

The background of the entire page is a deep blue with a complex, abstract pattern. It features numerous concentric circles and swirling lines, some of which are composed of small, light blue dots. The pattern is more pronounced in the upper half and fades slightly towards the bottom.

Vinson & Elkins

GOVERNMENT INVESTIGATIONS & WHITE COLLAR CRIMINAL DEFENSE REPORT

RECENT ENFORCEMENT TRENDS:
TECHNOLOGY SECTOR

TABLE OF CONTENTS

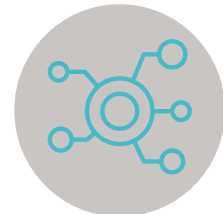
Introduction	2
Foreign Corrupt Practices Act: Government Enforcement Policies	4
Expanded Use of the FCPA Corporate Enforcement Policy	6
DOJ Moves Away From Yates Memo	8
DOJ Issues Anti-Piling-On Policy	9
DOJ Announces New Policy on Corporate Monitors	10
DOJ's China Initiative Could Trip Up Companies Doing Business in China.....	11
Foreign Corrupt Practices Act: Notable Enforcement Trends and Actions	12
FCPA Enforcement Trends	14
Notable Tech Sector FCPA Activity	15
Foreign Corrupt Practices Act: Notable Case Law	18
SEC Cannot Overcome Statute of Limitations in FCPA Case	20
Second Circuit Delineates the Reach of the FCPA.....	20
The DOJ Wins on Two Theories in FCPA Trial.....	21
Sanctions	22
Wire & Securities Fraud	26
Wire Fraud.....	28
Securities Fraud.....	29
Privacy	30
GDPR Enforcement is Underway	32
California Passes Comprehensive Privacy Law	33
Recent Lawsuits Filed Over Data Breaches.....	33
Cryptocurrency.....	34
Developments in Whether Crypto-Currencies are Securities.....	36
Anti-Money Laundering Developments	39
Website Liability.....	40
Changes Under SESTA/FOSTA.....	42
Internal Investigation Parameter Changes	44
Warrants & Subpoenas.....	48
New Legislation	50
Case Law	50
Looking Ahead	53
Conclusion	55

INTRODUCTION

Over the past year, the Technology Sector has faced a lot of developments in the government enforcement landscape. From settlements of bribery charges under the Foreign Corrupt Practices Act (“FCPA”) to the enactment of the European Union’s General Data Protection Regulation (“GDPR”) to the Securities and Exchange Commission’s (“SEC”) increased oversight of cryptocurrency and initial coin offerings, the Technology Sector faces a shifting environment of government inquiry and enforcement. With this report of recent enforcement trends, we are highlighting the key government enforcement policies and actions that Technology Sector professionals need to know.



Adopted in 2016, the **GDPR** was fully implemented in the European Union on May 25, 2018.



The SEC provided guidance on whether **crypto-currencies** operate as securities.

Diligence in preventing, identifying and handling violations is still prudent, particularly for technology firms doing business abroad. Companies with operations in China should be particularly attentive, as the Department of Justice (“DOJ”) has suggested that the region will receive greater scrutiny. But if violations emerge, companies are more likely than in the recent past to obtain friendly resolutions—if the matter is handled correctly. Reflecting new policies encouraging prosecution declinations for cooperating companies, in 2018, the DOJ seemed more inclined to resolve investigations with declinations or deferred prosecution agreements—although many of those resolutions involved a penalty paid to DOJ or a disgorgement of profits paid to the SEC. Consistent with DOJ guidance, individuals remain a target for prosecutors.

Technology companies are likely to see greater enforcement—and possibly new legislation—in the area of data privacy.

The GDPR went into effect in May 2018, and with it came a threat of enforcement of a suite of regulations that companies must adhere to or face significant penalties. California’s passage of similar legislation may inspire Congress to resume consideration of the myriad of federal data privacy and data breach statutes that have been proposed over the years.

The ongoing tension between law enforcement and the Technology Sector regarding the disclosure of third parties’ data is likely to continue. The courts are grappling with balancing new technologies against the protections afforded by statutes and the Constitution. That balancing act is likely to continue, foreclosing for now at least consistent guidance from the courts on the treatment of third party data in litigation and investigations.

We provide updates on these activities and more in this report.

PARTNER CONTACTS



MATTHEW JACOBS

Partner & Co-Chair of
Government Investigations
& White Collar Practice
San Francisco
+1.415.979.6990
mjacobs@velaw.com



WILLIAM LAWLER, III

Partner & Co-Chair of
Government Investigations
& White Collar Practice
Washington
+1.202.639.6676
wlawler@velaw.com



MICHAEL CHARLSON

Partner
San Francisco
+1.415.979.6910
mcharlson@velaw.com



MICHAEL DRY

Partner
Washington
+1.202.639.6525
mdry@velaw.com



JENNIFER FREEL

Counsel
Austin
+1.512.542.8538
jfreel@velaw.com



JESSICA HEIM

Partner
San Francisco
+1.415.295.5565
jheim@velaw.com



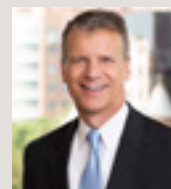
AMY RIELLA

Partner
Washington
+1.202.639.6760
ariella@velaw.com



CRAIG SEEBALD

Partner
Washington
+1.202.639.6585
cseebald@velaw.com



RON TENPAS

Partner
Washington
+1.202.639.6791
rtenpas@velaw.com

FOREIGN CORRUPT PRACTICES ACT: GOVERNMENT ENFORCEMENT POLICIES



Speeches and statements by senior DOJ officials regarding the FCPA reflect that the Department is setting a different enforcement tone: while still emphasizing that it seeks to hold wrongdoers accountable, the agency appears more sympathetic to the burdens that investigations place on companies.



WHAT YOU NEED TO KNOW

- The policies the DOJ announced this year reflect that cooperation and self-disclosure are likely to result in lenient results for companies.
- The DOJ has tightened the standard for imposing monitors on companies.
- To avoid “piling on” fines and penalties, the DOJ is requiring its attorneys to consider apportionment with other government authorities engaged in parallel investigations.
- Companies doing business in China should be wary of new scrutiny by the DOJ on possible FCPA violations.

EXPANDED USE OF THE FCPA CORPORATE ENFORCEMENT POLICY

BACKGROUND OF THE FCPA CORPORATE ENFORCEMENT POLICY

In 2016, the DOJ launched the [FCPA Pilot Program](#), a one-year program under which companies that voluntarily self-disclosed FCPA wrongdoing which the government did not already know about, cooperated fully with the subsequent investigation, and made full remediation for the wrongdoing, were eligible for significant reductions in the fines and penalties the DOJ could impose. In November 2017, in apparent recognition of the success of the Pilot Program, Deputy Attorney General Rod Rosenstein announced that the Pilot Program would be made permanent. Titled the FCPA Corporate Enforcement Policy (the “Policy”) and included in the Justice Manual,¹ the Policy added new incentives to encourage companies to self-report and cooperate:

1. A presumption that the DOJ would decline to prosecute the company, if the company a) self-reported, b) fully cooperated, and c) made timely and appropriate remediation;
2. If aggravating factors require that the DOJ bring an enforcement action, a company still would receive a 50% discount off the low-end of the U.S. Sentencing Guidelines range for fines and penalties if it self-reported, fully cooperated, and made timely and appropriate remediation.

EXPECTATIONS UNDER THE POLICY In an October 2018 speech, Principal Deputy Assistant Attorney General John Cronan [provided](#) guidance regarding the DOJ’s expectations for voluntary disclosure and cooperation under the Policy. For companies intending to self-disclose, “sooner rather than later” is the prevailing philosophy; companies “should not wait until after completing a significant internal investigation before coming forward.”

When companies do self-disclose, they should be prepared to provide certain information to the government. Mr. Cronan provided a useful checklist for companies of details they should have ready:

- Identities of the persons overseeing and undertaking the investigation, whether outside counsel, company employees, or other outside advisors like an accounting firm;
- Identity of who the investigative team reports to, whether an audit committee, management, the general counsel, or someone else;
- Whether anyone is walled off from the investigation and whether they are represented by counsel;
- The nature, scope and status of the investigation;
- Plans for the investigation, including the locations and conduct under scrutiny;
- Steps taken to preserve and collect potentially relevant evidence, including electronic documents and devices, and any obstacles with preservation efforts;
- Identities of individuals interviewed;
- Plans for future interviews; and
- Identities of individuals who know about the investigation.

Companies also must be prepared to explain how they intend to move forward, including offering a rational explanation for the company’s investigative plan.

Mr. Cronan emphasized that companies should promptly reach out to the government when they uncover key information in their investigation and should apprise the government if there is information the company cannot provide to the government, perhaps arising from privilege, data privacy, blocking statutes or other obstacles.

USE OF THE POLICY OUTSIDE OF TYPICAL FCPA CIRCUMSTANCES

FCPA cases in which the Policy likely applies most often involve allegations of a company and possibly its subsidiaries having been involved in bribery in foreign countries or having lax internal controls. In several speeches this year, however, DOJ senior officials announced that the principles articulated in the Policy would serve as guidance beyond the typical FCPA context.

In March, Mr. Cronan, then-Acting Assistant Attorney General, announced that the Policy would be “[non-binding](#) guidance” for all cases the DOJ’s Criminal Division brings, not just FCPA cases. The DOJ also plans to use the Policy as guidance for wrongdoing discovered before or soon after a merger or acquisition. In July, Deputy Assistant Attorney General Matthew Miner [announced](#) that successor companies in mergers or acquisitions will receive leniency under the Policy for disclosing FCPA wrongdoing discovered “in connection with” the transactions and cooperating with any follow-on investigations.

In September 2018, Mr. Miner [stated](#) that the Policy would serve as guidance for the DOJ’s approach to non-FCPA wrongdoing discovered as part of a merger or acquisition. For companies that discover wrongdoing after a merger or acquisition, Mr. Miner recommended following the steps outlined in the Policy, namely voluntarily disclosing the wrongdoing and fully cooperating with any follow-on investigation.

FCPA OPINION PROCEDURE For companies that unearth wrongdoing during due diligence prior to a merger or acquisition, Mr. Miner suggested using the DOJ’s [FCPA Opinion Procedure](#) (“Opinion Procedure”), which allows companies to obtain an opinion from the DOJ about whether actions the company intends to take comply with the DOJ’s current FCPA enforcement policy.

Under the Opinion Procedure, companies can submit a written request for an opinion from the DOJ about prospective conduct. After receiving all necessary information, the DOJ has 30 days to provide its opinion about whether the proposed activities comply with its FCPA enforcement policy. If the DOJ issues a written opinion that the activities comply with the enforcement policy, the company receives a rebuttable presumption in any subsequent enforcement action of compliance with the FCPA. To encourage use of the Opinion Procedure, Mr. Miner stated that the DOJ is able, “to a degree,” to expedite issuance of its analysis in light of acquisition and merger deadlines.

To be able to use the Opinion Procedure, companies should consider tailoring any non-disclosure agreements executed during pre-merger or acquisition due diligence to allow for limited disclosure of information suggesting wrongdoing.



V&E is named as one
of the world’s best
firms for international
investigations by
*Global Investigations
Review (GIR) 100*
(2015-2018)

DOJ MOVES AWAY FROM YATES MEMO

BACKGROUND OF THE YATES MEMO In 2015, then-Deputy Attorney General Sally Yates issued a memorandum titled [Individual Accountability for Corporate Wrongdoing](#) (“Yates Memo”), which outlined the DOJ’s focus on accountability for individuals culpable of wrongdoing. The Yates Memo required companies to disclose “all individuals involved in or responsible for” identified misconduct, regardless of position, status, or seniority. Companies that failed to comply would not receive any cooperation credit.

A NEW STANDARD FOR COOPERATION CREDIT

In November 2018, Deputy Attorney General Rod Rosenstein [announced](#) a step back from the all-or-nothing approach of the Yates Memo. Mr. Rosenstein said that individual culpability remains a top priority of the DOJ but explained that the requirement to identify “all” individuals that were involved could lead to delayed resolution of investigations and undue burdens on companies. The DOJ’s new policy focuses instead on individuals who were “substantially involved in or responsible for” the wrongdoing.

