleblower hotlines have been surprisingly controversial. Arguments against "report channels" have raged in Europe since at least 2005, when French decisions struck down American hotlines.[18] More recently, Europeans have grudgingly come to accept the utility of workplace hotlines.[19] In early 2019, Spain repealed its law that had prohibited anonymous hotlines.[20] European jurisdictions including France and the EU itself now mandate both internal company hotlines and government-run hotlines, too.[21]

Still, "hotline law" remains complex in Europe, with "data protection authorities" (particularly in France, Scandinavia and Eastern Europe) still taking strident anti-hotline positons in the name of privacy and GDPR compliance. Unhelpfully, the proposed EU directive requiring in-house hotlines expressly defers to GDPR and declines to offer any defense to a hotline privacy challenge.[22] Spanish hotline law imposes its own specific data privacy protections.[23] This said, though, *outside* of Europe, laws—even broad data protection laws patterned on the European model—rarely seem to get invoked to rein in whistleblower hotlines. But complications might arise. In Hong Kong, for example, employees may need to consent to a hotline.

A multinational is well advised (and in some cases required) to offer a global whistleblower hotline which can both initiate cross-border internal investigations and offer up valuable evidence for investigators. Launch and communicate a global hotline thoughtfully, complying with laws in relevant countries while keeping aware of cultural flash points.

3. **Build Channels for Cross-Border Data Exports:** An American multinational conducting a cross-border investigation inevitably sends (that is, "exports"), back to U.S. headquarters, personal information naming or identifying overseas employee whistleblowers, targets and witnesses. EU GDPR and laws in other comprehensive data protection law jurisdictions expressly prohibit exporting employee data to countries like the United States not deemed to offer "adequate protections," unless the data export travels through an approved channel. This is a huge issue under EU GDPR, where for practical purposes the approved data export channels are: "standard data protection clauses"; U.S./EU "Privacy Shield"; "binding corporate rules"; "approved code[s] of conduct"; and (in some contexts only) employee consents.[24]

   Before sending investigators into the EU or another comprehensive data protection jurisdiction to conduct an investigation, first build channels to allow the export of internal investigatory data back to headquarters. Building and expanding cross-border data flow channels can be slow and expensive, so waiting until a specific allegation or suspicion triggers an actual investigation may be too late. As a practical matter, U.S. headquarters may already have channels in place for exporting *other* personal data. For example, maybe U.S. headquarters is "Privacy Shield"

16 NY State Dep't of Financial Svcs. Memo of Jan. 7, 2019 from M.T. Vello, "Guidance on Whistleblowing Programs," pg. 5 point # 6.
17 EU dir. 2018/218, arts. 4-5.
18 *Cf.* D. Dowling, articles at 45 ABA THE INT'L LAWYER 903 (2011) and 42 ABA THE INT'L LAWYER 1 (2008).
19 *See* S. Fuller, "Whistleblowing: Signs of a Shifting Landscape," Int'l Bar Ass'n Global Insight, Mar. 2019.
20 *Ley Orgánica* 3/2018 at art. 24(1).
21 EU dir. 2018/218, arts. 4-6.
22 EU dir. 2018/218 at art. 18.
23 *Ley Orgánica* 3/2018 at art. 24(2).
24 *Cf.* EU GDPR arts. 6(1)(a); 46(2); 49; European Data Protection Board, Guidelines 2/2018 on Derogations of Art. 49 under [GDPR], May 2018.

self-certified or has standard data-protection-clause agreements in place with its European affiliates. Where this is the case, go back and check these channels—amend them, as necessary—to be certain that they expressly cover *investigatory* data.

And in countries like China and Russia that impose tough "state secret" laws prohibiting the export of even information that is not "personal," stake out a defensible compliance positon.

4. **Craft a Strategy for Processing "Criminal" Data:** In the EU and other comprehensive data protection jurisdictions, a special challenge to processing investigatory data locally (and to exporting it back to headquarters) is accounting for heightened data protection regulation of information about possible criminal conduct. This is an acute problem in Europe because EU GDPR article 10 and the EU criminal-data directive (directive 2016/680) impose strict consent and other requirements on handling "criminal" information. While "criminal" information includes data about "criminal convictions," fortunately that poses little problem for most internal investigations, because "criminal convictio[n]" information rarely surfaces during an investigation (conviction data is much more relevant as to pre-hire background checks). However, the problem here is that GDPR article 10 also expressly reaches pre-conviction personal data "relating to criminal…offences or related security measures." Internal investigations routinely look into allegations that some aggrieved employee or some proactive data law enforcer might characterize as a "criminal…offenc[e] or related security measur[e]."

   In the EU and other comprehensive data protection jurisdictions, before launching a specific investigation into a misdeed that might amount to a crime, an investigating organization should formulate a proactive compliance position by which its investigation complies with GDPR article 10, with the EU criminal data directive (directive 2016/680) and with equivalent rules in other countries regulating criminal "offence" data. One strategy is to frame investigations as looking into breaches of internal rules, not "criminal offences."

5. **Grant Mandated Access to the Investigation File:** All competent investigators protect the confidentiality of their investigations to uphold integrity, to shield witnesses and whistleblowers, and to minimize exposure to claims of retaliation, libel or invasion of privacy. In the United States, this comes down to three words: Keep It Confidential.

   Overseas, though, a legal concept unknown to U.S. law can obliterate the ideal of a confidential investigation. Law in the EU and other comprehensive data protection jurisdictions forces an investigating organization (a "data controller") to turn over investigation files, witness statements, whistleblower complaints and even final investigation reports ("personal data") to involved targets and witnesses ("data subjects") who come forward and request to see ("access") them. Specifically, under EU GDPR, whenever a target or witness in an investigation asks "to obtain…access to" investigation files, the organization maintaining those files "shall provide a copy."[25] Further, the investigating organization actually has to disclose to the target and witnesses both that an investigation file exists and that they enjoy a "right" to "access" it upon "request."[26] An EU body once decreed (under GDPR's predecessor law) that employers must tell investigation targets they are being investigated and that an investigation file exists as soon as there is no substantial risk that notice to the target "would jeopardize" the investigation.[27] In addition, a target or witness accessing an investigation file enjoys a "right" to force appropriate changes or additions to the text of investigatory documents in the file—a "right to obtain…the rectification of inaccurate personal data concerning him or her" and "to have incomplete personal data completed, including by… providing a supplementary statement."[28]

25 EU GDPR art. 15(1), (3).

26 EU GDPR art. 14(1)(d), (2)(c).

27 Opinion 1/2006, EU Article 29 Working Party, 00195/06WP 117, Feb. 1, 2006.

28 EU GDPR art. 16.

This so-called "data subject access request" doctrine reaches only personal information about only the person asking. Indeed, the responding organization must omit, redact or anonymize personal information about *others*. But in the investigation context, most all of an investigation file involves the investigated target, so a *target* "access request" in effect demands to see the whole investigation file (as redacted of identifying information about others). EU jurisdictions take this seriously in the investigatory context; cases in Germany, for example, presume a target can see an investigation file even *during* the investigation.

Of course, having to show targets and witnesses confidential investigatory notes and analyses while an investigation is in full swing confounds American investigators, and some have flouted foreign data-access rights to uphold investigatory integrity. But because an internal investigation that violates local law is itself illegal activity that some whistleblower could denounce, always balance investigatory confidentiality against data subject access rights. Stake out a compliance position. Articulate a legitimate business case for deferring access until investigations reach a stable point. Do all this *before* a real-world investigation target comes forward during the heat of a high-stakes investigation demanding to see investigation documents.

When an actual investigation launches, draft notes, interview transcripts and other documents aware that the target and witnesses might get access later. One strategy is to omit all names and identifiers; a fully anonymized investigation file without any "information relating to" any person "who can be identified, directly or indirectly" is not subject to data protection laws—in the EU, full anonymization completely sidesteps GDPR.[29] In practice, though, omitting all names and identifiers from a detailed investigation file will not be practical (using code names or numbers is not enough, because those are "indirect identifiers"). But in some cases it may be possible to draft certain documents, even a confidential final investigation summary report, without naming or "indirectly" identifying anyone.

