ALERT MEMORANDUM

U.S. Criminal Prosecution Based on Panama Papers Hack Raises Novel Legal Issues

January 17, 2019

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

NEW YORK

Victor L. Hou
+1 212 225 2609
vhou@cgsh.com

Lisa Vicens
+1 212 225 2524
evicens@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Martha E. Vega-Gonzalez
+1 212 225 2544
mvega-gonzalez@cgsh.com

Christine Jordan
+1 212 225 2347
cjordan@cgsh.com

Nearly a decade ago, WikiLeaks ushered in the age of mass leaks. Since then, corporations, governments, public figures and private entities have increasingly had to reckon with a new reality: that vigilantes, activists, extortionists and even state actors can silently steal and rapidly disseminate proprietary information, including customer data and other sensitive information. Last month, the Department of Justice ("DOJ") indicted four individuals based on information first revealed in the "Panama Papers" leak. This marks a significant milestone in law enforcement's reliance on evidence based on an unauthorized mass leak of information. While leaks and hacks are not a novel phenomenon—in 1971, the *New York Times* published top secret documents on the Vietnam War and, in 1994, a paralegal leaked tobacco industry documents that ultimately cost the industry billions of dollars in litigation and settlement costs—the frequency, scale and ease of dissemination of leaked information today presents a difference not only of degree, but of kind. The new Panama Papers-based criminal case will likely raise a host of novel legal issues based on legal challenges to the DOJ's reliance on information illegally obtained by a third party, as well as information that would ordinarily be protected by the attorney-client privilege. In this memorandum, we discuss the potential issues raised by the prosecution and their implications.

The Panama Papers

In April 2016, the International Consortium of Investigative Journalists unveiled the so-called Panama Papers. Then hailed as the largest leak in history, the Panama Papers represented 26 terabytes of data—11.5 million documents taken from Mossack Fonseca, a Panamanian law firm, containing financial, privileged, or otherwise confidential information of hundreds of thousands of individuals and entities.

According to press reports, the Panama Papers showed how Mossack Fonseca "helped clients launder money, dodge sanctions and avoid tax."[1] News reports explained in general terms how the law firm assisted clients who wanted to move their assets offshore, using allegedly illegal tactics. Based on the Panama Papers, journalists also named government officials and celebrities who used the law firm's services.

Unsurprisingly, regulators all over the world responded to the Panama Papers with significant interest. In the United States, New York's Department of Financial Services ("NYDFS") asked various financial institutions to produce communications between their New York branches and Mossack Fonseca shortly after the leak was revealed. On August 19, 2016, NYDFS fined Mega International Commercial Bank of Taiwan ("Mega Bank") $180 million for violating anti-money laundering laws, noting that its investigation determined that a substantial number of Mega Bank's customer entities "were apparently formed with the assistance of the Mossack Fonseca law firm."[2]

On December 4, 2018, federal prosecutors ventured into the Panama Papers controversy when they unsealed an indictment sought by the U.S. Attorney's Office for the Southern District of New York charging four individuals—a Mossack Fonseca lawyer, an investment manager for a Panama-based asset management company closely affiliated with Mossack Fonseca, an accountant and an alleged U.S. taxpayer client of the law firm—with tax fraud, money laundering and other offenses. One defendant is also charged with making false statements to the DOJ after reaching out to "correct" statements made in the press about him in connection with the Panama Papers coverage.

Potential Legal Challenges Related to the Government's Use of Hacked Information

In the criminal context, the Fourth Amendment protects against unreasonable searches and seizures by government officials and those private individuals acting as instruments or agents of the government. However, the Fourth Amendment does not protect against searches by private individuals acting in a private capacity. Thus, courts have long held that prosecutors may rely on evidence obtained illegally by private individuals, so long as those individuals were acting without the government's imprimatur.

The U.S. Courts of Appeals for the Eleventh and Fourth Circuits have analyzed the application of these Fourth Amendment principles to hacked materials in two related cases.[3] These cases concerned the admissibility of evidence obtained by the same anonymous hacker from the computers of two individuals, who were prosecuted for sexual exploitation and possession of child pornography.

The hacker, who claimed to be based in Turkey, identified the first individual and hacked into his computer. The hacker then reached out to U.S. law enforcement officials and provided them with evidence of the individual's crimes and his identifying information. With this information, law enforcement obtained a search warrant and ultimately an indictment. Subsequently, the same hacker provided

---

[1] Richard Bilton, *Panama Papers: Mossack Fonseca leak reveals elite's tax havens*, BBC NEWS (Apr. 4, 2016), https://www.bbc.com/news/world-35918844.