Notably, the policy differentiates between the standards that companies must meet in the criminal and civil contexts. For any cooperation credit in a criminal setting, the new policy requires companies to identify **all** individuals who were “substantially involved in or responsible for” the wrongdoing.

For credit in the civil setting, however, government attorneys have discretion to award full or partial credit depending on the nature of a company’s cooperation. To receive any credit, companies must identify all senior officials who meet the new standard of involvement in wrongdoing. To receive maximum credit, a company must identify all employees who meet the new standard of substantial involvement or responsibility.

As a practical matter (and as Mr. Rosenstein suggested in his remarks), this new standard may not mark much of a change from the DOJ’s actual implementation of the Yates Memo. According to Mr. Rosenstein, the DOJ was not strictly enforcing the standard set in the Yates Memo in either the civil or criminal context. The policy therefore may be mostly a way to bring the DOJ’s policy in line with the practice of its attorneys. The fact that the DOJ has not issued a formal memorandum with the new guidance nor revised relevant sections of the Justice Manual suggests that the DOJ may not see this change as a significant departure from the practices of its attorneys.

To effectively take advantage of the new policy, companies should establish with the government a metric for determining “substantial involvement” and “responsibility,” such as whether individuals had to actually partake in the wrongdoing to meet the standard or whether knowledge is sufficient to bring an individual within the scope of the government’s interest. An early determination of the standard of involvement may avoid complications or delays later in the investigation.

SEE V&E’S E-LERT
ON THE DOJ’S NEW POLICY:

*DOJ Announces Revised Policy
Reflecting Move Away From
Yates Memo*



DOJ ISSUES ANTI-PILING-ON POLICY

In a move that should provide some comfort for companies facing investigations by multiple government agencies, in May 2018 the DOJ announced a new [policy](#) regarding the treatment of penalties and fines in parallel investigations. The directive, which has come to be known as the “anti-piling-on” policy, recommends coordination with other government entities on penalties and fines when doing so would “allow the interests of justice to be fully vindicated.”

The new policy, which appears in [Section 1-12.100](#) of the Justice Manual, requires DOJ attorneys to coordinate internally to avoid duplicative fines and penalties. It also recommends that DOJ attorneys consult with other enforcement agencies, such as state, local, and foreign governments, who are engaged in parallel investigations to consider whether to coordinate the fines and penalties imposed on companies. Interestingly, the policy also

advises DOJ attorneys not to use the threat of criminal enforcement as a way to get companies to agree to civil or administrative penalties.

In determining whether and how to coordinate, DOJ attorneys have to consider several factors:

- the seriousness of the misconduct;
- statutory requirements for fines, penalties, and forfeitures;
- whether there is a risk of delay in reaching a final resolution; and
- the timeliness of a company’s disclosure and the nature of its cooperation.

When entering into negotiations with the DOJ or any other government entity, companies should use these factors to come prepared with arguments that the anti-piling-on policy applies.



V&E’s team is noted for its “extraordinary service and sophisticated understanding of various industries and government investigations.”

– *Legal500 USA: Dispute Resolution, Corporate Investigations and White-collar Criminal Defense 2018*



DOJ ANNOUNCES NEW POLICY ON CORPORATE MONITORS

In October, Assistant Attorney General Brian Benczkowski [announced](#) the DOJ's new [policy](#) for government-appointed monitors assigned to companies. The new policy provides a potentially heightened standard for imposing a monitor on a company.

BACKGROUND OF THE DOJ'S CORPORATE MONITOR POLICY

In the past, the government has imposed monitors on companies as a condition of non-prosecution agreements, deferred prosecution agreements, or plea agreements. The goal of a monitor is to have an outside individual (or team) that ensures company compliance with the terms of the agreements. Monitors, however, are imposed at the company's expense and can be burdensome to future operations.

Within the last decade, the DOJ has twice issued guidance on the issue of imposing corporate monitors, first in 2008 in what is known as the Morford Memorandum ("Morford Memo"), and again in 2009 in what is known as the Breuer Memorandum ("Breuer Memo").² The [Morford Memo](#), which this new DOJ policy supplements, requires federal prosecutors to consider the potential benefits to the corporation and the public from imposing a monitor as well as the costs and impact to the company that result from a monitor.

TOUGHER STANDARD FOR IMPOSING MONITORS

Coupled with Mr. Benczkowski's remarks, the new policy makes clear that the DOJ considers the imposition of monitors to be the exception, rather than the rule, a point Mr. Benczkowski made explicitly in his announcement. The policy itself also states that monitors "will not be necessary in many corporate criminal resolutions," especially where a company has demonstrated that its compliance program and internal controls are "effective and appropriately resourced at the time of resolution."

The new DOJ policy expands on what prosecutors must consider when weighing the benefits and costs of a monitor, requiring prosecutors to consider the following factors:

- Whether the wrongdoing involved the manipulation of a company's books and records or exploiting inadequate compliance programs and internal controls;
- Whether the wrongdoing was pervasive within the company, and especially whether senior management was involved;
- Whether companies have invested in and improved their compliance programs and internal controls; and
- If there are improvements to compliance programs and internal controls, whether the effectiveness of those programs and controls has been tested.

To best position themselves in the event of having to disclose wrongdoing, companies should regularly test their compliance programs and internal controls to ensure that they are effective. They should document the metrics they use for evaluating a successful compliance and controls program.

SEE V&E'S E-LERT ON THE DOJ'S NEW POLICY:



NEW TRAINING IN COMPLIANCE FOR DOJ

ATTORNEYS In his announcement, Mr. Benczkowski also explained that the DOJ intends to set up training for its federal prosecutors in how to assess the effectiveness of a company's compliance efforts. This training represents a move away from the DOJ's previous reliance on a single compliance expert who was tasked with counseling all prosecutors on the adequacy of companies' compliance programs. Assuming the DOJ follows through on the training, companies are likely to find prosecutors who are more fluent in the demands of compliance programs as well as the benefits possible from effective programs.

DOJ'S CHINA INITIATIVE COULD TRIP UP COMPANIES DOING BUSINESS IN CHINA

A new initiative by the DOJ to focus enforcement resources on China may expose companies doing business in China to additional FCPA scrutiny. In November, then-Attorney General Jeff Sessions [announced](#) a new focus by the DOJ on trade theft cases by Chinese nationals, on reviewing foreign investment in U.S. infrastructure and telecommunications, and on enforcement of the Foreign Agents Registration Act. Tucked away in the [fact sheet](#) for this China Initiative was the goal of "[i]dentify[ing] Foreign Corrupt Practices Act (FCPA) cases involving Chinese businesses that compete with American Businesses."

Although the language of the initiative is to police Chinese companies that use corruption to unfairly compete with American businesses, the FCPA generally only applies to companies that do business in the United States, trade on U.S. exchanges, or do something in the United States as part of their scheme to bribe a foreign official (like taking a foreign official on a trip in the United States). Companies that may be targets of the DOJ's new initiative are likely to have fairly close ties to the United States.

Given that industry players in China are often state-owned (and therefore considered government agents under the FCPA), there is already risk of bribery charges under the FCPA for companies that operate in China. Combined with the DOJ's new spotlight on corporate operations in China, 2019 could see more companies with ties to China being swept into FCPA investigations.

SEE V&E'S E-LERT ON THE CHINA INITIATIVE:



DOJ's Spotlight on China May Shed Light on More Than Intended



V&E Foreign Corrupt Practices Act Update, December 6, 2018

2018 has seen the United States and China trade a number of blows before a preliminary accord was reached between Presidents Donald Trump and Xi Jinping earlier this week. But time will tell if a ceasefire in the trade war will

FOREIGN CORRUPT PRACTICES ACT: NOTABLE ENFORCEMENT TRENDS AND ACTIONS



The DOJ and SEC FCPA Tech Sector investigations and enforcement actions underscore that friendly resolutions are possible when companies self-disclose and cooperate.³



WHAT YOU NEED TO KNOW

- Voluntary disclosure and cooperation is more likely to lead to a decision not to bring charges by the DOJ, the SEC, or both, even if companies have to pay fines, penalties, or disgorgement.
- Complacency can be problematic as a failure to voluntarily disclose or to have a robust compliance program and internal controls are more likely to lead to criminal charges, imposition of a corporate monitor, or both.
- Accountability for individuals remains a focus of the SEC and DOJ.

FCPA ENFORCEMENT TRENDS

In 2017 and 2018, the number of FCPA corporate enforcement actions decreased, with the 11 resolutions in 2017 and 15 resolutions in 2018, which is far below the Obama administration's peak in 2016 of 25 resolutions.⁴

Of the 16 corporate enforcement actions in 2018, the SEC resolved charges against companies in 14 of the cases. The DOJ, in contrast, imposed penalties pursuant to an agreement in only six of the cases. In two additional cases, the DOJ imposed "declinations with disgorgement" (the DOJ declined to prosecute but required the company to disgorge its profits from the misconduct) under the Corporate Enforcement Policy. The DOJ formally declined to bring charges pursuant to that Policy in two additional cases. For the remaining six cases, the DOJ did not offer any formal disclosure about its decision.

The 16 corporate enforcement actions in 2018, however, is still the third largest number of resolutions in a particular year over the last ten years, with 2016 (25 resolutions) and 2010 (21 resolutions) the only years to surpass that number. The early enforcement trends of the administration suggest that the FCPA is likely to remain an enforcement priority for the DOJ and the SEC.

The number of formal declinations by the DOJ pursuant to the Corporate Enforcement Policy has likewise remained steady.⁵ In 2016, the DOJ formally announced declinations in five cases pursuant to the Pilot Program, the predecessor to the Corporate Enforcement Policy. In 2017, there was a dip with only two formal declinations announced by the DOJ, but that number increased again in 2018 to four declinations. The number of formal declinations is likely to increase as the Corporate Enforcement Policy gains more traction with the Department.



NOTABLE TECH SECTOR FCPA ACTIVITY

The Tech Sector saw its share of FCPA enforcement actions in the past year, which is unsurprising as technology companies often operate overseas, either through manufacturing their products or by entering into foreign markets. Two of the 16 enforcement actions in 2018 involved tech sector companies, and the sector saw three declinations. As these actions reflect, compliance programs and internal controls remain important tools to avoid running afoul of the FCPA.

Below, we provide details of the enforcement actions against technology companies.

Corporate FCPA Enforcement Actions

DEFERRED PROSECUTION AGREEMENT AND CORPORATE MONITOR FOR PANASONIC AVIONICS CORPORATION

In April 2018, the DOJ [announced](#) that Panasonic Avionics Corporation (“PAC”), a subsidiary of in-flight entertainment and communication system designer Panasonic Corporation, entered [into a Deferred Prosecution Agreement](#) (“DPA”) to resolve charges that the subsidiary caused its parent company to falsify its books and records. The DOJ alleged that PAC retained the consultants, including one who simultaneously was working for a state-owned airline, who did little or no work for the company. According to the DOJ, PAC paid the consultants from a slush fund over which a single PAC executive had control. PAC also allegedly used third-party agents in Asia that had not cleared the company’s diligence process, a fact it purportedly concealed from the parent company.

PAC did not voluntarily disclose the wrongdoing to the government. Instead, the company began cooperating after receiving a request for documents from the SEC. The DOJ claimed that PAC’s remediation efforts were “untimely in certain respects” and noted that the company’s compliance efforts were “more recent” and had not been tested.

PAC received a DPA, which allows the government to bring charges if PAC fails to comply with any of the terms of its agreement with the government. Under the DPA, PAC agreed to pay a penalty of over \$137 million, to cooperate with the DOJ investigation, and to undertake a two-year corporate monitor to ensure future compliance. In parallel proceedings with the SEC, PAC agreed to pay an additional \$143 million in disgorgement.

Individual FCPA Enforcement Actions

FORMER PAC EXECUTIVES FACE SEC CHARGES

In December, the SEC announced resolutions with former PAC executives, the former [President and CEO](#) and the former [CFO](#), arising out of the same facts leading to PAC’s charges. The SEC alleged the executives violated provisions of federal securities laws and the FCPA that 1) prohibit individuals and companies from providing or causing false statements in books, records, or accounts and 2) that require companies to maintain internal controls that provide “reasonable assurances” that recorded transactions are accurate and compliant with management directives.