All this said, though, check applicable data law. Fortunately, not all comprehensive data protection laws are as strict as EU GDPR in the investigatory context. The British Columbia Personal Information Protection Act, for example, offers a helpful investigatory exception relaxing certain obligations to collect employee consents to process data during internal investigations.[30]

6. **Disclose Investigation Procedures:** If the organization has any standing bodies of labor representatives overseas, consider informing or consulting with them about a high-level set of investigatory practices. This suggestion may seem counter-intuitive, because American organizations are reluctant to lock themselves into a rigid protocol or framework setting out how they will conduct all their internal investigations, and are even more reluctant to publicize that protocol to rank-and-file employees. Investigators need flexibility—every investigation is different, no one can predict an investigation's twists and turns, and a blueprint showing how an organization will conduct internal investigations might fall into the wrong hands and help a wrongdoer stay a step ahead of investigators. From an American point of view, issuing and communicating a detailed internal investigation protocol probably does not make much sense.

   But in the international context, this can play out differently. Labor laws in Europe and elsewhere might require disclosing ("informing") in-house investigatory frameworks to employee representatives like union committees, "works councils" and "staff delegates," as well as to health and safety committees empowered to consult over investigations into industrial accidents. Or, at least, militant overseas labor representatives have *argued*

29 *Cf.* EU GDPR art. 4(1).

30 British Columbia Personal Information Protection Act sec. 12(1)(c).

that their labor laws require disclosing or consulting over investigatory procedures. The labor representatives might claim the employer cannot launch a high-profile workplace investigation without having first collectively bargained or consulted over the process. Separately, in-house Data Privacy Officers may also ask for an internal investigation protocol.

An employer that "bites the bullet" and discloses to staff representatives at least a skeletal investigatory-practices outline might actually free itself up to conduct broader internal investigations later, with less interference from labor representatives. When an allegation or suspicion of wrongdoing arises later, the organization might then just go ahead and investigate. If militant employee representatives start asking obstreperous questions or making troublesome demands about the investigation, the employer can point out that its investigatory practices are "good to go" in this workplace, already consulted over, agreed-to or bargained to impasse.

Stage 2: Respond Initially to a Suspicion or Allegation Arising Abroad

Having taken pre-investigatory steps paving the way for international investigations, a multinational is ready to investigate a specific allegation or suspicion of wrongdoing that arises at, or reaches into, its operations overseas. Before interrogating overseas staff, take necessary pre-interview steps in ways that comply with applicable law. Assess the scope of the investigation. Mobilize an investigation team. Nail down a cross-border investigating strategy. Collect up the relevant documents and evidence.

7. **Assess Whether a Full Investigation Is Appropriate:** Some employee-facing whistleblower hotline communications claim the employer investigates "all" complaints received, and some companies claim they "always" investigate allegations of wrongdoing that come in. Do not believe this. In the real world, lots of reports come in that do not merit investigating. Some are insufficient. Some are misdirected. Some would lead to investigations that would be either futile or cause more problems than they resolve. Before jumping in and launching an international investigation, verify an investigation even makes sense.

   On one end of the spectrum are insufficient allegations impossible to investigate appropriately. For example, some complaints are too vague to follow up on, like a denunciation from an anonymous whistleblower who refuses to self-identify and who fails to identify the target or anyone else involved. Some complaints are obviously groundless, like fantastical allegations from psychologically unstable serial complainers and strategic charges by ex-employees already pursuing aggressive litigation in court. Some would-be allegations, even if true, merely amount to questionable judgment or rude behavior, or else are either impossible to fix or are susceptible to a quick resolution that does not require an investigation—examples include complaints about the parking situation, a broken toilet, a chronically-empty vending machine and complaints about loud, obnoxious and smelly co-workers. Also, never investigate a complaint that, even if legitimate, is a mischaracterized human resources matter best referred over to the HR team, like a complaint about compensation, workload, workspace, work hours and being passed over for promotion. Whistleblower hotlines at some organizations attract more HR gripes than allegations of wrongdoing appropriate for an investigation.

   At the other end of this spectrum is the problem scenario of the allegation that might be legitimate, but where an investigation is sure to fail or come up empty because even if investigators find evidence of wrongdoing, the organization will take no action—the decisionmaker will protect the target and bury or ignore an incriminating report. And there is the scenario where "the fix is in," and the investigators are either biased or under pressure to exonerate, and so an investigation would be a subterfuge or cover-up. Before launching an international investigation, verify it is legitimate and that upper management will support it, whatever the result.

8. **Appoint a Qualified Investigator or Investigation Team:** Employers often do streamlined investigations into low-stakes allegations with just a single investigator or two (maybe a supervisor or human resources professional and an outside expert or lawyer) checking some records and asking some questions. At the other extreme, a complex and high-stakes internal investigation can be an expensive, months- or years-long project mobilizing a team of internal executives, forensic experts, HR leaders and in-house counsel as well as company directors, outside lawyers, accountants, consultants, private investigators and translators.[31]

   Depending on the scope of a given cross-border investigation, either appoint a single investigator or assemble an investigatory team. Select an investigator or team leader competent in investigatory technique, familiar with applicable law, and experienced with how investigations in the jurisdictions at issue differ from domestic American investigations. Avoid the common mistake of appointing an all-star team of Americans expert in U.S. law, U.S. investigatory best practices, and U.S. criminal prosecutions but with little experience abroad and little understanding of host-country law. American investigators might focus so intently on the American issues that they may be blinded to compliance challenges under host-country employment, data and investigatory procedure laws.

   Often a U.S.-led international investigation purposely excludes ("screens") target-country locals from the investigation team because headquarters considers the locals inexperienced in internal investigations or susceptible to bias, prone to confidentiality leaks, or vulnerable to the influence of local management (maybe the local target himself). Where these are legitimate concerns, consider including on the investigation team at least one disinterested local *outsider* (say, a local consultant or outside lawyer) familiar with host-country culture, language and law.

   Verify that no one on the investigation team has a conflict of interests or might be a witness. Include on the investigation team someone expert in the subject of the allegation—say, an accountant in an embezzlement or FCPA accounting-provisions charge, an industrial safety expert in a workplace accident investigation, or a computer programmer in an inquiry into a data breach. Consider language fluency. Consider including an investigation team member from the internal audit function and an in-house or outside lawyer who can confer attorney-client privilege. As to outside lawyers, consider tapping investigatory counsel who is not the organization's regular advisory counsel and is therefore less likely to trigger a lawyer-as-witness conflict and be too close to interested local managers. And consider who is the lawyer's client: In the biggest investigations, different lawyers advise different affiliated parties—the headquarters company, local affiliates, the board of directors, the auditors, key executives. Also, consider local issues that affect who should be on the investigation team; for example, in France, often the company doctor actually needs to play a role (and yes, French employers have company doctors). Finally, think about who beyond the investigation team might need to become involved in the matter—for example, who will impose discipline and handle grievance procedures? Is the discipline-imposer best included on, or screened from, the investigation team?

   Be sure everyone on the investigation team has good investigation skills and is familiar with the legal and strategic issues in an investigation. A recommended practice, of course, is to have trained investigators in advance of the investigation.

9. **Impose Immediate Punishment, if Necessary, and Consider a Suspension:** Before taking any other step in an overseas investigation, first check whether local law imposes a *discipline deadline*. Ideally, of course, punishment

31 *See* Laura Brevetti, "Self Detection: So Key, So Difficult," *NY Law Journal*, July 13, 2009 at S2.

comes after the end of an internal investigation; to an American point of view, to "shoot first and ask questions later" would defeat the whole purpose of an investigation. The challenge is that overseas, employment laws can impose rigid discipline mandates that may not even occur to American investigators. Laws in some countries flatly require imposing punishment, including dismissal, quickly. Miss the short deadline and the wrongdoer goes unpunished, in that discipline or "for cause" dismissal after the deadline is too late and is illegal.