[2] Press Release, N.Y. Dep't of Fin. Servs., DFS Fines Mega Bank $180 Million For Violating Anti-Money Laundering Laws (Aug. 19, 2016), https://www.dfs.ny.gov/about/press/pr1608191.htm.

[33] *United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003); *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003).

law enforcement with hacked information on another child pornographer, who was also indicted.

Both individuals challenged the government's reliance on hacked information on Fourth Amendment grounds. The courts analyzed these challenges and the question of whether the hacker was acting as the government's agent considering two factors: (1) whether the government knew of and acquiesced in the intrusive conduct and (2) whether the private actor's purpose was to assist law enforcement efforts rather than to further his own ends. Both courts held that the hacker was not an agent of law enforcement and that the evidence was admissible. Because neither factor was met with respect to the anonymous hacker in the first prosecution, the Eleventh Circuit affirmed the defendant's conviction. Notably, in the second prosecution, the government conceded that the hacker's purpose was to assist law enforcement, so the primary question before the court was whether the government knew of and acquiesced in the hacker's intrusive conduct. The Fourth Circuit found that the hacker's interactions with law enforcement leading up to the second defendant's arrest did not amount to "affirmative encouragement" and therefore no agency relationship existed, but noted in dicta that the apparent encouragement the hacker had received from law enforcement after the arrest was probably sufficient to create an agency relationship going forward.

While other circuits have analyzed the agency factors slightly differently, these cases illustrate that the traditional framework for analyzing whether the government will be precluded from using information illegally obtained from a third party centers on the relationship between the private source of the information and U.S. government actors. It is thus unlikely that information obtained from typical mass leaks could be suppressed on Fourth Amendment grounds given the general pattern that—to the extent they are identified at all—the individuals behind such incidents usually are non-government actors. Indeed, there is nothing in the public record to suggest that the John Doe who leaked the Panama Papers has an agency relationship with the United States government. Although he has publicly expressed his view that much of Mossack Fonseca's activity was criminal and his willingness to assist law enforcement, John Doe has disclaimed any past or present association with government and intelligence agencies.[4] Thus, to the extent the defendants in the Panama Papers case challenge the legality of the government's reliance on illegally obtained information, the arguments will likely rise and fall on whether the defendants can otherwise show that John Doe (or any other persons who obtained the hacked information) were in fact acting in concert with law enforcement.

Potential Legal Challenges Related to the Government's Access to Privileged Information

Privileged information caught in mass leaks may pose a more difficult hurdle for prosecutors.

As a threshold matter, attorney-client communications and attorney work product are typically protected by evidentiary privileges. Thus, unlike the information obtained by the anonymous hacker discussed above, privileged information may be inadmissible in court, regardless of how it was obtained, unless the privilege has been waived by the client or some other exception applies. Additionally, when law enforcement obtains privileged information—regardless of whether it was obtained through a lawful seizure or an illicit leak—criminal defendants may argue that any government investigator or witness who reviews the privileged information is then "tainted" by their exposure to privileged materials and that the government must establish that its prosecution team is free from that taint.

[4] John Doe, *John Doe's Manifesto*, SÜDDEUTSCHE ZEITUNG, https://panamapapers.sueddeutsche.de/articles/572c897a5632a39742ed34ef/.

In the context of compelled testimony protected by the Fifth Amendment, under the Supreme Court's seminal decision in *Kastigar v. United States*, the government must show that a prosecution is not based on the compelled testimony through a procedure commonly called a *Kastigar* hearing.[5] Indeed, the Second Circuit recently held in *United States v. Allen* that this applies even in those cases where the testimony was compelled by a foreign government.[6] There, one of the government's cooperating witnesses had reviewed testimony of the defendants compelled by the U.K. Financial Conduct Authority. On appeal of the defendants' convictions, the Second Circuit found that during a post-trial *Kastigar* hearing, the DOJ did not meet its heavy burden of showing that the evidence supplied by its cooperator was untainted by information gleaned from the compelled testimony. The Second Circuit therefore reversed the convictions.

The Courts of Appeals are divided on whether *Kastigar*'s strictures apply when the attorney-client privilege is implicated: the Fourth and Sixth Circuits have held that *Kastigar* is limited to cases involving compelled testimony, while the Second Circuit has suggested otherwise.[7] Nevertheless, concerns over *Kastigar*-like hearings have, in many cases, motivated the government's use of so-called "taint teams" to insulate investigators and prosecutors from attorney-client privileged information. These taint teams are composed of government investigators and lawyers who are screened from the prosecuting team and review materials with the aim of removing privileged documents from the scope of the prosecuting team's review. In these circumstances—unlike in normal discovery—initial privilege determinations are made by the government's taint team, *not* the attorneys of the person claiming the privilege.