The SEC claimed that the CEO had a third party pay over \$1.76 million to consultants to assist PAC in getting business from a state-owned airline, and in the process, circumvented company policies for handling consultants, who performed minimal work. SEC claimed that the CFO had backdated an agreement with a state-owned airline to recognize revenue in an earlier quarter. The two employees will have to pay penalties of \$75,000 and \$50,000 under a deal with the SEC. The DOJ has not pursued charges against either executive or any other individuals involved in the PAC case. The executives neither admitted nor denied the SEC’s claims.

V&E's Government Investigations & White Collar Criminal Defense co-chair, **William Lawler III**, is nationally recognized in FCPA and in the D.C. area for Litigation: White-Collar Crime & Government Investigations.

– Chambers & Partners USA 2018

Declinations of FCPA Charges

POLYCOM, INC. REACHES DECLINATION WITH DISGORGEMENT DEAL WITH DOJ, SETTLEMENT WITH SEC

In late December 2018, the DOJ published a [letter](#) to Polycom, Inc. ("Polycom") stating that the Department was declining to pursue charges for possible FCPA violations pursuant to the Corporate Enforcement Policy. The DOJ required Polycom to disgorge nearly \$31 million in profits earned from the alleged misconduct, with the amount being split between the SEC, the U.S. Treasury Department, and the U.S. Postal Inspection Service Consumer Fraud Fund.

Polycom also settled with the SEC, which issued an [administrative order](#) detailing the settlement. Under the agreement, Polycom had to disgorge \$10,672,926 (incorporated into the DOJ's declination agreement), pay \$1,833,410 in prejudgment interest, and \$3.8 million in penalties. As noted in the DOJ's letter, the amount in disgorgement paid to the SEC was the amount of profits earned within the five-year FCPA statute of limitations.

In the administrative order, the SEC alleged that a vice president at Polycom's China subsidiary established a system by which the subsidiary would provide discounts to its distributors so that those distributors could provide payments to government officials. The SEC claimed that the payments to the government officials were for the purpose of influencing customers to buy Polycom's products. The China subsidiary allegedly maintained a separate set of books to record the discounts and payments to government officials. Polycom neither admitted nor denied the SEC's allegations.

The SEC charged Polycom with violating the FCPA's accounting provisions by falsely recording the discounts as legitimate expenses and with violating the internal controls provision by failing to have sufficient controls in place to detect the executive's actions.

Both the SEC and the DOJ noted Polycom's voluntarily disclosure, its cooperation with the investigations, and its remedial actions, including terminating and disciplining numerous employees, increasing compliance trainings, and improving the policies governing its relationships with third parties.

The resolution is notable for the fact that the DOJ required disgorgement in excess of the amount earned during the five-year statute of limitations. It appears that to deal with the Supreme Court's 2017 *Kokesh v. SEC* decision, which held that the SEC could only obtain disgorgement within the five-year limitations, Polycom paid to the SEC only the amount of profits made within that period. The nature of the resolution suggests that companies that want to take advantage of the Corporate Enforcement Policy may need to be prepared to pay full disgorgement or be willing to challenge the DOJ's requirements.

DOJ AND SEC DECLINES TO BRING CHARGES AGAINST TERADATA In February 2018, Ohio-based enterprise software company Teradata Corporation ("Teradata") [announced](#) in an SEC filing that both the SEC and the DOJ had decided not to bring FCPA charges involving "questionable expenditures" in Turkey by its international subsidiary. Teradata uncovered the travel, gift, and other expenses itself, conducted an internal investigation, and self-disclosed the investigation to the DOJ and SEC in February 2017. The company reported that it had "fully cooperated" with both agencies and had taken remedial actions, including terminating employees.

In January 2018, the SEC advised Teradata of its decision to close the matter without any enforcement action, and the DOJ told the company it was closing the matter without any enforcement action in February 2018.

DOJ DECLINES TO BRING CHARGES AGAINST JUNIPER NETWORKS In February 2018, the networking equipment company Juniper Networks [stated](#) in an SEC filing that the DOJ had closed its investigation into possible FCPA violations at the company and would not be bringing an enforcement action. Juniper reported that the DOJ's letter "acknowledged [its] cooperation in the investigation." According to the filing, the SEC is also conducting an investigation, and the SEC's investigation remains pending.

Ongoing Investigations

MICROSOFT FACES FCPA INVESTIGATION FOR ACTIVITIES IN HUNGARY In August 2018, the [Wall Street Journal](#) reported that both the DOJ and SEC are investigating allegations of potential bribery related to the sale of Microsoft products in Hungary. The Journal reported that the DOJ and SEC were investigating Microsoft's sale of software products to middleman firms at high discounts in 2013 and 2014, and whether those discounts were utilized to pay bribes or kickbacks to government officials. In its public filings, Microsoft has disclosed several FCPA investigations and past cooperation with enforcement authorities, including as recently as April 2017. To date, Microsoft has not reported any enforcement actions in connection with any of the reported investigations.

FOREIGN CORRUPT PRACTICES ACT: NOTABLE CASE LAW



As the DOJ and the SEC have pursued more FCPA cases in court against individuals, federal courts have weighed in with their interpretations of the jurisdictional and statute of limitations requirements under the FCPA. Traditionally, because the DOJ and the SEC often resolved FCPA charges through settlements, there was little case law interpreting the FCPA statute and even less case law discussing corporate obligations under the FCPA. These recent cases offer guidance from the courts about the scope of the FCPA's reach.



WHAT YOU NEED TO KNOW

- The SEC is likely to face tighter control by courts over FCPA cases that fall outside of the five-year statute of limitation.
- A conspiracy charge under the FCPA can only reach a foreign citizen who can be held directly liable under the FCPA either 1) as an agent or employee of an American entity or 2) for engaging in activity in the United States in furtherance of the misconduct.
- The DOJ can pursue alternative theories of FCPA violations to establish that it has jurisdiction over an individual.

SEC CANNOT OVERCOME STATUTE OF LIMITATIONS IN FCPA CASE

A July [decision](#) in *SEC v. Cohen, et al.*⁶ may be the start of the curtailment of the SEC's broad interpretation of its FCPA enforcement powers. Relying on the Supreme Court's 2017 *Kokesh v. SEC*⁷ decision, a district court in the Eastern District of New York held that the five-year statute of limitations barred the SEC from bringing FCPA and Investment Advisors Act claims.

The SEC filed a lawsuit under the FCPA and the Investment Advisors Act against two former employees of Och-Ziff Capital Management Group ("Och-Ziff") for a bribery scheme to direct African business toward Och-Ziff. In the suit, the SEC sought disgorgement and an injunction against future violations. The defendants moved to dismiss, arguing that the SEC's claims against them were barred by the statute of limitations.

The district court agreed with the defendants that the SEC's claims were barred by the five-year limitation under the *Kokesh* decision. In *Kokesh*, the Court held that the five-year statute of limitations applies to the SEC's disgorgement remedy because the disgorgement remedy served as a penalty, even if the SEC did not label it as such. Relying on that reasoning, the district court held that the SEC's disgorgement claims against the defendants, which arose out of conduct occurring before the five-year statute of limitations, were time barred.

In a possible further curtailment of the SEC's interpretation of its enforcement powers, the district court also held that the SEC's sought-after "obey the law" injunctions (i.e., requiring the defendants to obey all securities laws in the future) were also penalties that were subject to the five-year limitation.

The district court's decision is a departure from pre-*Kokesh* case law in which the SEC routinely pursued cases beyond the five-year statute of limitations on grounds that disgorgements and injunctions were not subject to the statute of limitations (or, indeed, any statute of limitations). The district court also acknowledged that its decision on the nature of the "obey the law" injunctions was in tension

with an Eighth Circuit decision, *SEC v. Collyard*,⁸ in which the Court of Appeals suggested that an injunction may never be a penalty subject to the five-year limitation.

Cohen and *Collyard* reflect the changing landscape for SEC enforcement after *Kokesh*. The next few years could see additional challenges by parties facing SEC enforcement and possibly changes in the types of FCPA cases the SEC decides to bring.

SECOND CIRCUIT DELINEATES THE REACH OF THE FCPA

In August 2018, in *United States v. Hoskins*,⁹ the Second Circuit [outlined](#) the boundaries of the FCPA's jurisdiction outside the United States against foreign nationals. The Court of Appeals held that a charge of conspiracy to violate the FCPA does not reach a foreign national who is not accused of taking any steps to further the scheme within the United States.

In 2013, the DOJ sought to charge Lawrence Hoskins, a British national and former Alstom UK executive, with conspiring to violate the FCPA for an alleged scheme to bribe Indonesian officials through payments to consultants for a \$118 million project to build power stations. In late 2015, the district court dismissed one count of Mr. Hoskins' indictment, finding that he could not be held liable solely for aiding and abetting or conspiring to violate the FCPA. The district court reasoned that the FCPA applied only to three categories of persons: 1) issuers of securities registered on national exchanges; 2) American companies, American persons, and their agents; and 3) foreign persons taking acts to further a corruption scheme in the United States, and that the defendant did not fall into any of the categories.

On appeal, the Second Circuit agreed that Mr. Hoskins had to fall within one of the three categories of direct liability to be liable for conspiracy to violate the FCPA. The Second Circuit held that the structure of the FCPA statute made clear that Congress did not intend to extend accomplice or conspiracy liability to persons that did not fall within the three explicit categories. Because Mr. Hoskins was never a U.S. citizen, national, or resident, and was never accused of committing

acts in furtherance of the alleged bribery scheme in the United States, he could only be charged as an agent of a domestic concern. The Second Circuit reversed the district court, however, to the extent that the district court's ruling did not allow for the DOJ to prove conspiracy on the theory that Mr. Hoskins was an agent of Alstom's U.S. subsidiary.

As the DOJ continues to pursue individual cases under the FCPA, it nevertheless may pursue this theory in other courts to test whether other circuit courts will have a different interpretation of the FCPA. In other words, *Hoskins* may be only the first word in a longer debate about the scope of the FCPA's jurisdiction.

THE DOJ WINS ON TWO THEORIES IN FCPA TRIAL

A district court in the Southern District of New York allowed the DOJ to go to trial against defendant Chi Ping "Patrick" Ho on two distinct but parallel theories of FCPA jurisdiction in the Southern District of New York: 1) that Dr. Ho was an agent of a domestic concern and 2) that he committed prohibited acts while in the United States.¹⁰ The DOJ alleged that at the time of two alleged bribery schemes in Chad and Uganda,

Mr. Ho was the head of and acting on behalf of an NGO that was based in part in Virginia, where it was registered as a Section 501(c)(3) organization. The DOJ also alleged that Dr. Ho participated in a conference in New York City, where introductions between eventual participants in the scheme took place.

In a motion to dismiss several of the charges against him, Dr. Ho argued that the structure of the FCPA did not permit him to be charged as both an agent of a domestic concern and as a foreign national who committed an act on U.S. soil. Dr. Ho asserted that if he qualified as an agent of a domestic concern, under the statute's language, he could not also be a foreign national committing an act on U.S. soil. The government argued that the FCPA did not preclude "agents" of domestic concerns from also being foreign nationals who committed acts on U.S. soil. The district court denied Dr.

Ho's motion and allowed the government to present both theories at trial. In December 2018, the jury convicted Dr. Ho under both theories.

Reflecting his intention to appeal the conviction, Dr. Ho asked the district court to enter a judgment of acquittal to preserve his arguments before the circuit court. The district court denied Dr. Ho's request.

If Dr. Ho follows through with his intention to appeal the conviction, the Second Circuit will have another opportunity to weigh in on the scope of the FCPA, specifically whether the DOJ can properly bring charges—and get convictions—based on theories that an individual is both an agent of a domestic entity and a foreign national acting on U.S. soil. In the meantime, the DOJ is likely to continue pursuing both theories against individuals to the extent possible.