Foreign jurisdictions' discipline-deadline laws either do not foresee exhaustive internal investigations or else they actively try to legislate away the luxury of a thorough investigation. Jurisdictions like Austria impose tight deadlines of only days during which an employer can legally invoke evidence of misbehavior as good-cause support for a firing. In Belgium, an employee's dismissal for good cause "must occur within three working days from the moment the facts are known to the terminating party; the facts must be notified to the dismissed [employee] by registered mail within three working days from the date of dismissal."[32] France gives employers longer—a calendar month from the day the employer is "informed" of a wrongful act—to impose for-cause discipline.[33] In Iraq, an employer firing an employee for cause must notify the Iraqi Labour office within 24 hours of the time of the *incident*—not 24 hours after the end of an internal investigation—although perhaps the employer might be able to dismiss later.

It is easy to advise expediting all internal investigations to comply with these discipline-deadline mandates, but obviously that will not always be possible, especially where the deadline is short and the allegations complex. Rather, an American investigation team will want to take the position that the discipline-deadline "clock" starts only after its investigation is complete, but local law may not be so accommodating. How this plays out will depend on case law under the local discipline-deadline mandate and on the facts—how much evidence about the alleged infraction the employer got, and when. Paraphrasing the title of Richard Nixon counsel John Dean's Watergate memoir, the legal issue here is what the employer knew and when it knew it.

In a jurisdiction that imposes a short discipline deadline but where the employer cannot tolerate punishing a target until after its investigation concludes, develop a proactive and defensible position under local law that, in this situation, the discipline-deadline clock is somehow tolled (stopped) till the investigation winds up. And as a fall-back, check whether local law will allow a post-deadline *no-cause* dismissal, providing notice and paying severance pay.

Separately (regardless of whether a discipline-deadline mandate applies), at the outset of an internal investigation take any necessary *interim* discipline or personnel measures, like separating an accused harasser from the alleged victim and imposing a paid or unpaid suspension until the end of the investigation. But check whether local law regulates suspensions—and remember that suspended employees can become much less cooperative witnesses, even though a paid suspension is essentially extra vacation. Overseas, most suspensions during an investigation will have to be paid, and in some jurisdictions (England, for example), even a paid suspension may itself be a form of discipline that an employer must justify. Where an unpaid suspension is possible, consider whether it is legitimate or if it stays in place too long. In Canada, the Supreme Court once awarded CAN$485,100 in constructive dismissal damages to an executive put on an "indefinite suspension."[34]

32 Carl Bevernage, "Belgium" chap. 3 in INTERNATIONAL LABOR & EMPLOYMENT LAWS vol. IA (ABA/BNA 2017), at pg. 3-44.

33 French Labor Code art. L.124-10 *as interpreted by* French Ct.App. dec. no. 38634 of Apr. 3, 2014.

34 *Potter v. New Brunswick Legal Aid*, 2015 SCC 10 (CanL II) (Mar. 6, 2015).

10. **Define Investigation Scope and Draft an Investigation Plan:** An investigation without a well-defined scope takes unpredictable turns—remember the outrage at Ken Starr when his Whitewater land-deal investigation abruptly shifted to focus on Monica Lewinsky sex allegations.[35] Delineate the scope of an internal investigation at the outset, defining goals, setting boundaries and establishing the endpoint. Where corporate bylaws require a board of directors resolution to launch an investigation, that resolution should define investigatory parameters.

    In defining the scope of an overseas investigation, factor in the nature of the allegation and the logistical, linguistic and geographic barriers. In some European states, where a whistleblower allegation is anonymous, the fact of anonymity itself restricts the scope of an internal investigation—under EU GDPR and European employment law, an investigation target might argue an anonymous whistleblower denunciation is inherently less credible and so it offers less "probable cause" supporting a broad internal investigation leading to discipline.

    Some overseas investigators recommend drafting a detailed outline or plan setting out what the investigatory team will and will not do, consistent with the investigation's scope. According to an Australian law firm:

    > An investigation plan should be drawn up. Key witnesses should be identified, and persons potentially affected by the investigation should be listed. Practical details, such as location and order of witnesses, should be set out. An outline of the questions to be asked should be drawn up. The objective of the investigation should be noted."[36]

    But remember that, as already discussed, in the EU and other jurisdictions with comprehensive data protection laws, any document outlining the scope or plan of an investigation of an identified target is subject to a "data subject access request."

11. **Comply With Investigatory Procedure Laws:** We mentioned that under American law, a non-government employer's internal investigation is essentially a business or corporate governance matter unrelated to criminal procedure, because there is no "state action." *Upjohn* warnings and *Weingarten* rights aside, American domestic internal investigations (separate from discipline) are largely unregulated. But as mentioned, in jurisdictions in Eastern Europe and beyond, local criminal procedure laws can restrict and even prohibit a non-government employer or other private party from conducting an investigation. These laws are meant to prohibit private parties from intruding on the exclusive investigatory police power of law enforcers. Further, in jurisdictions that require private investigators be government-licensed, internal company investigators are vulnerable to a charge of illegally investigating without a license. And some countries' bar association rules limit or prohibit lawyers (even American lawyers not on the local bar) from conducting internal investigations, particularly if they need someone to administer an oath, such as for an affidavit.

    Before embarking on any internal investigation overseas, find out whether local procedural restrictions rein in private party or lawyer-led investigations. Adapt the investigation to conform. One strategy might be simply to characterize the internal investigation as mere "analysis," "checking," "verifying," "asking questions" or "internal compliance" that does not rise to the local-law threshold for a regulated "investigation." Also, in some contexts it might be possible to conduct a cross-border investigation from *outside* the territorial reach of local legal restrictions curtailing private investigations.

35 *Cf.* KEN GORMLEY, THE DEATH OF AMERICAN VIRTUE: CLINTON VS. STARR (2010) at pgs. 324-62.

36 Harmer's Work Insights (Australia), Winter 2012, at p. 11.

A related but separate issue (discussed below) is complying with local laws that regulate specific steps in an investigation, like regulations on searching employee emails/computers/internet history, searching lockers, desks and work spaces, conducting video surveillance and intercepting phone calls. Another related but separate issue (also discussed below) is complying with any local laws that require disclosing to local police evidence of a crime that an investigation might uncover.

12. **Research Applicable Rules and Substantive Law:** Some internal investigations merely look into alleged breach of an internal rule, some look into alleged breach of a law, and some look into allegations that, if true, would breach both an internal rule and a law. At the outset of any investigation, understand textual nuances of the applicable internal rules and laws that control—after all, the investigators' task is to uncover evidence of (or to exonerate a target accused of breaking) the applicable provisions of rules or law. And so, for example, in a bribery investigation, understand the applicable definition of "bribery." In a conflict of interest investigation, understand what constitutes a prohibited "conflict." When investigating alleged "harassment," check whether the applicable rule or law covers non-discriminatory bullying, or whether it prohibits only protected-group-motivated harassment.

    We mentioned that the employer should already have issued a clear code of conduct or other policies setting out its internal rules. So finding applicable internal rules should be easy. Of course, in an international investigation, be sure to check both applicable *global* policies and the overseas facility's *local* rules (which may not be in English). Then, research applicable laws. In international investigations, American investigators sometimes focus on American laws with "extraterritorial" reach—U.S. trade sanctions laws, the FCPA, the Alien Tort Claims Statute, and U.S. antitrust, securities and employment discrimination laws. Those laws are indeed important "applicable law" even abroad, but never overlook applicable *local* law. For example, a U.S. organization's international bribery investigation should account for the U.S. FCPA, maybe the UK Bribery Act 2010, and also host-country domestic bribery laws. In one situation, an "American businessman" found "guilty of taking nearly US$5.5 million in bribes as head of [a] Dubai-based company" was sentenced to 15 years in a UAE prison even as the U.S. government affirmatively sought to *defend* him.[37] In that particular international bribery case, the accused American apparently did not violate any U.S. law, but he obviously violated Emirati law. The point: Local law may be more relevant and more strict than applicable American law, as to an incident that happened overseas.