Courts have frequently permitted prosecutors to employ taint teams to review documents seized from attorneys, even over the objections of the privilege holders. In certain cases, however, a more impartial arbiter of privilege may be selected. For example, after the government lawfully seized the files of President Trump's attorney, Michael Cohen, the prosecuting attorneys initially sought to use a taint team to review Mr. Cohen's files, but later withdrew their objection to the appointment of a special master, who made privilege determinations before releasing information to the prosecution team.

In the case of the Panama Papers, given that this information originated from a law firm, it is almost certain that the leaked documents contain a mountain of potentially privileged information. The DOJ has not revealed whether it used a taint team to review the Panama Papers, although this may become public as the case proceeds. To the extent the defendants launch a challenge on this basis, they will need to establish that the government was required to use a taint team—which no circuit has required in the context of attorney-client information—*and* that the government's taint team was not effective in screening prosecutors from privileged material.[8] Even if the defendants are able to meet these hurdles, the government may respond that the information is not privileged in the first place, on the basis of the crime-fraud exception or otherwise.

Takeaways

It remains to be seen whether the defendants will be able to challenge any of the government's uses of the leaked information. In the meantime, mass leaks will undoubtedly continue, as will the interest of prosecutors and litigants in their content, and this dual

[5] 406 U.S. 441 (1972).

[6] 864 F.3d 63 (2d Cir. 2017).

[7] *Compare United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) *and United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000) *with United States v. Schwimmer*, 892 F.2d 237 (2d Cir. 1989).

[8] Notably, the attorney-client privilege is a creation of the common law, not the Constitution. Nevertheless, certain governmental intrusions into the attorney-client privilege may implicate constitutional rights under the Fourth, Fifth and Sixth Amendments.

dynamic will raise further novel issues at the intersection of law, ethics and privacy.

The recent indictment illustrates various ways in which prosecutors may address some of the pitfalls associated with mass leaks and potentially privileged information. In particular:

- Prosecutors and regulators can respond to leaks that reveal potential wrongdoing by independently seeking evidence from targets and third parties rather than relying on potentially illegally leaked information. With respect to the Panama Papers, NYDFS asked various financial institutions to produce communications between their New York branches and Mossack Fonseca. Additionally, the documents requested by NYDFS—ostensibly between a law firm and a non-client party—would not ordinarily be protected by the attorney-client privilege.
- Relatedly, the government may be able to directly obtain documents and testimony from cooperating witnesses implicated by the leaks. For example, an unnamed client of Mossack Fonseca provided the DOJ with email correspondence related to that client's dealings with the defendants and others, allegedly showing the roles of various defendants in providing this client with "the tools to conceal millions of dollars in assets offshore."[9] To the extent that these emails contained privileged information, the cooperating witness, as the holder of the privilege, would be in a position to waive it, although prosecutors must be cognizant of DOJ policy that discourages seeking waivers of the attorney-client privilege in exchange for cooperation credit.[10]
- Prosecutors may also seek to rely on the crime-fraud exception to the attorney-client privilege: communications that otherwise would be protected by the attorney-client privilege or the attorney work product privilege are not protected if they relate to client communications in furtherance of contemplated or ongoing criminal or fraudulent conduct. As alleged in the indictment, many of the communications involving Mossack Fonseca related to the establishment of fraudulent accounts or structuring transactions to illegally avoid paying taxes, and would therefore not be protected by the attorney-client or work product privileges.

The Panama Papers leak and the recent related indictments underscore that it is virtually impossible to put the genie back in the bottle after a mass leak. To that end, companies should ensure that their cybersecurity systems—and those of their third-party vendors—are effective and up to date. In sensitive cases, special care and attention should also be given to privileged communications to minimize the likelihood that a later decision maker will reach an adverse privilege conclusion. And, when cybersecurity defenses fail and a leak does occur, victims of a leak should carefully consider their potential legal exposure; where exposure may exist, potential targets should consider the costs and benefits of proactively approaching law enforcement to assert their rights in connection with the leaked information, including, if necessary and appropriate, asserting that any unlawfully obtained information should not be in the hands of any third parties, including the government. Where leaks contain privileged information, attention should be paid to continuing to assert privilege over leaked documents, and avoiding potential waiver.

…

CLEARY GOTTLIEB

[9] Indictment at ¶ 70, *U.S. v. Owens*, No. 18 cr 693 (S.D.N.Y. Sept. 27, 2018), ECF No. 7.

[10] U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-28.710 (Aug. 2018).