SEE OUR BULLETIN

Jury Convicts on Both Bites at the Apple in FCPA Case



VIA: FCPA and Global Anti-Corruption Update, December 14, 2018

FCPA cases infrequently make it to trial. But, on December 5, 2018, a jury convicted Chi Ping "Patrick" Ho on seven counts related to his participation in bribery schemes involving officials of Chad and Uganda. Even more

SANCTIONS



In 2018, enforcement of sanctions prohibitions spilled into the headlines with a high profile export control action against ZTE Corporation and indictments against Huawei Technologies Co., Ltd. (“Huawei”) and its Chief Financial Officer, alleging they committed bank fraud and wire fraud to circumvent sanctions against Iran. The Tech Sector also saw several OFAC enforcement actions aimed at activities in countries against which the Treasury Department has imposed sanctions. Notably, OFAC’s annual enforcement volume decreased in 2018, with only seven enforcement actions being resolved—less than half the number resolved in 2017. Those seven enforcement actions resulted in the collection of over \$71 million in penalties and settlements, which is a decrease from the \$119 million collected in 2017 and significantly lower than the over \$1 billion collected in 2012 and 2014.¹¹



WHAT YOU NEED TO KNOW

- Voluntary disclosure and steps to remediate are key mitigating factors for OFAC resolutions.
- Failure to have compliance programs in place increases not only the risk of violating sanctions prohibitions but also the risk of a large penalty.
- China has been a focus of this administration, with the Department of Commerce and the DOJ taking actions against major Chinese companies ZTE and Huawei, respectively.

ZTE TEMPORARILY LOSES EXPORT PRIVILEGES AFTER ALLEGEDLY VIOLATING TERMS OF 2017 SANCTIONS SETTLEMENT

In April 2018, the U.S. Department of Commerce [announced](#) a denial of export privileges against Zhongxing Telecommunications Equipment Corporation of Shenzhen, China and ZTE Kangxun Telecommunications Ltd. of Hi-New Shenzhen, China (collectively, “ZTE”), and placed both companies on the Department of Commerce’s Bureau of Industry and Security’s Denied Persons List. In 2017, ZTE was subject to a combined civil and criminal penalty settlement and forfeiture totaling \$1.19 billion for violations of North Korea and Iran sanctions. OFAC [imposed](#) a \$100 million penalty on the company for the sanction violations. The settlement contained a seven-year suspended denial of export privileges that could be triggered if ZTE failed to comply with any of the terms of the agreement or committed additional sanction violations. In imposing the denial of export privileges, the Department of Commerce claimed that ZTE had made false statements during and after the settlement negotiations about having taken disciplinary actions against employees involved in the sanctions violations.

In May 2018, the Department of Commerce [restored](#) ZTE’s export privileges after ZTE agreed to pay a \$1 billion fine, place \$400 million in a U.S. bank escrow account, and be subject to a compliance team selected by the Bureau of Industry and Security (“BIS”), the Department of Commerce section that oversees export controls. Under the agreement, the compliance team will stay at ZTE for 10 years and report to BIS officials on ZTE’s conduct. Further, ZTE was required to replace its board of directors and executive leadership. The agreement also contained a provision that allows the Department of Commerce to activate a ten-year suspension in the event that ZTE violates any other sanctions.

The White House is currently considering an executive order that would prevent U.S. companies from using telecom equipment made by ZTE.

HUAWEI CFO ARRESTED IN CANADA FOR ALLEGED SANCTIONS VIOLATIONS

On December 1, 2018, Huawei Technologies Co., Ltd.’s (“Huawei”) Chief Financial Officer—daughter of the company’s founder—was arrested in Vancouver, Canada at the request of the United States. The DOJ has not publicly stated its reasons for requesting the arrest, but there are [reports](#) that the DOJ has been investigating Huawei for violating sanctions prohibiting

sales of telecom equipment to Iran and for misleading U.S. financial institutions as to the nature of transactions involving Iran. *The Wall Street Journal* [reported](#) that the bank HSBC had turned over information about suspicious transactions by Huawei to the prosecutors seeking the CFO’s extradition, suggesting that Huawei had used the bank to cover tracks of its sales in Iran.

In late January 2019, the DOJ unsealed its indictments against both Huawei and the CFO. The DOJ alleged that Huawei and the CFO had engaged in a years-long plan to deceive the company’s banking partners as to Huawei’s contact with Iran. The DOJ claimed that Huawei had an affiliate in Iran, known as Skycom, but that the CFO and the company misrepresented to banks that Skycom was a separate entity. The CFO is charged with bank and wire fraud; the company is charged with bank and wire fraud, conspiracy to commit both bank and wire fraud, violations of the International Emergency Economic Powers Act, and money laundering.

The CFO was released on \$10 million in bail and must remain in Vancouver pending the resolution of the U.S. extradition request. Her arrest has put U.S. and Canadian business men and women traveling to China on edge, especially after the Chinese government [detained](#) multiple Canadians after the arrest. The arrest came in the midst of trade negotiations between the U.S. and China, leading President Trump to state that he would be willing to intervene in the case if it would help him reach a deal with China. The White House is currently considering an executive order that would stop U.S. companies from using telecom equipment made by Huawei.

As we [detailed](#) in a recent post on the National Association of Corporate Directors BoardTalk blog, the CFO’s arrest provides insights into current enforcement trends:

1. The government is focusing on cross-border cooperation to detain parties that are the targets of investigations. As a result, avoiding the United States is likely to be insufficient to prevent U.S. government enforcement.
2. As its policies over the last few years have highlighted, the government remains focused on holding individuals accountable in the corporate context.
3. The CFO’s arrest combined with the DOJ’s China Initiative reflects that China increasingly is a target of the government’s enforcement efforts.

4. Individuals and companies can get swept up into the political activities of national governments.
5. Companies and their executives need to ensure that they know and are following the most current trade and sanctions laws.

COBHAM HOLDINGS, INC.'S SCREENING SOFTWARE MISSED NEW SANCTIONED ENTITIES, COMPANY SETTLED FOR \$87,507

OFAC [entered](#) a settlement with Cobham Holdings, Inc. (“Cobham”), a global provider of technology and services in aviation, electronics, communications, and defense. Cobham agreed, after voluntarily self-disclosing apparent violations, to pay \$87,507 on behalf of its former subsidiary, Aeroflex/Metelics, Inc. (“Metelics”), to settle its potential liability for three apparent violations of the Ukraine Related Sanctions Regulations. The three violations related to shipments of goods through distributors in Canada and Russia to an entity that was 51% owned by a company sanctioned under the Russian/Ukraine sanctions program.

Notably, Metelics had used screening software before engaging in the transactions to ensure that it was in compliance with sanctions requirements. The software, however, returned only exact matches rather than partial matches, thereby failing to alert Metelics of a sanctions issue.

In addition to the monetary fine, Cobham agreed to take several steps to minimize the risk of reoccurrence of similar conduct, including: using a new sanctions screening software that generates partial name matches; incorporating a new business intelligence tool that flags companies owned by sanctioned parties into Cobham’s due diligence process; and circulating a bulletin to its U.S.-based international trade compliance employees with a description of how the illegal sale occurred and an emphasis on compliance with sanctions laws.

ERICSSON'S VOLUNTARILY DISCLOSURE, REMEDIATIONS ALLOW FOR SANCTIONS SETTLEMENT OF \$145,893

Ericsson AB (“EAB”), headquartered in Sweden, and Ericsson, Inc. (“EUS”), headquartered in Texas, both of which are subsidiaries of Telefonaktiebolaget LM Ericsson (collectively “Ericsson”), [entered](#) into a settlement agreement to resolve possible violations of U.S. sanctions against Sudan. In reaching the \$145,893 figure, OFAC [noted](#) that Ericsson’s voluntary disclosure, “thorough internal investigation,” and adoption of “additional compliance

controls and procedures” served as mitigating factors.

According to OFAC, Ericsson violated sanctions against Sudan by having EUS, its United States subsidiary, indirectly aid a project that EAB, the Swedish subsidiary, was completing in Sudan. The apparent violations involved employees who conspired with employees of a third-party communications company in Lebanon to export and re-export a satellite hub and satellite-related services from the United States to Sudan. According to OFAC, an EUS employee initially stated that he could not help with the project because it involved Sudan, and Ericsson’s compliance department at one point warned the involved employees not to engage in the project. Nevertheless, the EUS and EAB employees purportedly continued the project and said the project was occurring in Bangladesh instead of Sudan to avoid detection by Ericsson’s compliance department.

In its announcement of the settlement, OFAC identified several aggravating circumstances, including the fact that the employees conspired to avoid the Sudan sanctions and ignored the company’s compliance department directives. Although OFAC determined the violation was “egregious,” it nevertheless allowed Ericsson in the settlement agreement to not admit that Ericsson engaged in the violation.

EPSILON ELECTRONICS, INC. AND OFAC SETTLE LITIGATION FOR \$1.5 MILLION

OFAC and Epsilon Electronics, Inc. (“Epsilon”) entered into a settlement following a 2017 D.C. Circuit decision¹² overturning in part OFAC’s penalties against Epsilon for sales of electronics to a Dubai distributor that regularly sold the products into Iran. As part of the agreement, Epsilon agreed to pay \$1,500,000 to settle OFAC’s allegations that the company had violated the Iranian Transactions and Sanctions Regulations. OFAC alleged that Epsilon sold audio and video equipment, valued at \$2,823,000, to a Dubai-based company, Asra International LLC, known to distribute most of its products to Iran.

In reaching the agreement, OFAC considered Epsilon’s failure to have a compliance program and its alleged “systematic pattern of conduct”—specifically 34 different shipments to the Dubai company—as aggravating factors. OFAC noted that Epsilon did not voluntarily disclose the alleged violations and provided only limited cooperation, namely by entering into an agreement to toll the statute of limitations. OFAC considered the tolling agreement as a mitigating factor, as well as the fact that Epsilon was a small business.

WIRE & SECURITIES FRAUD



A couple of high profile wire fraud cases against executives in the Tech Sector may provide insight into how the DOJ will use wire fraud to police companies' representations, especially when soliciting investments.

Social media has become an increasingly common outlet for tech company executives to issue messages about their companies and for companies to disclose material information that might affect their share price. The high profile settlement this year between Tesla, Elon Musk, and the SEC underscores the importance of controls over those accounts.



WHAT YOU NEED TO KNOW

- Companies should consider the representations made about products or services when building customer or investor bases.
- Companies should implement controls over social media accounts, including the personal accounts of executives, through which they announce material information.
- Failure to inform investors that social media platforms will be a method of disclosing material information will likely lead to SEC enforcement actions.

WIRE FRAUD

THERANOS CEO AND COO INDICTED

In June 2018, the DOJ indicted Elizabeth Holmes, CEO of Theranos, and Ramesh “Sunny” Balwani, Theranos’ former COO, on 11 counts of wire fraud and conspiracy to commit wire fraud.¹³ The indictment alleges that Ms. Holmes and Mr. Balwani made false and misleading statements while they were running Theranos as part of a scheme to defraud investors as well as doctors and patients.

The government has charged Ms. Holmes, who [founded](#) Theranos in 2003, and Mr. Balwani of misrepresenting the abilities of the company’s proprietary technology to investors. Theranos had to [retract or correct](#) tens of thousands of medical tests, and was sanctioned by the Centers for Medicare and Medicaid Services.

The indictments came after the SEC [settled](#) fraud charges with Theranos and Ms. Holmes, with Ms. Holmes agreeing to pay a \$500,000 penalty and be barred from servicing as an officer or director of a public company for 10 years. The DOJ cases are ongoing and pending in San Jose federal court; no trial dates have been set.

AUTONOMY EXECUTIVES CHARGED, CONVICTED

In April, a jury convicted Sushovan Hussain, the CFO of Autonomy Corporation (“Autonomy”), of 15 counts of wire fraud and one count of securities fraud. Autonomy was a UK software company acquired by Hewlett-Packard Co. (“HP”) in 2011 for approximately \$11 billion.¹⁴ The jury found that Mr. Hussain had defrauded HP by falsely inflating Autonomy’s revenue through various accounting mechanisms, such as backdating contracts, and making misleading statements about how much of Autonomy’s revenue came from hardware sales.

Following Mr. Hussain’s conviction, in November, the DOJ [indicted](#) Autonomy’s former CEO, Michael Lynch, and former Vice President of Finance, Stephen Chamberlain, with 14 counts of wire fraud and conspiracy to commit wire fraud.¹⁵ The indictments allege that Mr. Lynch and Mr. Chamberlain artificially increased reported sales to meet targets that secured them performance bonuses, and also portrayed Autonomy as a highly profitable business before the acquisition by HP.