13. **Safeguard but Do Not Guarantee Confidentiality:** Confidentiality in internal investigations is vital for a number of reasons, including minimizing data privacy and defamation claims and avoiding human resources and public relations blow-back. But today's social media climate makes confidentiality hard to preserve. Further, companies' own promotion of whistleblowing (sponsoring hotlines and imposing strict rules against retaliation) might embolden some staff to feel entitled to divulge sensitive company data internally, and even to leak or whistle blow externally.

    Investigatory confidentiality can be a compliance issue because EU GDPR and other comprehensive data protection laws affirmatively require preserving confidentiality of identifiable complainants, whistleblowers, witnesses and targets who have not consented to being identified. Therefore, strictly confine investigation-uncovered information to company personnel with an actual need to know—the investigation team, retained experts, auditors, counsel, upper management, the board of directors. Resist temptations to inform too wide a circle as the investigation proceeds. Have any outside expert not bound by a privilege (e-discovery provider, forensic computer analyst, accountant, translator and the like) sign a non-disclosure agreement and data-law

37 "U.S. Businessman Gets 15 Years in Dubai Fraud Cases," *Miami Herald*, Mar. 25, 2013.

compliance warranty. Also, as already mentioned, transmit overseas-gathered investigation data back to U.S. headquarters confidentially, complying with data export rules. (Another confidentiality issue, discussed below, is instructing interviewed witnesses to keep investigatory interviews confidential.)

In the real world, maintaining confidentiality in an investigation is hard, particularly where the incident is the subject of workplace rumors, where circumstances point to a source, and where data protection laws grant "data subject access request" rights to investigatory files. If the investigated infraction is harassment, for example, disclosure of a complaining witness's identity is virtually inevitable. The recommended practice is never to *guarantee* whistleblowers or witnesses absolute confidentiality. (And as a matter of semantics, address this as a confidentiality issue without speaking in terms of preserving "anonymity"—as soon as just one person on the investigation team knows who a complainant is, anonymity no longer exists.)

14. Secure the Attorney/Client Privilege: We already mentioned the complexities of attorney/client privilege analysis in the context of a cross-border investigation. Before gathering documents and questioning witnesses, affirmatively stake out a strategy for how or whether the privilege will cover investigatory notes and files. A Canadian law firm once recommended, as to domestic investigations in Canada: "Give some thought…at the very beginning of the process, as to whether you wish the investigation process, report and surrounding communications to be privileged. It is much easier to attempt to set this up at the beginning of the [investigation] than mid-way through."[38]

    Where the investigation team has a lawyer who will assert attorney/client privilege, check how or whether relevant countries' laws offer the privilege, and to what extent. Does local law extend the privilege to in-house lawyers and to foreign lawyers like American counsel who are *not* members of the local bar? Account for lawyer-as-witness doctrines and any foreign law analogues to the U.S. domestic investigatory-context privilege and work-product doctrine.

    Think about who might later attack the privilege by demanding investigators' files, remembering that broad, American-style civil discovery does not exist overseas. If attacks on the privilege are most likely in American court litigation, then maybe *U.S.* privilege law is most relevant.[39] Outside broad civil discovery, attacks on attorney/client privilege may be most likely if there is either a "data subject access request" or a government enforcer "dawn raid." Stake out a privilege analysis for those contexts.

15. Account for U.S. Government Enforcement Issues: Most international internal investigations look into allegations that will never lead to inquiries, enforcement actions or criminal prosecutions by any U.S. government agency, be it the U.S. Department of Justice, the Internal Revenue Service, the Securities Exchange Commission, the Equal Employment Opportunity Commission or any other. But those international investigations that might involve U.S. government enforcement proceedings and prosecutions are particularly serious, and tend to be particularly complex. For those situations, craft an effective U.S. enforcement compliance strategy.

    Cross-border internal investigations involving U.S. government inquiries or possible U.S. criminal prosecutions raise *sui generis* U.S.-law administrative and criminal procedure issues such as, for example, U.S. government-context attorney/client privilege waiver, advancing defense fees, voluntary disclosures to government ("self-

38 Rubin Thomlinson LLP *Workplace Investigation Alert #14*, Aug. 2012.

39 *See Wultz, supra* note II (S.D.N.Y. 2013); E. Herrington & T. McCann, "Privilege Pitfalls: Companies Must Be Careful to Preserve Right During Internal Probes," *Corporate Counsel*, July 2014 at pg. 35; L. Krigten, "Waiver of Attorney-Client Privilege to Protect the Company" *Nat'l Law Journal*, Nov. 22, 2012 at 16; J. Nathanson, "Walking the Privilege Line," *NY Law Journal*, July 13, 2009, at S8.

reporting" and "suspicious activity reports"), "deferred prosecution" and "non-prosecution" agreements, parallel prosecutions and cross-jurisdictional prosecutorial cooperation. And a different cluster of specialized legal issues can emerge around international e-discovery and producing overseas documents in American-court litigation.

Whenever an international investigation triggers these issues, stake out a reasoned position that accounts for foreign laws, such as so-called "blocking statutes," EU GDPR, "state secret" laws, and criminal procedure mandates in overseas jurisdictions that might also prosecute. Certain formal U.S. government positions and memoranda on these topics have been criticized as inadequately accounting for the very real force of foreign law, and American prosecutors might be seen as failing to defer to inconsistent overseas legal mandates.[40]

16. **Impose an Enforceable Legal Hold:** Investigators will want to be sure staff in all affected jurisdictions retain relevant documents at least until investigators get copies. Further, "spoliation" claims (alleging improper destruction of documents relevant to litigation) are increasingly common in domestic American lawsuits, even though this issue remains rarely litigated abroad. A recommended practice is to require that employees in affected countries (particularly the identified key custodians of the relevant documents) preserve data possibly relevant to a cross-border investigation until the inquiry and any litigation wind up—maybe even until all statutes of limitations run.

    To effect this "preservation of evidence," multinationals often order staff, across borders, to suspend routine data destruction practices like automatic email deletion and routine compliance with company record-destruction policies. And multinationals' global information technology teams disable computer programs that routinely swab or erase old electronic business data. Software exists for implementing and enforcing these internal retention orders, often called "litigation holds" or "legal hold notices" or "LHNs." Companies sometimes bring in outside e-discovery providers to administer LHNs. This said, remember that issuing a broadly-communicated litigation hold or LHN all but announces to everyone that an investigation is underway, which raises a threshold confidentiality issue, and maybe even tips off targets inclined to cover their tracks.

    Outside the United States, legal holds can be vital, but they are less routine and, so, are less familiar. A multinational will have to explain its legal hold clearly in countries where local staff is unfamiliar with the practice. Outside of Europe, fortunately, these holds tend to raise few legal hurdles. However, under EU GDPR, and in some other jurisdictions with strict data protection laws and enforcement, an overbroad litigation hold kept in place too long butts into the data-law mandate to purge obsolete personal information including all copies—particularly where an employee or other "data subject" requests the purge as part of the "right to be forgotten."[41] In these jurisdictions, be sure to articulate a defensible business rationale for any long-term litigation hold: Articulate the multinational's specific GDPR article 5(1)(b) "legitimate purpos[e]" for retaining investigatory documents because they remain "necessary" under GDPR article 17(1)(b). Then, regularly review the need for the litigation hold, accounting for the fact that legal holds can be suspect in some contexts under GDPR—processing GDPR-regulated personal data for purposes of U.S. court litigation might even require a GDPR article 6(1)(f) derogation to balance data subjects' "fundamental rights and freedoms" with the litigant data controller's "legitimate interests."