In November 2012, HP wrote down \$8.8 billion of Autonomy’s value. In 2016, HP sold Autonomy to Micro Focus, a UK-based software company



SECURITIES FRAUD

ELON MUSK AND TESLA SETTLE WITH SEC

In September, the SEC reached an agreement with Mr. Musk and Tesla to resolve charges that Mr. Musk had engaged in securities fraud and that Tesla had failed to implement sufficient controls over public dissemination of material information. Mr. Musk and Tesla did not admit to the facts underlying the charges. They each agreed to pay \$20 million in penalties.

The agreement stemmed from a series of tweets from Mr. Musk in August 2018 communicating his intention to take Tesla private and implying that the only thing preventing that action was a shareholder vote. Mr. Musk subsequently [disclosed](#) that the discussions to take Tesla private were preliminary and subject to negotiation and due diligence. Two weeks later, Mr. Musk [stated](#) that Tesla would remain a public company.

The SEC alleged that Mr. Musk's statements were false and misleading because Mr. Musk purportedly had knowledge when he sent his tweets that there were no discussions for Tesla to go private at \$420 per share. The SEC pointed to

Tesla's stock price closing nearly 11% higher from the day prior to Mr. Musk's tweets and alleged that the disruption and confusion in the market injured Tesla investors.

In 2013, the SEC [clarified](#) that companies are allowed to use social media outlets to announce material information so long as investors are alerted beforehand about what platforms would be used to disseminate the information. Consistent with that guidance, in 2013 Tesla filed a form 8-K with the SEC stating that Mr. Musk's Twitter account would be an official channel for announcing material information to the public about Tesla's products and services. The SEC alleged in this case that Tesla had insufficient controls in place over Mr. Musk's account.

After Mr. Musk initially [rejected](#) an SEC deal, the Commission [filed](#) an action in federal court, and at the end of September, Mr. Musk and Tesla [settled](#) the SEC's charges. As part of the settlement, Mr. Musk had to step down as Chairman of Tesla's board, and his replacement had to be an independent director. Mr. Musk is ineligible to serve as Chairman for three years. Tesla must appoint two new independent directors to the board and establish a new committee of independent directors. Tesla must implement new controls and procedures to oversee Mr. Musk's social media posts and other communications.



V&E's Government Investigations & White Collar Criminal Defense co-chair, **Matthew Jacobs**, is recognized in California for Litigation: White-Collar Crime & Government Investigations and is held in high regard for his "extensive experience in the area of government investigations."

– Chambers & Partners USA 2017

PRIVACY



Privacy has moved front and center for the Tech Sector, with new laws providing more protections for personal data and with increasing government scrutiny over how companies are securing (or not securing) the data they collect. With enforcement of the European Union's ("EU") General Data Protection Regulation ("GDPR") beginning in 2018 and California passing its own version with enforcement set to take effect in 2020, companies are likely to face new government enforcement actions in the next few years.



WHAT YOU NEED TO KNOW

- The GDPR is in full effect, and with potentially high penalties, companies should ensure their policies and practices comply with the regulation. EU governments are already enforcing the regulation.
- The GDPR has broad jurisdictional reach and data processing activities of businesses with no assets or employees in the EU may still be subject to the GDPR if they are processing personal data of individuals based in the EU.
- California has passed a law that is similar in many respects to the GDPR, complete with a private right of action for consumers. Other states are beginning to legislate in this area too, particularly with respect to use of new kinds of personal data such as biometrics. Calls for a federal version of a comprehensive data privacy law that would preempt the California Consumer Privacy Act may come to fruition in 2019.
- State attorneys general and other local government agencies have undertaken enforcement actions against tech companies, alleging violations of consumer protection laws for purported failures to protect privacy.

GDPR ENFORCEMENT IS UNDERWAY

The GDPR, which went into effect in May 2018, beefs up data protections for personal data relating to individuals within the EU. Notable [requirements](#) under the new regulation include:

- Unless certain conditions apply, the ability to rely on an individual's consent to process their personal data is limited and, to the extent it can be used, must use clear, unambiguous language and be revocable;
- Requiring data processors to notify individuals regarding the processing of their data and their rights as data subjects (such as through notices and data protection policies);
- Upon request (and provided that certain conditions apply), providing individuals with a copy of personal data collected about them, free of charge;
- Not retaining data for longer than necessary and, upon request, and unless certain exceptions apply, erasing data collected about individuals;
- Implementing internal procedures and policies to protect data, such as putting in place appropriate physical and technological safeguards, appointing a data protection officer (which is mandatory for certain types of businesses and optional for others), creating data protection policies with training and audits, and performing data protection impact assessments for high-risk processing activities;
- Depending on the size of the company and the type of data collected, maintaining records of the processing of data;
- Reporting to government authorities and possibly to affected individuals within 72 hours breaches involving individuals' personal data that are "likely to result in a risk to the rights and freedoms of individuals;" and
- Restricting transfers of personal data outside of the EU and to third parties, unless certain requirements are satisfied and appropriate safeguards are in place.

Companies face significant potential penalties for failure to comply with these requirements. Under the GDPR, penalties can be up to €10 million (approximately \$11.36 million U.S. dollars) or 2% of annual revenue, whichever is greater, to €20 million (approximately \$22.7 million U.S. dollars) or

4% of annual revenue, whichever is greater. In determining a penalty, the government enforcement agency has to [consider](#) several factors:

- The nature of the infringement of the GDPR;
- Whether the infringement was intentional or negligent;
- Actions taken to mitigate the damage;
- A company's degree of responsibility for the infringement, in light of the requirements to implement technical and organizational measures to stay compliant;
- Relevant previous infringements;
- The degree of cooperation;
- The categories of personal data affected;
- Whether a company voluntarily disclosed the infringement;
- Compliance with any prior measures imposed on a company;
- Adherence to codes of conduct or certifications prescribed by the GDPR; and
- Any other mitigating or aggravating factors

Regulators have already started to enforce the GDPR's provisions. For example, the UK's Information Commissioner's Office ("ICO"), which is enforcing the GDPR's provisions in the UK, issued an [enforcement notice](#) on AggregatIQ Data Services ("AggregatIQ"), citing concerns about the company's use of "data analytics in political campaigning." According to the ICO, AggregatIQ received UK citizens' names and email addresses to target the citizens for campaign ads. The ICO alleged that AggregatIQ was not in compliance with the GDPR because the company purportedly had not alerted individuals that it possessed their data and had not "processed" the data in a way the individuals would have expected. The ICO required AggregatIQ to erase the personal data within thirty days or face penalties under the GDPR.

In other examples, Ireland's Data Protection Commission announced in December 2018 that it had opened "statutory inquiries" into [Facebook](#) and [Twitter](#) to investigate the two companies' compliance with the GDPR. The Commission claimed its receipt of breach notifications from both companies had led to the inquiries.

CALIFORNIA PASSES COMPREHENSIVE PRIVACY LAW

Companies with California customers will face challenges similar to those posed by the GDPR following the passage of the [California Consumer Privacy Act](#) ("CCPA"). The CCPA was passed in response to the Cambridge Analytica scandal and has several provisions that are similar to the GDPR. The CCPA is the first of its kind in the United States.

The CCPA protects only personal data of California residents but given the nature of commerce today, companies outside of California that do business with California residents will need to comply once the law goes into effect in 2020. In addition to the state attorney general's enforcement powers, consumers have a [private right of action](#) against companies that fail to implement reasonable security procedures and that result in a breach of personal data. Before filing suit, consumers must give companies an opportunity to cure the breach.

The CCPA has led to [an initiative](#) to pass a comprehensive federal privacy law that would preempt, and presumably be less stringent than, California's law. Given that enforcement of the CCPA will start once the California AG finishes its rulemaking (which must occur before July 2020, 2019 may see more movement on a federal law).


RECENT LAWSUITS FILED OVER DATA BREACHES

Although there is not yet a federal data privacy law, the Technology Sector can still face litigation under a variety of state law statutes. Recent litigation involving Uber and Facebook demonstrate the litigation risks for tech companies when they are faced with allegations of data breaches.

Uber recently resolved allegations involving a data breach that occurred in 2016. The company's disclosure of the breach led to investigations by state attorneys general and a subsequent lawsuit alleging that Uber had violated state law data breach notification requirements. In September 2018, Uber [settled](#) the litigation for \$148 million. According to its Chief Legal Officer, the settlement is part of an effort by the company to change its image and to "earn[] the trust of [its] customers."¹⁶

In April, Uber also [settled](#) with the Federal Trade Commission over the breach. Uber agreed to an expanded settlement with the FTC that requires Uber to provide the FTC with the results of all required audits of its privacy program.

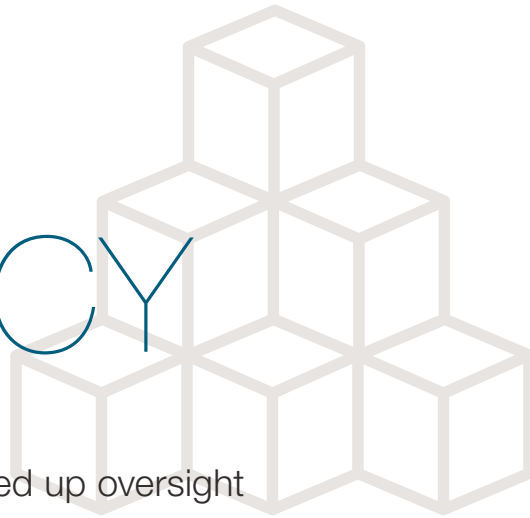
Facebook is facing civil enforcement lawsuits over allegations that the company had a data breach involving Cambridge Analytica. In March, the Cook County, Illinois district attorney [filed](#) a lawsuit against Facebook and Cambridge Analytica, alleging that both companies violated Illinois's Consumer Fraud and Deceptive Business Practices Act. Washington D.C.'s attorney general has also [filed](#) a lawsuit, similarly alleging that the company violated D.C.'s Consumer Protection Procedures Act.



"First of all, their quality of work is excellent. What I like about them is they have people with business backgrounds and they appreciate what the client is going through – what they're thinking. They just have a good business-orientation, rather than a strictly legal approach."

– Chambers & Partners USA, *Litigation: White Collar Crime & Government Investigations – California 2017*

CRYPTO CURRENCY



Federal regulators have recently stepped up oversight over cryptocurrency and initial coin offerings. Following its 2017 DAO Report of Investigation,¹⁷ in which the SEC outlined its theory of classifying cryptocurrencies as securities, the SEC has been engaged in enforcement that is modeled after the framework laid out in the report. And while the value of cryptocurrencies (as measured by market capitalization) plummeted,¹⁸ blockchain-enabled initial coin offerings (or “ICOs”)¹⁹ picked up steam in 2018.²⁰ 2019 promises increased regulatory oversight and enforcement as well as industry leaders learning to operate within the emerging regulatory framework as innovations in applications for blockchain technology continue.

WHAT YOU NEED TO KNOW

- The SEC and DOJ have taken the position that most cryptocurrencies offered in ICOs qualify as securities. While some companies and defendants have pushed back on the emerging regulations, the SEC has taken the position that most ICOs must be registered.
- Some of the industry's leaders, such as Coinbase, have announced changes to comply with government regulations.
- Governments are beginning to implement new anti-money laundering regulations and directives aimed at cryptocurrencies.

DEVELOPMENTS IN WHETHER CRYPTO-CURRENCIES ARE SECURITIES

As the DOJ and the SEC have stepped up enforcement against parties engaged in ICOs and cryptocurrency exchanges, a question that predominated is whether cryptocurrencies qualify as “securities” and therefore are subject to federal securities laws.

SEC OFFICIAL PROVIDES GUIDANCE

A June speech by William Hinman, the SEC’s Director of the Corporation Finance Division, offered insight into the SEC’s analysis of the issue. Mr. Hinman’s guidance echoes the SEC’s 2017 DAO Report of Investigation, in which it determined that virtual or crypto-currencies operate as securities (and fall under the securities laws) when they fall within the “investment contract” definition.

As explained by Mr. Hinman, cryptocurrencies are securities if they satisfy the Supreme Court’s “investment contract” test: does the cryptocurrency represent an “investment of money in a common enterprise with an expectation of profit derived from the efforts of others”? If so, the cryptocurrency is a security subject to SEC regulation; if not, it operates as something else. Mr. Hinman offered as an example of a cryptocurrency-as-security ICOs where the promoters offer the coins on the basis that they can develop new blockchain technology. In his example, the investor buys coins in the ICO in the hopes of turning a profit from the efforts of the company developing the blockchain technology.

As Mr. Hinman explained, this form of ICO is not unlike a more traditional IPO, where stocks are offered to raise money for a company. Mr. Hinman noted that Bitcoin, which is not connected to a third party’s efforts, likely would not fall within the definition of a security.

SEC AND DOJ RECEIVE MIXED RESULTS IN COURTS OVER DEFINING CRYPTOCURRENCIES AS SECURITIES

Two defendants challenged the SEC’s and the DOJ’s respective determinations that cryptocurrencies were securities, and the courts delivered mixed responses:

- In *United States v. Zaslavskiy*,²¹ the defendant argued in a motion to dismiss the indictment against him that the cryptocurrencies he sold in two ICOs were not “securities.” The district court denied his motion, finding that, regardless of the label, the coins he sold in the ICO were “investment opportunities” because he had claimed that the coins were backed by real estate and diamonds.
- In *SEC v. Blockvest, LLC, et al.*,²² however, the district court rejected the SEC’s bid for a temporary injunction to prevent Blockvest and its founder from pursuing an ICO. The district court held that the SEC had not established that Blockvest had provided tokens to third parties as investments; according to the court, the evidence showed only that Blockvest’s founder had allowed 32 people to test the Blockvest exchange without any intention of seeing returns on their tokens. The district court is currently considering the SEC’s motion for reconsideration.

SEC DINGS ETHERDELTA FOR FAILING TO REGISTER AS NATIONAL EXCHANGE

The SEC has nevertheless pursued settlements on the basis that cryptocurrencies qualify as securities. In an application of the “investment contract” test, in November, the SEC [announced](#) a settlement with EtherDelta—a platform for secondary market trading of blockchain-based ICO tokens—over charges that EtherDelta was operating as an unregistered securities exchange. The settlement for \$388,000 is the Commission’s first enforcement action against a crypto asset trading platform.

Citing the DAO Report of Investigation, the SEC claimed that the EtherDelta platform operated as a national exchange that required registration. The SEC [contended](#) that the tokens traded on the platform met the “investment contract” test because purchasers invested money in the tokens with the expectation that the tokens would go up in value based on the efforts of third parties who were managing the entities who had issued the tokens.

SEE V&E’S E-LERT
ON THIS TOPIC:

*A First in Crypto-Regulation:
SEC Settles Charges and Imposes
Civil Penalties*



SEC AND DOJ BRING CHARGES FOR FRAUDULENT, UNREGISTERED ICOS

Relying on their determination that cryptocurrencies qualify as securities, in 2018 both the SEC and the DOJ initiated enforcement actions against individuals and companies that attempted to raise money through ICOs this year. Notable examples include:

- **PARAGON COIN INC.** The SEC [settled](#) with Paragon Coin Inc. ("Paragon") for an ICO Paragon used to raise roughly \$12 million for its plan to implement blockchain technology in the cannabis industry. Under the settlement, Paragon agreed to pay \$250,000 in penalties, to compensate investors, to register its tokens as securities, and to file reports with the SEC for at least a year. Paragon did not have to admit or deny the SEC's findings.
- **CARRIEREQ INC. (AIRFOX)** The SEC also [resolved](#) charges against Airfox for its ICO, through which it raised approximately \$15 million in financing for its plan to develop a mobile application through which users in emerging markets could earn tokens and exchange them for data by engaging with advertisements. Like Paragon, Airfox agreed to pay \$250,000 in penalties, compensate its investors, register the tokens, and file reports with the SEC.
- **ARISEBANK** The SEC [settled](#) charges of securities fraud and selling unregistered securities against AriseBank's two founders, requiring them to pay \$2.7 million and agree to a lifetime ban of serving as officers or directors of public companies or from participating in digital securities offerings. According to the SEC, the founders falsely [claimed](#) that they had purchased an FDIC-insured bank and had an agreement with Visa to issue a Visa-branded credit card. The DOJ [indicted](#) one of the founders on wire fraud and securities fraud charges. The case is set for trial in the Northern District of Texas on February 4, 2019.

- **CENTRA TECH** Both the DOJ and the SEC charged the founders of Centra Tech, Inc. with defrauding investors in their ICO. According to the [DOJ](#) and the [SEC](#), the three founders falsely claimed that they had agreements with Visa, Mastercard, and Bancorp for a debit card that purportedly allowed cardholders to use digital currencies at any location that accepted a Visa or Mastercard credit card. The DOJ has charged all three founders with one count each of wire fraud and securities fraud and one count each of conspiracy to commit wire fraud and conspiracy to commit securities fraud. Their cases are pending in the Southern District of New York with trial set to start on October 15, 2019. The SEC has charged them in the Southern District of New York with securities fraud and failure to register their securities. That case has been stayed pending the resolution of the criminal case.

The indictments of the AriseBank and Centra Tech founders may result in additional challenges to the DOJ's (and thereby the SEC's) argument that the underlying cryptocurrencies qualify as securities.

Coinbase, which provides a platform for people to buy and sell cryptocurrencies, took a different tack this year. The company [opted](#) to seek approval from the SEC and the Financial Industry Regulatory Authority ("FINRA") to exchange security-type cryptocurrencies. In June, Coinbase acquired Keystone Capital Corp., Venovate Marketplace, Inc., and Digital Wealth LLC to obtain a broker-dealer license and eventually to get approval to list security tokens.

Given these divergent responses to the increase in government oversight, 2019 is likely to see additional development on where cryptocurrencies fall within the existing legal framework governing financial transactions.

ANTI-MONEY LAUNDERING DEVELOPMENTS

FINANCIAL ACTION TASK FORCE OFFERED NEW ANTI-MONEY LAUNDERING STANDARDS

In October, the Financial Action Task Force (“FATF”), an intergovernmental body that promotes the implementation of legal and regulatory measures to combat money laundering, [adopted](#) changes to its global anti-money laundering (“AML”) standards to address cryptocurrencies.

The changes target the “misuse of virtual assets” and include recommendations that the governments that are a party to the FATF: 1) ensure that cryptocurrency providers are licensed or registered, monitored by the government, and subject to anti-money laundering regulations including due diligence, reporting, and record keeping; and 2) assess and understand the risks associated with cryptocurrencies and identify effective systems to conduct risk-based monitoring or supervision of virtual asset service providers. If FATF’s recommendations are followed, the key features of cryptocurrencies, namely decentralization and lack of regulation, are likely to diminish.

EUROPEAN UNION’S AND UNITED STATES’ AML EFFORTS The FATF’s recommendations come in the wake of the Council of the European Union [adopting](#) its Sixth Directive on Combating Money Laundering by Criminal Law. In the new Directive, the Council noted that “[t]he use of virtual currencies presents new risks and challenges

from the perspective of combating money laundering” and advised that “Member States should ensure that those risks are addressed appropriately.”

2018 also saw the United States launch AML initiatives directed at cryptocurrencies:

- The President [established](#) a Task Force on Market Integrity and Consumer Fraud, which will “provide guidance for the investigation and prosecution of cases involving fraud ... with particular attention to fraud affecting the general public; digital currency fraud; money laundering ... and other financial crimes.”
- The Treasury Inspector General for Tax Administration [issued](#) a report recommending that the IRS work with its Bank Secrecy Act enforcement section, which helps enforce anti-money laundering statutes, to develop the IRS’s virtual currency policies.
- The House of Representatives [passed](#) the FinCEN Improvement Act of 2018 with bipartisan support, which would amend FinCEN’s anti-money laundering oversight authority to explicitly include cryptocurrencies. It is unclear whether the bill will pass the Senate, but FinCEN has already been using its existing authority to oversee cryptocurrencies.

As cryptocurrencies continue to gain a greater foothold in the global economy, there are likely to be additional regulatory efforts by the United States and other governments.



WEBSITE LIABILITY



Legislation this year has increased the uncertainty for website providers about their scope of civil and criminal liability for content that users post. In April, Congress passed the Stop Enabling Sex Traffickers Act (“SESTA”)/ Allow States and Victims to Fight Online Sex Trafficking Act (“FOSTA”),²³ which allows prosecutions and civil lawsuits against website providers that “promote” or “facilitate” sex-trafficking on their websites and, most controversially, removes a long-standing safe harbor for advertisements for prostitution on their websites.



WHAT YOU NEED TO KNOW

- SESTA/FOSTA establishes civil and criminal liability for website providers whose websites feature sex-trafficking advertisements.
- Criminal and civil enforcement under SESTA/FOSTA is likely to increase in 2019, as will challenges to the constitutionality of the law.

CHANGES UNDER SESTA/FOSTA

SESTA/FOSTA amends Section 230 of the Communications Decency Act, which provided immunity from civil litigation to website providers for the content that users published on their websites. SESTA/FOSTA peels back some of that immunity by allowing website providers to be sued civilly if content on their websites violates federal criminal statutes prohibiting sex-trafficking.

Other provisions of SESTA/FOSTA are equally unsettling for companies that host websites. For example:

- Website providers who intend to “promote or facilitate” the prostitution of another person can be criminally fined and imprisoned up to ten years and can be held civilly liable.
- The Act amends 18 U.S.C. § 1591, the federal criminal statute prohibiting sex-trafficking, so that website providers who “knowingly assist[], support[], or facilitate[e]” advertising for prostitution on their websites can be held criminally liable.
- State attorneys general may bring civil suits against website providers for violations of the newly amended federal criminal statutes regarding sex-trafficking.

Several organizations challenged the Act, arguing it was impermissibly vague and overbroad and unconstitutionally targeted speech based on viewpoint and content, but the D.C. district court [dismissed](#) the case on grounds that the organizations lacked standing to challenge the law.

The impetus for SESTA/FOSTA appears to have been Backpage.com, a website known for its prostitution advertisements. Backpage.com had relied on Section 230's safe harbor in lawsuits by alleged sex-trafficking victims. SESTA/FOSTA was Congress's attempt to close a perceived loophole in its legislation.

SESTA/FOSTA may have been unnecessary for the DOJ to seize Backpage.com and obtain a guilty plea from its co-founder and CEO. Although Section 230 immunized website providers from civil liability, it already provided no shield to criminal liability. As a result, Backpage.com's co-founder and CEO was [convicted](#) in the District of Arizona of conspiracy to facilitate prostitution and money laundering and will be sentenced in July 2019. The DOJ also [seized](#) and shut down Backpage.com

“I think they bring an enormous and in-depth knowledge of the subject matter and an ability to interpret it. They are very good at handling foreign clients whose first language is not English and require an interpretation of the judicial system. They are very good at handling those trans-Pacific relationships. It takes a really deft and good political hand to manage all those moving parts. They’re one of the firms that do that really well. They’re very successful and for good reason.”

– *Chambers & Partners USA, Litigation: White Collar Crime & Government Investigations - California 2017*

INTERNAL INVESTIGATION PARAMETER CHANGES



This year, developments in both the Supreme Court and in lower court cases suggest shifts in the landscape of internal investigations. From the (in)ability to recover the costs of an investigation from criminal defendants to new incentives for whistleblowers to go straight to the government and new scrutiny over government roles in internal investigations, companies are likely to need to update their internal investigation practices in the coming years.



WHAT YOU NEED TO KNOW

- The Supreme Court limited the ability of companies to recoup the costs of internal investigations under the Mandatory Victims Restitution Act of 1996 but kept open the question of whether restitution is available when the government requests the investigation.
- The Supreme Court also held that Dodd-Frank's whistleblower protections only apply to individuals who report violations directly to the SEC, and not to whistleblowers within a company.
- The government has faced court scrutiny over its role in company internal investigations and is likely in 2019 to face rulings about whether it is converting private actors into arms of the state, thus subjecting them to the same restrictions as government agents or prosecutors.
- The GDPR limits how personal data can be taken out of the EU, leading to possible barriers in internal investigations.