40 *See* principles 3—7 in Sedona Conf., Int'l Principles, *supra* note 14, 19 SEDONA CONF. J. 557 (2018), at pgs. 606-21.

41 EU GDPR arts. 5(1)(b); 17.

17. **Collect Relevant Documents Legally:** In internal investigations, gathering up the relevant documents and information is usually the most important piece, apart from witness interviewing—and in some investigations, documents say a lot more than witnesses do. So the internal document-gathering step is vital. Collecting documents relevant to an investigation can require overcoming *technological* challenges, such as locating electronic files, crafting searches, recovering internet search histories, capturing metadata, retrieving ostensibly-deleted documents and text messages, and remotely accessing company devices in employee custody. While the technological challenges may be significant, within the United States, fortunately, investigatory document-gathering presents few *legal* challenges as long as the organization followed recommended practices and previously told staff both that the employer owns all company information and systems and that management reserves its right to access company data without notice—employees cannot reasonably expect privacy in company emails or documents. Issuing a notice to that effect is a strongly recommended practice in the United States.

    This plays out very differently abroad, especially under EU GDPR and other comprehensive data protection laws. In these jurisdictions, even if management has issued a statement explaining it owns the company systems and reserves a right to search them without further notice, data protection law might nevertheless restrict or even prohibit the organization from looking at ("processing") its own files, systems and security camera footage to conduct an investigation. The legal analysis here is that data law allows an organization to look at its own (personal) data only for "the specified, explicit and legitimate purposes" for which that organization had originally "collected" that data in the first place (GDPR art. 5(1)(b)). For example, a company that maintains an email system for the "specified, explicit and legitimate purpose" of fostering internal and external communications arguably cannot legally access ("process") its own email system for the very separate "purpose" of conducting an investigation that might get somebody fired. Separately, where an investigation looks into conduct that would constitute a "criminal…offenc[e]," GDPR is argued to curtail the employer's right to collect ("process") investigatory data.[42]

    In addition to this fundamental data-law analysis, some jurisdictions throw up other barriers specific to company investigators searching and reviewing employee text messages, emails, company documents, internet search histories and security camera footage. For example, some EU jurisdictions in effect decree that an employer may never read any employee email with the word "Personal" in the subject line, because those emails are presumptively not company-related and therefore inappropriate for the employer ever to see—even though savvy employees who understand this might easily misuse the "Personal" label to hide inappropriate communications. As another example, France prohibits management from accessing employee emails until the company goes to court and brings in a bailiff-like court officer to oversee the review process in real time. In Germany and elsewhere, collective labor law can be argued to require notifying employee representatives before the employer searches workers' emails and documents. And any company "Data Privacy Officer"[43] may have to be involved, and the DPO will inevitably argue that less employer access during the investigation is better. Further, unless the employer took careful preventive steps earlier, in Germany, Italy, Poland and some other European jurisdictions, the whole company email and intranet system might be deemed a "telecommunication" network regulated under "telecoms" law, and in that case the employer searching its own systems risks doing an illegal wiretap, akin to a telephone company listening in on its customers' private phone calls.

    These issues are not theoretical. They become hotly contested and high-profile whenever an employer in one of these jurisdictions is thought to be accessing employee emails, text messages and other company systems for an

42 EU GDPR art. 10.

43 EU GDPR arts. 37-39.

investigation. And these issues extend far beyond the EU. For example, in Alberta, Canada, an employer usually cannot read employee emails unless the employee has consented in advance to the search.[44] In a 2013 Chinese case, even though the employer's code of ethics had notified employees that emails on company servers were "company property rather than personal communication," and even though China had no broad data protection law, the Guangdong Foshan Intermediate People's Court held an employer's review of staff emails during an internal investigation illegal.[45]

In a cross-border investigation, think through all the legal issues before accessing internal documents. Then work up a defensible compliance strategy, and implement it. Complying with all the legal strictures here can be complex. Unfortunately, there is no easy advice to offer or "magic bullet," because the analysis is situation-specific and depends on many factors, including:

- the jurisdictions at issue
- the types of searches the employer wants to conduct (remote computer monitoring versus desk search, for example)
- how the company had set up its systems, and whether its systems trigger "telecoms" laws
- the content of the employee communications (notices) the organization has made about its systems
- whether affected employees have signed any consents relevant to employer access to investigatory data
- whether the searches will uncover personal data about customers, suppliers and other non-employee outsiders
- whether the searches will uncover any "sensitive" or criminal "offence" data[46]
- how the company's own employee representatives and Data Privacy Officer are likely to respond to the search

One tip is that when making mandated data-processing-system disclosures in the EU and other comprehensive-data-law jurisdictions, go on record declaring that one of the "specified, explicit and legitimate" and "necessary" "purposes" for all company communication systems—email, intranet, security cameras and the like—is, always, "internal investigations."[47] Being on record with this position facilitates gathering up documents in an investigation later. This is a preparatory step to take before launching an investigation.

18. **Conduct Surveillance Tactics Legally:** We have been addressing the standard scenario of investigators gathering up historical information—documents and evidence already generated in the past that relate to the allegation under investigation. A separate issue is the scenario of a more proactive investigation that generates its own investigatory documents, such as trying to catch a perpetrator in the act or making an admission. This might involve, for example, conducting video surveillance, live telephone monitoring or phone tapping, "tailing" a suspect, having an undercover investigator "wear a wire," administering a post-accident drug test, or administering a polygraph test (although polygraphs, illegal in the U.S. workplace, also seem to be extremely rare in internal investigations abroad).

44 *Moore's Industrial Svc. Ltd.*, Alberta Office of Info. & Privacy Comm'r order #P2013-07, Nov. 29, 2013, at ¶ 53.

45 A. Lauffs & J. Isaacs, "Court Dismisses Evidence Obtained from Employee's Work Email," Lexology, Oct. 23, 2013 (this said, Chinese court decisions on this point are unpredictable, and the China case law authority is inconsistent).

46 EU GDPR arts. 9-10.

47 EU GDPR arts. 5(1)(b), 6, 12.

Overseas, not surprisingly, any of these proactive surveillance tactics can trigger data protection laws, collective labor laws, general employment laws, as well as legal issues specific to the tactic—for example, wiretapping laws, private-investigator-licensing mandates and video-monitoring statutes (which, for example, are particularly complex under state and federal law in Australia). There is no easy advice here or "magic bullet," because the analysis is situation-specific as to the jurisdiction and the surveillance tactic at issue. Be sure to work up a compliance position.

Stage 3: Interview Witnesses Abroad

After taking preliminary investigatory steps and securing documents, the time comes to interview employee witnesses. Work out a strategic order for interviews, such as accuser-then-witnesses-then-target. Work up strategic outlines for the interviews, such as going from the general to the more specific, or such as early in the interview jumping into unexpectedly direct questions to elicit unplanned candid answers. In conducting each interview, factor in overseas cultural and strategic issues. During interviews, comply with local employment and data protection laws. Keep in mind legal issues that might emerge later relating to discipline and dismissal.

19. **Verify Sources and Try to Interview the Whistleblower:** The American mindset promotes anonymous whistleblowing to coax out allegations in the first place, but in parts of Europe and elsewhere, anonymous whistleblowing is suspect because of the fear that a vindictive employee might surreptitiously implicate enemies without standing accountable for bad-faith accusations. Regardless of which view is the better-reasoned position on anonymous whistleblowing in principle, when it comes time to investigate an actual allegation, being able to identify and interview a known whistleblower is always (yes, *always*) preferable to having to chase down the allegations of some unknown tipster. In Europe, investigations into a complaint from an identified whistleblower proceed more smoothly and enjoy more latitude under law than inquiries following up on anonymous denunciations. Therefore, before conducting interviews, if a communication channel to an anonymous whistleblower remains open—outsourced whistleblower hotlines actually offer this functionality—try to coax the whistleblower to self-identify and be interviewed, subject to an offer but not guarantee of strict confidentiality.