SUPREME COURT RULES CRIMINAL DEFENDANTS NOT RESPONSIBLE FOR COSTS OF INTERNAL INVESTIGATIONS

Companies can no longer obtain restitution from convicted criminals under the Mandatory Victims Restitution Act of 1996 (“MVRA”) for the costs of their independent investigations into criminal conduct.

In May 2018, the Supreme Court held in *Lagos v. United States*²⁴ that the MVRA did not entitle a company to recover the cost of its investigation conducted before turning over information to the government. In that case, the defendant pled guilty to wire fraud after using false documents to secure loans from General Electric Capital Corporation (“GE”). As part of his sentence, the defendant paid restitution to GE. The government argued that the MVRA required the restitution to include the costs of GE’s investigation of the matter, as well as GE’s costs from participating in the bankruptcy proceedings of the defendant’s company.

The Supreme Court unanimously disagreed, overruling the precedent of five Circuit courts and holding that the MVRA only requires the restitution of costs incurred by those participating in the government’s investigations and involvement in criminal prosecutions. As a result of the Court’s holding, companies that initiate their own internal investigations are not entitled to restitution from criminal defendants for those expenses. On the other hand, if companies incur expenses as part of their participation in government investigations, they may be able to recover those expenses under the MVRA. And, as the Court observed, companies can file civil litigation against defendants to recover their expenses.

Also interesting is an issue the Court did not address: whether the MVRA covers the costs of a private investigation conducted at the “government’s invitation or request.”²⁵

In response to the government’s argument that GE’s investigation costs should be reimbursed because it shared the product of its investigation with the government, the Court noted that GE incurred its investigation costs *prior* to coordinating with the government, placing those costs outside the statute’s coverage.

In light of the programs the government has adopted to encourage companies to voluntarily self-report wrongdoing, there is the possibility that companies could argue that participation in one of those programs acts as a government “invitation” to investigate, thereby falling within the MVRA.

Of course, as other cases this year have highlighted, close interaction with the government may give rise to an argument that a company has become a state actor. Until the Supreme Court returns to this question, companies will face a degree of uncertainty in these areas.

WHISTLEBLOWERS HAVE MORE INCENTIVE TO RUN TO THE SEC

There could be an increase in the number of whistleblower reports to the SEC under Dodd-Frank. In February, the Supreme Court held that Dodd-Frank’s anti-retaliation whistleblower protections only apply after a whistleblower reports a securities law violation directly to the SEC. *Digital Reality Trust v. Somers*²⁶ was about a whistleblower who was fired after internally reporting suspected violations. The whistleblower’s former employer ultimately prevailed in the Supreme Court, securing the suit’s dismissal on the grounds that Dodd-Frank does not protect a whistleblower who does not report the potential violation to the SEC.

This holding arguably gives an incentive to whistleblowers to bypass internal reporting procedures and go directly to the SEC with reports of suspected securities law violations. To help counter this incentive, companies should reevaluate and recirculate their whistleblower protection policies to emphasize to employees the protections they will receive by using internal reporting structures.

WHEN A PRIVATE COMPANY IS AN ARM OF THE STATE

The government faced scrutiny by courts this year about its role in internal investigations. As detailed elsewhere in this report, the government has increasingly incentivized companies with promises of leniency in exchange for full cooperation, including responding to government requests for information and witness interviews. Although the government sidestepped adverse rulings this year, these cases suggest that the rules of government involvement in private internal investigations may be about to change.

In the two cases, *United States v. Connolly*²⁷ and *United States v. Blumberg*,²⁸ defendants argued that the government’s role in their respective former employers’ internal investigations transformed the investigators into state actors, subjecting companies and their outside counsel to the same obligations that bind government prosecutors. In *Connolly*, the issue was whether statements made by one of the co-defendants to the internal investigators

under the threat of termination were effectively compelled by the government in violation of the Fifth Amendment. In *Blumberg*, the issue was whether the internal investigation team was required to produce any exculpatory documents in its possession, as would be required of a government prosecutor. In both cases, the government was able to avoid potentially adverse rulings by agreeing in *Connolly* not to call a witness to testify about the defendant's statements and in *Blumberg* by offering the defendant a fairly lenient plea agreement.

The district court continues to scrutinize the government's role in *Connolly*, tasking the government with differentiating its investigation from the company's in response to the defendant's argument that the government's entire case is tainted by his purportedly compelled statements. In the meantime, companies should keep records of their interactions with the government, including government requests, and should consider getting counsel for employees who are the targets of an investigation.

THE GDPR LIMITS ACCESS TO PERSONAL DATA IN THE EUROPEAN UNION The GDPR applies to internal investigations too, not just personal data collected as a part of regular business. The regulation's requirements for the lawful processing of EU individuals' personal data apply whenever such data is lawfully processed by private parties.

Chapter V of the GDPR governs when data can be transported outside the EU. Personal data may be transferred outside of the EU where (1) there is a determination by the European Commission that the country where the data is sent adequately ensures data protection measures are in place pursuant to [Article 45\(3\)](#); (2) the controller or processor seeking to transfer the data complies with a number of requirements for safeguarding the data pursuant to [Article 46](#); or (3) the transfer is subject to one of the derogations listed in [Article 49](#). Notably, Article 49(e) permits taking personal data out of the EU if necessary for establishing or defending a legal claim. According to the European Data Protection Board's Guidance on Article 49, this can include for the negotiated resolution of criminal fines.

Special note should also be paid to the strict limitations imposed by the GDPR on the collection of criminal history data, such as prior prosecutions or convictions, during investigations.

SEE V&E'S E-LERTS AND BULLETINS ON THIS TOPIC:



WARRANTS & SUBPOENAS



The pervasive use of various technologies, such as cell phones and email, has generated a tremendous amount of data about users, capturing their communications, locations, and much more. Law enforcement has collected and attempted to use such digital evidence in investigations and prosecutions. This year, statutory revisions and a new Supreme Court opinion have shifted the legal landscape governing law enforcement's ability to collect digital evidence.

WHAT YOU NEED TO KNOW

- New legislation requires companies to respond to law enforcement search warrants with data that is stored abroad.
- The Supreme Court determined that collection of an individual's cell phone records constitutes a search that requires a warrant under the Fourth Amendment.
- A magistrate judge in California held that the Fifth Amendment protects against law enforcement compelling individuals to use biometrics to unlock their phones.
- A D.C. appellate court held that the Stored Communications Act does not allow criminal defendants to subpoena social media companies.

NEW LEGISLATION

THE CLOUD ACT AMENDS THE STORED COMMUNICATIONS ACT TO APPLY TO RECORDS STORED ABROAD

This year, Congress enacted the Clarifying Lawful Overseas Use of Data Act (the “CLOUD Act”).²⁹ The CLOUD Act clarified that when the government obtains a warrant pursuant to the Stored Communications Act (“SCA”),³⁰ service providers must disclose the sought-after communications even if the communications are stored abroad.

Congress was responding to a case brought by Microsoft that had made its way to the Supreme Court.³¹ Law enforcement had applied for and received a warrant pursuant to the SCA requiring Microsoft to disclose records associated with a certain email account to the extent the information was within Microsoft’s “possession, custody, or control.” The email contents, however, were stored in Microsoft’s Dublin, Ireland, servers so Microsoft moved to quash the warrant. On appeal, the Second Circuit found that ordering Microsoft to disclose the sought information would be an unauthorized extraterritorial application of the SCA. The Supreme Court granted certiorari to decide whether Microsoft must disclose the communications stored abroad. Congress passed the CLOUD Act before the Court issued its decision, and with it, the Court found Microsoft’s case moot.

In addition to requiring companies to provide data that is stored abroad, the CLOUD Act creates a new structure for the transfer of data for law enforcement purposes between countries. The Act provides for the use of “executive agreements” between the U.S. and other countries to streamline requests for and access to communications data held by companies. Under the agreements proposed by the Act:

- Other countries can request communications data about non-U.S. citizens directly from companies without having to use the procedures in a mutual legal assistance treaty (“MLAT”);
- Other countries’ requests for communications data about U.S. citizens will continue to be processed under MLATs; and
- The U.S. and the other countries will lift any prohibitions on the export of communications data for law enforcement purposes obtained pursuant to the agreement.

To enter into an executive agreement with another country, the Attorney General and the Secretary of State must certify to Congress that the other country has sufficient protections for privacy and civil liberties, including protections to avoid the “acquisition, retention, and dissemination of information concerning United States persons.”³²

Companies faced with a request for communications data that is located in a foreign country still have the ability to move to quash the request. If the data is stored in a country with which the United States has entered into an executive agreement, companies have 14 days to move to quash and must show 1) that the person whose data is requested is not a U.S. person or resident, and 2) the disclosure “creates a material risk” that companies will violate the other country’s laws. If the data is stored in a country with which the United States has not entered into an agreement, courts must perform a “comity analysis” to determine whether to quash a request, namely balancing the interests of the foreign government and the United States.

So far, no countries have entered into an executive agreement with the United States, although the United Kingdom and the United States are [in negotiations](#). As the United States starts to enter into these agreements in the coming years, expect the CLOUD Act’s process to become more mainstream—and for challenges to its procedures to increase.

CASE LAW

OBTAINING CELL-SITE LOCATION INFORMATION CONSTITUTES A SEARCH UNDER THE FOURTH AMENDMENT

The Fourth Amendment protects against “unreasonable searches and seizures” without a warrant based upon probable cause. In *Carpenter v. United States*,³³ the Supreme Court determined that historical cell phone records and cell-site location information (“CSLI”) constitute an unreasonable “search” by the government that requires a warrant.

In *Carpenter*, the defendant allegedly robbed a series of Radio Shack and T-Mobile stores. Based on information from another participant in the robberies, the government applied for and received court orders under the SCA to obtain CSLI pertaining to the defendant from MetroPCS and Sprint. In response to the subpoena, the government acquired 12,898

location points over the approximately four-month period when the robberies occurred. The defendant moved to suppress the data, arguing it violated the Fourth Amendment because the government had obtained the records without a warrant supported by probable cause. The district court and circuit court rejected the defendant's argument.

The Court held that allowing government access to CSLI contravenes a reasonable expectation of privacy in the "whole of [the defendant's] physical movements."³⁴ CSLI contains a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."³⁵ This "retrospective quality" provides "access to a category of information otherwise unknowable," and affects nearly everyone.³⁶ Although users reveal such information to their wireless carriers, the Court found that cell phones are "indispensable to participation in modern society," and, as a consequence, "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a comprehensive dossier of his physical movements."³⁷ Accordingly, the government generally must obtain a warrant before acquiring CSLI.

Although the Court characterized its holding as a narrow one, it emphasized its role "to ensure that the 'progress of science' does not erode Fourth Amendment protections."³⁸ As technologies continue to improve, this ruling will be an important guide to courts evaluating access to digital evidence.

MAGISTRATE JUDGE RULES FIFTH AMENDMENT PROTECTS AGAINST COMPELLED USE OF BIOMETRICS

Relying in part on *Carpenter*, a magistrate judge in Oakland recently held that compelling people to use their fingerprints, facial recognition, or "any other biometric feature" to unlock electronic devices is a violation of the Fifth Amendment's protection against self-incrimination.³⁹ At issue in the case was a warrant application by the government to search the residence of two suspects in an extortion investigation. As part of the application, the government sought approval to compel "any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features."

The magistrate judge rejected the government's request on both Fourth Amendment and Fifth Amendment grounds. Analyzing the request under the Fourth Amendment, the

court found that the warrant failed to provide probable cause to compel "any individual" — rather than just the two targets of the investigation — to unlock electronic devices found in the residence.

Looking to the Fifth Amendment's protection against forcing individuals to provide self-incriminating testimony, the court went further to hold that even for the two suspects, for whom there was probable cause to search their electronic devices, compelling them to unlock those devices was unconstitutional. Noting that the Fifth Amendment protects against the government compelling self-incriminating testimony, the court held that the use of biometric features, like a thumbprint or facial recognition, is a "testimonial" act. The court reasoned that the act of unlocking an electronic device with a biometric confirms possession and control of the device. In other words, the biometric essentially "testifies" that the person has sufficient control over the device to have entered his or her biometric as a passcode and, therefore, has sufficient control over the contents of the device.