    Usually it makes sense first to interview the whistleblower or complainant who kicked off the internal investigation, to get the fullest picture of what to investigate. Seek corroborating evidence and witnesses. When interacting with an identified whistleblower, check whether the accuser stands by the complaint—accusers in harassment scenarios and those who target a powerful boss, for example, might back down later. When addressing whistleblowers who want to keep their identity secret, remember not to guarantee confidentiality.

20. **Neutralize or "Demilitarize" Interrogations:** Sometimes an American interrogating a foreign employee conveys an air of professionalism and authority that, overseas, may prove counterproductive and culturally inappropriate. As mentioned, as a matter of employment law, employees overseas may not have to cooperate in an investigation. That means aggressive questioning might make a witness "clam up." Therefore, consider neutralizing the international interrogation process by "demilitarizing" witness interviews, coaxing out better information using a softer touch. For example, while an internal investigator's background as a former U.S. prosecutor may enhance investigatory credibility stateside, overseas that background might be off-putting—foreign witnesses actually have alleged harassment when questioned by someone introducing himself as an American ex-prosecutor and making intimidating statements about criminal penalties. American witnesses might respect prosecutorial authority, but abroad, downplaying an interviewer's prosecutorial credentials and criminal law expertise may more likely open up witnesses, and lower the chances of a collateral harassment allegation from the interview itself. In short,

former U.S. prosecutors who are so well qualified to conduct domestic American internal investigatory interviews can face special challenges when questioning witnesses in foreign contexts where U.S. law expertise is less relevant and witnesses are more wary of (and remote from) American criminal justice.

When questioning employees overseas, one strategy is to neutralize the *semantics* of the interrogation itself. Investigators might refer to the internal investigation and their interrogation as merely "some questions," "talks," a "conversation," "checking" or "verifying." They might refer to an allegation, suspicion, complaint or denunciation as merely an "issue" or "matter" or "question." Documentary evidence and proof might be mere "emails," "records," "papers" or "files." A witness statement might be "notes." Whistleblowers, informants, sources and witnesses might simply be "employees" or "colleagues" (any who are not on the payroll would be "business partners"). The target of an investigation might be "our colleague." And an investigator zeroing in on a confession might request a mere "confirmation," "affirmation" or "acknowledgement."

Under employment law outside the United States, management enjoys less leverage when interviewing staff, because many employees outside employment-at-will are not under a duty to cooperate. Rank-and-file workers refusing to cooperate in an internal investigation probably do not give the employer good cause for discipline or dismissal. They may in effect enjoy a right to remain silent. (Therefore, avoid falsely instructing overseas witnesses that they "must cooperate.")

When conducting staff interviews, be sensitive to local conceptions of privacy. Outside the United States, expect employees to believe they have some sort of right to remain silent, in particular a right to refuse to answer personal questions about their sex lives, hobbies, families, workplace friendships, and outside income, as well as a right to keep their personal notes, documents, emails and social media postings private. In overseas investigatory interviews, show sensitivity for this view—even if, to American investigators, it seems inconsistent with the bright line under American law between government police investigations versus private-party inquiries where there is no "state action."

21. Comply With Collective Labor Law: We mentioned that collective labor laws in some jurisdictions in effect require consulting with local employee representatives (union committees or works councils) before investigators launch a slate of staff interviews. American investigators who burst into an overseas workplace and start interviewing staff (even managers) without first having given local management a chance to confer with local labor representatives about the interviews can commit an unfair labor practice. Be sure to comply with any requirements here. As a practical matter, the easiest approach is for the investigators to ask the overseas office's local management-side labor liaison—the manager who bargains or consults with worker representatives on behalf of management—how local labor leaders would likely respond to on-site investigatory interviews conducted without having given a labor representative advance notice.

    A separate collective labor law issue in the investigatory context is foreign local *Weingarten* rights. In jurisdictions including the United States, to interrogate employee witnesses who may be implicated in allegations and subject to discipline without letting them bring in a representative can constitute an unfair labor practice. Be sure to respect mandatory interview-context representation rights. This said, "foreign *Weingarten* rights" are limited. In England, for example, while employees who make a "reasonable request" enjoy "a statutory right to be accompanied by a companion" to a *disciplinary hearing*, that right does not necessarily reach routine investigatory interviews.[48] In Australia and New Zealand, staff have a right to bring a "support person" into a meeting that might lead to discipline, but again, this right probably does not reach routine investigatory interviews.

48 ACAS *Code of Practice on Disciplinary and Grievance Procedures*, Mar. 2015 at ¶¶13, 15.

Going further, aggressive employees in Europe occasionally invoke article 6(3)(c) of the European Convention on Human Rights to argue they have a right to bring a *lawyer* to investigatory (particularly disciplinary) interviews. But actually that Convention only extends this right to defendants "charged with a criminal offence."

22. **Notify Targets and Witnesses of Their Rights, and Demand Confidentiality:** American police read criminal suspects their *Miranda* rights, but in the non-government workplace investigation context, an American employee witness enjoys no such rights. By contrast, as discussed, many other countries confer more robust procedural rights in workplace investigatory interviews. And so in the international context, investigatory interviewers need to understand witnesses' rights, and need to know which rights have to be expressly communicated to witnesses. One sweeping right in Europe is the right to be told precisely what your other investigatory rights are. We have seen that EU GDPR and comprehensive data laws elsewhere require telling targets and witnesses about internal investigation notes and files that identify them, and requires offering targets and witnesses "data subject access rights." Even in countries outside Europe where local law does not force internal investigators to brief witnesses on their rights, a local recommended practice may be to begin an investigatory interrogation by advising each witness of relevant due process protections under employment and data protection law.

    This relates to the "foreign *Upjohn* warnings" issue. A lawyer interviewing domestic American employee witnesses in an internal investigation should always give so-called *Upjohn* warnings telling staff witnesses that the investigator represents the employer and may be covered by confidentiality obligations and attorney-client privilege, and explaining that the employer might waive its privilege and offer interview information to third parties including law enforcement.[49] As U.S. domestic law, the *Upjohn* Supreme Court case does not extend into overseas workplaces, but giving modified *Upjohn*-style warnings tweaked to reflect local law is a recommended practice worldwide. Some investigators even recommend delivering foreign *Upjohn* warnings in writing, in the local language, acknowledged (signed) by the witness.

    Beyond *Upjohn*, investigators should instruct overseas employee witnesses to keep the interrogation and investigation strictly confidential, not discussing it with anyone. Indeed, to leave a foreign witness free to go off and chat about a pending internal investigation concerning a colleague could actually violate GDPR and other comprehensive data protection laws overseas.

    This said, to give a strict confidentiality instruction to investigatory witnesses may unnerve American investigators who have gotten gun-shy on this issue, because demanding employee confidentiality in domestic American investigatory interviews risks violating U.S. labor law (even where there is no union) as an impermissible restriction on "protected concerted activity."[50] While savvy American investigators have stopped demanding confidentiality of rank-and-file stateside investigatory witnesses, this practice is best confined to U.S. soil. The broad American "protected concerted activity" doctrine is all but unknown overseas, even in Canada and other common-law countries. For example, under law in Australia and New Zealand, "procedural fairness and natural justice" are said to compel investigatory context confidentiality instructions to protect the target and others involved. *Banner Health* appears to raise an issue of purely domestic American law. There may be no good reason to extend it abroad. Imposing a confidentiality mandate on overseas witnesses is strongly recommended.

    Otherwise, conduct overseas investigatory interviews legally, complying with local criminal procedure. As one example, in any interviews in an investigation where the suspected wrongdoing would constitute a crime, be

49 *See* R. Jossen & N. Steiner, "The Upjohn Pitfalls of Internal Investigations;" *NY Law Journal*, July 13, 2009, at S4.

50 *See Banner Health System*, 358 NLRB No. 93 (2012), *questioned by Canning v. NLRB*, case no. 12-1115 (D.C. Cir. 2013).

careful asking staff to summarize what they may have already told local police—some jurisdictions prohibit this line of questioning. As another example, when recording witness interviews, first give appropriate data notices and get written recording consents that comply with applicable data protection law.

Stage 4: Impose Discipline, Take Remedial Measures and Issue Communications *after* the International Investigation

Information gathering completed, after collecting documents and conducting investigatory interviews, the task becomes summarizing the investigation, making recommendations—and making decisions. Conceptually, the investigation ends when the investigators deliver a report or recommendations; subsequent decisions made and actions taken are *post-investigatory*. Often, investigators report in to a decisionmaker who was not part of the investigation, but who decides next steps going forward, such as how to memorialize the investigation findings, whether to impose discipline and whether to implement any remedial measures. Take those steps consistent with applicable employment and criminal procedure laws. Memorialize, preserve and report on investigation results consistent with applicable data protection laws.

23. **Involve the Audit Function and Comply with Accounting Rules:** Where an investigation uncovered financial impropriety, money losses or bribery/improper payments, tackle the accounting and financial-statement issues head-on. Involve the audit function. Comply with U.S. FCPA accounting (payment-disclosure-reporting) rules as well as Sarbanes-Oxley accounting mandates and applicable Generally Accepted Accounting Principles. Financial losses at an overseas affiliate reach the "bottom line" of a U.S. parent, so at a publicly traded multinational an overseas investigation might implicate U.S. securities mandates and auditing/accounting disclosures. Manage strategy with inside and outside auditors. Implement auditor/accountant recommendations.

24. **Report to Upper Management or the Board of Directors:** Limit the circle of who receives an investigatory report (whether oral or written) to those with a demonstrable need to know. Consider the pros and cons of delivering an oral versus a written report detailing investigation findings to upper management and the board of directors. Keep in mind data protection law restrictions on "exporting" a written investigation report, and remember that employee "data subjects" may have "access rights" to see any written report. Also, privilege analysis and discoverability in U.S. or other jurisdictions proceedings may weigh against a written report. In jurisdictions including Australia and New Zealand, some investigators actually draft two written reports, one expressly privileged and the other expressly not.

    Draft any written investigation report carefully, with findings of fact grounded in the evidence. Refrain from having the report declare anyone guilty of a crime—internal investigators are powerless to declare guilt in any criminal justice system, and some investigators believe the word "guilty" does not belong in an investigator's vocabulary. Determine whether the context supports, and whether upper management or the board of directors expect, that the report stick to the facts found, or whether it should offer recommendations as to discipline and other next steps.

25. **Account for Whistleblower Retaliation:** Protecting whistleblowers against retaliation has been a high-profile issue in the United States for a couple of decades, and in recent years has drawn a sharp focus globally (overseas, retaliation is sometimes called "victimisation"). After an international internal investigation—before disciplining an employee who was the whistleblower—and before disciplining any target or witness who might plausibly claim to have lodged a workplace complaint as part of the underlying incident or the investigation that followed—consider whether an employee to be disciplined might allege whistleblower retaliation.

Assess the threat of a whistleblower retaliation claim carefully before imposing discipline, and take steps to minimize the threat. Because no organization concludes a good-faith internal investigation by deciding to punish the whistleblower for, in good faith, having pointed out the situation investigated, in the context of a good-faith internal investigation, retaliation claims emerge in unpredictable ways. That is, because employers acting in good faith do not commit whistleblower retaliation on purpose, after a legitimate internal investigation, any whistleblower retaliation claim asserted is likely to advance a creative or unpredictable theory. (There is an exception, one post-investigatory scenario obviously likely to spawn a retaliation claim—disciplining someone for having lodged a *bad faith* accusation against a co-worker.)

When assessing how a disciplined employee might be positioned to allege retaliation, account for the text of all applicable rules against whistleblower retaliation. Look at the multinational's own global and local policies—retaliation provisions in the code of conduct, hotline communications and local work rules. Research applicable laws against whistleblower retaliation, such as the anti-retaliation provisions in the incoming EU whistleblower directive.[51] Account for retaliation and reporting rules under any industry-specific retaliation or discipline-reporting regulations, such as in the U.S. and UK financial services sector. And consider the international reach of America's patchwork of tough anti-retaliation laws—U.S. state and federal whistleblower retaliation prohibitions are so aggressive that sometimes, overseas employees sue in U.S. courts to invoke them. That said, most court decisions construing the extraterritorial reach of these laws tend to confine the protections to U.S.-based staff.

Even where not disciplining would-be whistleblowers involved in an investigated incident, track retaliation scenarios *going forward*. Sometimes after the investigation is closed and the underlying incident all but forgotten, some involved employee who later gets denied a bonus, passed over for promotion or laid off in a reduction-in-force frames the adverse employment action as delayed covert retaliation for a previous whistleblower report.

26. **Impose Discipline Consistent with Procedural Mandates:** Where the investigation uncovered solid evidence of wrongdoing (and where the employer did not already take final disciplinary action at the beginning of the investigation because of a short discipline deadline requirement), the local affiliate employer entity—not the investigators and not headquarters—should impose discipline consistent with the investigation findings and with upper management or board of directors buy-in.

    If the investigation exposed sufficient evidence to dismiss the suspect for good cause under local law, then structure the dismissal as for good cause. Yet sometimes an investigation uncovers enough evidence of wrongdoing to convince the employer to dismiss the target, but not enough evidence to support a good-cause dismissal under the high employer burden of proof of local employment law. For example, a harassment investigation overseas might find the accused harasser did indeed commit harassment that violates the employer's policy, but under local law, the harassment that occurred might not amount to a "major breach of duty" subject to dismissal. In those situations, the employer (where legal and tolerable to management) might decide to dismiss the target *without* cause, paying notice and severance pay.

    In dismissing someone, follow local-law dismissal procedures. Chad, France, the Netherlands, the United Kingdom and many other countries require that an employer firing even demonstrably culpable staff follow detailed procedures that can involve written notices, grievance filing rights and internal appeals.[52] In the Netherlands, these procedures require getting a government agency or court permission to dismiss the employee.

51 EU dir. 2018/218, arts. 13-16.

52 *See,* e.g., ACAS Code of Practice on Disciplinary and Grievance Procedures, Mar. 2015 at ¶¶18-47.

Assess whether the disciplined employee might have a data-law claim arising out of the investigation itself. In the EU and other comprehensive data protection law jurisdictions, scrupulously having followed data protection law during the investigation pays off at the discipline stage, because disgruntled fired employees increasingly allege data law breaches along with their dismissal claims.

27. **Ensure Internal and External Communications about the Incident Comply:** With confidentiality paramount in internal investigations, a multinational usually would prefer to keep its investigation results under wraps. But in the real world, especially in high-profile incidents, internal and even external communications about an investigation can be inevitable. Trying to get by saying only "No Comment" will not always be feasible. Staff aware of the incident investigated (and aware that an investigation followed) may demand to know what happened, especially if
no one got fired and rumors are circulating. Confidentiality instructions notwithstanding, word about the incident and investigation could leak onto social media and over into traditional news sites. In one particularly high-profile American internal investigation in the academic sector, television stations around the United States actually interrupted their regular programming to report on the release of an employer's internal investigation report. For that matter, one of the biggest U.S. news stories of the decade was the press coverage around releasing Robert Mueller's report of his investigation into Donald Trump (granted, that was a government, not internal, investigation).

    Before issuing any employee communications or external statements about an incident of wrongdoing and the internal investigation that followed, a recommended practice is first to close the loop with the original whistleblower (where that channel remains open). Tell the whistleblower what the investigators found out and what the employer will do about it.