The court rejected the government's warrant application as drafted but permitted the government to submit a revised application consistent with its order.

SEE V&E'S E-LERT ON THIS TOPIC:

Fingerprints as Testimony



V&E Government Investigations Update, January 22, 2019

A magistrate judge in the Northern District of California recently held that compelling people to use their fingerprints, facial recognition, or "any other

COURT AGREES THAT SCA DOES NOT PERMIT FACEBOOK TO RESPOND TO CRIMINAL DEFENDANT'S SUBPOENA

In the fall of 2018, a criminal defendant asked the D.C. Superior Court to allow him to serve subpoenas on Facebook and a Facebook subsidiary to require them to produce records about Facebook account holders, including those holders' communications.⁴⁰ Facebook refused to comply with the subpoenas, arguing that Section 2702 of the SCA prohibited it from disclosing the requested information without the account holders' consent or another statutory exception. The trial court held Facebook in civil contempt for its failure, and Facebook filed an emergency appeal to the D.C. Court of Appeals.

The D.C. Court of Appeals reasoned that based on the SCA's plain language, structure, and legislative history, "the SCA prohibits providers from disclosing covered communications in response to criminal defendants' subpoenas." The Circuit Court found that Sections 2702 and 2703 (which control when the government can obtain communications) "appear to comprehensively address the circumstances in which providers may disclose covered communications," and neither section explicitly includes complying with criminal defendants' subpoenas. This decision, the Circuit Court noted, is also consistent with how other courts have treated civil subpoenas by private litigants under the SCA.

The appellate court rejected the defendant's argument that interpreting the SCA to bar Facebook from complying with his subpoenas infringes on his constitutional right to obtain evidence and present a complete defense. The Circuit Court explained that defendants can subpoena the account holders directly for their Facebook communications. That process, the Circuit Court reasoned, "increases the chances that affected individuals can assert claims of privilege or other rights of privacy" before their communications are produced, in part, because the affected individuals have a greater incentive than third parties to object to a subpoena.

NEW TECHNOLOGY DRIVES NEW COURT RULINGS

Courts continue to muddle through Fourth Amendment and privacy challenges to the use of data collected by new technologies. Here are just a few recent examples:

- **AMAZON ECHO** In a double-murder case pending before a New Hampshire state court, the government moved for an order allowing the search of audio recordings made by an Amazon Echo⁴¹ and information identifying cellular devices

linked to the Echo. After finding that the defendant lacked standing to object and that there was probable cause to believe that the sought-after information contained evidence of the alleged crimes, the court [granted](#) the government's motion to search the recordings in lieu of a search warrant and ordered Amazon to produce the information.

- **CELL-SITE SIMULATORS** A Florida appeals court [affirmed](#) a lower court order suppressing evidence that resulted from the warrantless use of a cell-site simulator called a Stingray to pinpoint a criminal defendant's location.⁴² Noting that "[t]echnological advancement often collides with the Fourth Amendment," and relying on the U.S. Supreme Court's decision in *Carpenter*, the court explained, "If a warrant is required for the government to obtain historical cell-site information voluntarily maintained in the possession of a third party, we can discern no reason why a warrant would not be required for the more invasive use of a cell-site simulator." The Florida Supreme Court's decision is just the latest in a [string](#) of courts requiring warrants for the use of cell-site simulators.
- **FACEBOOK MESSENGER** Facebook and federal prosecutors sparred over Facebook's refusal to comply with requests to wiretap voice calls made using Facebook's Messenger app. In response to a government motion to hold Facebook in contempt, the U.S. District Court for the Eastern District of California [reportedly](#) issued a sealed order in favor of Facebook. The ACLU and other organizations have [moved to unseal](#) the court records related to the motion to compel. This is a case to watch in the new year.

SEE V&E'S E-LERT ON THIS TOPIC:

Court Backs Facebook's Refusal to Comply with Criminal Defendant's Subpoena



LOOKING AHEAD



Looking ahead to 2019, the Supreme Court will decide two criminal procedure cases that are likely to have an impact on the tech sector when it faces state and federal enforcement actions.



WHAT YOU NEED TO KNOW

- This term, the Supreme Court is deciding two criminal procedure cases that are likely to have an impact on tech sector companies facing state and federal investigations.

States, in addition to the federal government, can use their enforcement powers to bring criminal and civil cases. But two cases on the Supreme Court's docket this year are likely to affect the scope of the states' enforcement powers.

WILL STATES BE ABLE TO PURSUE IDENTICAL CRIMINAL ACTIONS AS THE FEDERAL GOVERNMENT?

In *Gamble v. U.S.*, the Supreme Court is considering whether it should overrule the separate sovereigns exception to the Sixth Amendment's Double Jeopardy Clause. The separate sovereigns exception states that because the federal and state governments are "separate sovereigns," the Double Jeopardy Clause does not apply to prosecution of the same crime under both federal and state laws. If the justices decide not to overturn the separate sovereigns exception, companies will continue to be subject to both federal and state prosecution.

ARE STATES, LIKE THE FEDERAL GOVERNMENT, LIMITED IN HOW THEY FINE DEFENDANTS?

In *Timbs v. Indiana*, the Court is considering whether the Eighth Amendment's Excessive Fines Clause applies to the states. The excessive fines clause prohibits the federal government from imposing "excessive fines" on defendants. The issue before the Supreme Court is whether that clause applies to states as well. Amendments to the Constitution do not, on their face, apply to state governments. The Supreme Court has held in the past that the Fourteenth Amendment requires states to respect many, but not all, of the rights engendered in the Constitution. The Court will determine whether the excessive fines clause is one of those rights.

There is still ambiguity as to the scope of the Clause and how courts decide whether a particular fine is excessive or not. Companies and individuals should remain alert to use of the Clause in cases where state or federal law enforcement attempts to impose large penalties or fines.

On February 20, 2019, the Supreme Court issued its decision in Timbs, holding that the Excessive Fines clause applies to the states. V&E will have additional details about the case on its website.





CONCLUSION

As our report details, the Technology Sector is likely to face a shifting enforcement landscape. In particular, as the new legislation we describe in this report is enforced by state and federal law enforcement, there will be ongoing changes in the risks facing technology companies. As these enforcement trends develop, we will provide ongoing updates.

ENDNOTES

- ¹ In 2018, the DOJ [updated and renamed](#) the U.S. Attorneys Manual to the Justice Manual.
- ² The [Breuer Memo](#) provided a procedure for the selection of monitors. The new policy technically supersedes the Breuer Memo but largely maintains the same structure for selecting monitors.
- ³ The DOJ and SEC share some jurisdiction over enforcement of the FCPA. Unlike the DOJ, the SEC can only bring civil enforcement actions and can only regulate companies (and their subsidiaries and employees) who have stock listed on a public exchange (i.e. “issuers”).
- ⁴ These statistics are drawn from the DOJ Fraud Section’s Related Enforcement Actions webpages (see <https://www.justice.gov/criminal-fraud/related-enforcement-actions>) and the SEC’s SEC Enforcement: FCPA Cases webpage (see <https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml>), both of which list FCPA resolutions by year. In calculating the resolutions, settlements with a company and its subsidiaries are counted as one settlement.
- ⁵ See <https://www.justice.gov/criminal-fraud/pilot-program/declinations> (last visited Feb. 5, 2019).
- ⁶ 332 F. Supp. 3d 575 (E.D.N.Y. 2018).
- ⁷ 137 S. Ct. 1635 (2017).
- ⁸ 861 F.3d 760 (2017).
- ⁹ 905 F.3d 97 (2d Cir. 2018).
- ¹⁰ *United States v. Ho*, Case No. 17-cr-779-LAP, Dkt. No. 108 at 15:15-19:2 (E.D.N.Y. July 19, 2018).
- ¹¹ See U.S. Dept. of the Treasury, Resource Center, available at <https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx> (last visited Jan. 28, 2019).
- ¹² *Epsilon Electronics, Inc. v. U.S. Dept. of Treasury*, 857 F.3d 913 (2017).
- ¹³ *United States v. Holmes, et al.*, Case No. 18-cr-00258-EJD, Dkt. No. 1 (N.D. Cal. June 14, 2018).
- ¹⁴ *United States v. Hussain*, Case No. 16-cr-462-CRB, Dkt. No. 394 (N.D. Cal. Apr. 30, 2018).
- ¹⁵ *United States v. Lynch, et al.*, Case No. 18-cr-577-CRB, Dkt. No. 1 (N.D. Cal. Nov. 29, 2018).
- ¹⁶ “Uber Settles Data Breach Investigation for \$148 Million,” *New York Times*, Sept. 26, 2018, available at <https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html?login=email&auth=login-email> (last visited Jan. 24, 2019).
- ¹⁷ In its 2017 DAO Report of Investigation, the SEC asserted that certain crypto assets may be securities and therefore subject to the SEC’s jurisdiction.
- ¹⁸ Some estimates show a decrease in overall value of 80% or more. See <https://coinmarketcap.com/charts/>; <https://www.cnbc.com/2018/11/23/cryptocurrencies-have-shed-almost-700-billion-since-january-peak.html>.
- ¹⁹ Although often used in the same breath, cryptocurrency and blockchain are different. Cryptocurrencies, which are generally broken down into coins or tokens, are a digital form of money, essentially, which can be exchanged without an intermediary. They are typically tied to digital (and anonymous) addresses, which allows significant privacy. When cryptocurrency owners exchange their coins, the transactions are recorded in a public ledger known as a blockchain. A blockchain is a distributed ledger that appears on all computers with the blockchain program installed. Whenever a transaction is recorded on one computer in the blockchain network, the blockchain updates on all other computers within the network. See generally, Cryptocurrencies and blockchain, Legal context and implications for financial crime, money laundering, and tax evasion; European Parliament Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, available at [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU\(2018\)619024_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf).
- ²⁰ ICOs generated over \$21 billion in capital in 2018, nearly four times the amount raised in 2017. See <https://www.coinschedule.com/stats.html?year=2018>
- ²¹ Case No. 17CR647 (RJD), 2018 WL 4346339 (E.D.N.Y. Sept. 11, 2018).
- ²² Case No. 18CV2287-GPB (BLM), 2018 WL 6181408 (S.D. Cal. Nov. 27, 2018).
- ²³ Pub. Law No. 115-164.
- ²⁴ 584 U. S. ____ (2018).
- ²⁵ See *id.*, slip op. at 7.
- ²⁶ 583 U.S. ____ (2018).
- ²⁷ No. 1:16-cr-00370-CM.
- ²⁸ No. 14-cr-00458-JLL.
- ²⁹ Pub. L. 115–141.
- ³⁰ 18 U.S.C. § 2701 *et seq.*
- ³¹ *United States v. Microsoft*, 138 S. Ct. 1186 (2018).
- ³² CLOUD Act § 105.
- ³³ 138 S. Ct. 2206 (2018)
- ³⁴ *Id.* at 2217, 2219.
- ³⁵ *Id.* at 2220.
- ³⁶ *Id.* at 2218.
- ³⁷ *Id.* at 2220.
- ³⁸ *Id.* at 2223.
- ³⁹ *In the Matter of the Search of a Residence in Oakland, California*, Case No. 4:19-mj-70053-KAW, Dkt. No. 1 (N.D. Cal. Jan. 10, 2019).
- ⁴⁰ *Facebook v. Wint*, Case No. 18-CO-958, 2019 WL 81113 (D.C. Jan. 3, 2019).
- ⁴¹ *State of New Hampshire v. Verrill*, Case No. 219-2017-CR-072 (Strafford Cnty. Super. Ct. Nov. 5, 2018).
- ⁴² *State of Florida v. Sylvestre*, 254 So. 3d 986 (Fla. 2018).



Vinson & Elkins

Join Us on LinkedIn
Vinson & Elkins

Follow Us on Twitter
@vinsonandelkins

Vinson & Elkins LLP Attorneys at Law Austin Beijing Dallas Dubai Hong Kong
Houston London New York Richmond Riyadh San Francisco Tokyo Washington

velaw.com

Prior results do not guarantee a similar outcome. ©2019 Vinson & Elkins LLP