    Then, frame internal communications and external press communications about the incident and investigation carefully, using effective human resources and public relations strategies. Ensure that whatever is said is defensible. Avoid the word "guilty," because internal investigations do not assess criminal guilt or innocence. Heed EU GDPR and other applicable data-law restrictions on disclosing and exporting personal information. Be alert to defamation and tortious invasion of privacy claims.

28. **Disclose to Authorities Appropriately:** Where the investigation uncovered evidence of criminal acts, consider whether to turn that evidence over to local police or government authorities. Assess whether turning over criminal evidence to the government is mandatory, prohibited or optional.

    - *Mandatory:* Local law in some jurisdictions requires denouncing suspected criminals, including an employer's staff, to local authorities. Slovakia, for example, requires that parties including employers with knowledge of a criminal act notify authorities.[53] New South Wales, Australia requires parties, including employers with evidence about a "serious indictable offence," to report it to local police. China, too, mandates reporting information on crimes to police authorities. Some jurisdictions require turning over to police only evidence of certain crimes (child abuse and child pornography, for example). In some cases, reporting obligations are sector-specific; in England, for-cause dismissals in the financial services sector, even if not necessarily for indictable crimes, may have to be reported to authorities on "Form C" under the "FCA" and "RPA" handbooks. And of course where an investigation uncovers information that would be material to the investing public, securities laws require publicly-traded companies to make disclosures in securities filings.

53 Slovak Crim. Code no. 300/2006.

Heed any such reporting mandate, remembering that the mandate may kick in early, when an employer first gets evidence of a crime. Waiting until the end of an internal investigation may be too late.

- *Prohibited:* At the same time, other legal doctrines go in the opposite direction and can be argued to prohibit denunciations to government authorities, absent a court order. EU GDPR and comprehensive data protection laws in other jurisdictions might be argued to restrict an employer's freedom to volunteer, even to government law enforcers, personal information about "criminal…offences," if the denunciation does not occur under "the control of official authority."[54]

  Reporting to police could also raise challenges under employment law—fired staff in jurisdictions including France might actually argue that a police denunciation amounts to additional, excessive discipline. The theory is that where local employment law allows a for-cause dismissal for an illegal act, an employer would go too far if it were both to dismiss *and* to denounce the employee to authorities.

- *Optional:* Where reporting to police is optional (neither required nor prohibited), consider human resources and public relations fallout. Some denunciations to the authorities will very likely spark blow-back from co-workers and the public—for example, an employer turning in an employee for possessing marijuana or for working without legal immigration status.

29. Implement Appropriate Remedial Measures: Where an investigation reveals what might be a wider or recurring problem of systemic wrongdoing, consider doing a post-investigation internal audit—or even an *external* audit, bringing in an outside auditor—to assess the underlying problem that caused the incident. For example, where an investigation found embezzlement or bribery, consider a financial or accounting-practices audit. Where a workplace injury investigation found an unsafe condition, consider a workplace safety audit.

    Audit aside, consider implementing remedial measures—"fixes" to help prevent the problem from happening again. Considering tougher new work rules, new training, or adopting new tools for oversight, security, monitoring or surveillance. If, for example, a sex harassment investigation involved a novel scenario, consider discussing that scenario during harassment training going forward. If an investigation found an employee submitted fraudulent overtime pay records and expense reports, consider upgrading timekeeping and expense-reimbursement technology.

    In taking these measures, account for collective labor representation laws and vested/acquired rights concepts that restrict employers from unilaterally tightening terms and conditions of employment without consulting staff representatives or getting employee consent. Verify that any new surveillance tools comply with applicable law on data protection and employee monitoring. For example, before installing a new security camera, check whether employee notice or consent is necessary (as for example in Australia), and consider labor bargaining mandates (U.S. law, for example, can require bargaining with a union before installing a security camera[55]).

30. Preserve Investigation Data Appropriately: Preserve the investigation file—notes, interview transcripts, expert reports and summary report—consistent with applicable law and investigatory recommended practices. The recommended practice domestically in the United States is that the "details of every investigation…be memorialized in writing, regardless of the findings, including a description of the allegation, the steps taken to

54 EU GDPR art. 10.

55 *Cf. Brewers v. Anheuser-Busch*, 414 F.3d 36 (D.C. Cir. 2005).

investigate it, factual findings and legal conclusions, and any resultant disciplinary or remedial actions."[56] And of course the employer should *retain* that "writing," in case it is needed later. There are many good business reasons for retaining investigation records indefinitely. For example, even where an investigation finds no conclusive proof of wrongdoing, the file will become invaluable later if a similar allegation arises involving the same suspects. This said, there is one clear advantage to destroying *international* investigation files: As mentioned, in EU and other countries with comprehensive data protection laws, investigatory files are subject to "data subject access requests."[57] But an employer cannot provide access to what no longer exists.

The American practice of retaining investigation documents indefinitely is argued to be flatly illegal in Europe. Under EU GDPR, simply preserving an investigatory file can conflict with the data-law duty to purge obsolete personal information (including all copies, even the copy in the United States)—particularly where the target requests the purge as part of the "right to be forgotton."[58] Indeed, case law in Europe has invalidated local European laws that tried to mandate retaining certain documents for short periods to keep them available for police investigations; European courts invalidate those laws as violating the data-law duty to purge personal data promptly.[59] Sometimes an employer might be able to justify retaining an investigation file until relevant statutes of limitations run, but European GDPR enforcers—even a company's own in-house Data Privacy Officer[60]—may argue for destroying or completely anonymizing investigation files surprisingly soon after investigations end. Where the investigation did not lead to discipline, one influential (albeit outdated) EU recommendation calls for destroying the file just *two months* after the investigation closes.[61] Law on this issue differs from state to state within the EU. This said, the quick-mandatory-destruction-of-investigation-files issue seems largely confined to Europe; elsewhere, specific laws forcing the destruction of investigatory files tend to be rare. For example, Australia's Telecommunications Interception and Access Amendment Data Retention Act of 2015 requires *retaining* "metadata" relating to crimes, for law enforcement evidence purposes.

* * *

American recommended practices for how to investigate a suspicion or allegation of employee wrongdoing are well-developed, and so U.S.-headquartered multinationals setting out to investigate possible wrongdoing in their overseas operations tend to want to export their domestic U.S. investigatory practices. But doing that legally and appropriately requires flexibility, adaptation, compromise—and a lot of advance planning. Put in the work necessary to be positioned to conduct effective, legally-compliant and culturally appropriate internal investigations across worldwide operations.

56 S. Folsom, V. McKenney & P.F, Speice, "Preparing for a FCPA Investigation," ABA *International Law News*, Winter 2013 at p. 6.

57 EU GDPR art. 15.

58 EU GDPR arts. 5(1)(b); 17.

59 *Cf. Digital Rights Ireland v. Seitlinger,* EU Ct. Justice decision of Apr. 8, 2014; *Privacy First Foundation v. Netherlands*, Netherlands Dist. Ct., The Hague, Mar. 11, 2015.

60 EU GDPR articles 37-39.

61 Opinion 1/2006 at ¶ 4, EU Article 29 Working Party, 00195/06WP 117, Feb. 1, 2006.

At Littler, we understand that workplace issues can't wait. With access to more than 1,500 employment attorneys in over 80 offices around the world, our clients don't have to. We aim to go beyond best practices, creating solutions that help clients navigate a complex business world. What's distinct about our approach? With deep experience and resources that are local, everywhere, we are fully focused on your business. With a diverse team of the brightest minds, we foster a culture that celebrates original thinking. And with powerful proprietary technology, we disrupt the status quo—delivering groundbreaking innovation that prepares employers not just for what's happening today, but for what's likely to happen tomorrow. For over 75 years, our firm has harnessed these strengths to offer fresh perspectives on each matter we advise, litigate, mediate, and negotiate. Because at Littler, we're fueled by ingenuity and inspired by you.

For more information visit littler.com.

Littler®

Labour & Employment Law Solutions

06.19