The Alfa Bank Hoax Is Looking A Lot Like Crossfire Hurricane

April 04, 2022

A lawyer for former Hillary Clinton campaign attorney Michael Sussmann revealed last week that federal agents never asked Sussmann the origin of the data he provided the FBI related to the Alfa Bank hoax. Beyond highlighting the hackery of the Crossfire Hurricane team, this revelation raises broader concerns about the cozy relationship between the government and private cybersecurity experts.

On Thursday, Sussmann's Latham and Watkins attorney Michael Bosworth pushed for the dismissal of the special counsel's criminal case. That case charged Sussmann with lying to former FBI General Counsel James Baker when he provided Baker "white papers" and data ostensibly showing a secret communications channel between the Trump organization and the Russia-connected Alfa Bank. According to the indictment, Sussmann falsely claimed during his meeting with Baker that he was not acting on behalf of a client, when in fact he was working for both the Clinton campaign and tech executive Rodney Joffe.

During last week's oral argument on Sussmann's motion to dismiss, Bosworth posited that Sussmann's allegedly false statement was not "material" to the FBI—and thus not a crime—by arguing that because the FBI never questioned Sussmann on the source of the Alfa Bank information, it was irrelevant to the investigation.

Not once will the evidence show, Bosworth argued, that "anyone at the FBI ever asked Mr. Sussmann, 'Hey, by the way, where did this information come from?' No one asked. Not once. Ever." Sussmann's attorney continued: "Regardless of who his clients were, if the source of his information was so critical to the government's investigation, if it mattered so much, you'd think at some point someone would have said, 'Hey, buddy, you provide this tip to the government. Where did this stuff come from? Who gave it to you? Where did—how did they get it?"

Bosworth's argument came in response to prosecutor Andrew DeFilippis's assertion that the special counsel's office would "put on the stand at trial witnesses who will say that, when you're analyzing data, you don't simply close your eyes to where the data came from and compare it to other data or look for corroboration through other sources. The first thing any responsible forensic analysis will ask is 'Where was the data from?'"

Picking up on Bosworth's argument, the court interrupted DeFilippis, asking: "If that's the first thing a responsible investigator would ask, then why would it matter whether Mr. Sussmann was there on behalf of a client or not? Wouldn't the natural question have been, 'Where did this stuff come from?'"

DeFilippis responded that because the former FBI general counsel wrongly believed Sussmann had come forward "as a good citizen," that lulled Baker into accepting the data and white papers without question. Sussmann's attorney called that argument "nonsensical," saying that, "if, as the special counsel claims, the first question that investigators would ask is where did the data come from, that's the question that's paramount."

Bosworth then stressed that the FBI knew the data didn't originate with Sussmann because he's "a lawyer" and isn't "sitting on a pool of DNS data," and because Baker testified repeatedly that "Sussmann told him that the information originated with various cyber experts." "At no point did the FBI say, "Who are those experts? Can we talk to them? Where did they get it from?" Bosworth continued. "So, the notion that Mr. Sussmann's statement about a client somehow affected the FBI's willingness to ask the basic questions they ask in any case just doesn't hold water," Sussmann's attorney concluded.

Bosworth made an excellent point—actually two, as we will soon see—just not the winning point he thought. The failure of the FBI to ask "the basic questions" about the data and white papers Sussmann provided on the purported Trump-Alfa Bank secret communications speaks not of the unimportance of that information, but of the incompetence (or political corruption) of the Crossfire Hurricane team.

The Tips of Many Icebergs

The FBI's glaring lack of curiosity concerning the source of the Alfa Bank "intel" mirrors in many respects how the agents assigned to investigate Trump approached the Steele dossier. With Christopher Steele's supposed intel, the Crossfire Hurricane team undertook some steps to identify Steele's sources and to verify the information contained in the memoranda. Yet before they were able to do either, the Department of Justice submitted a Foreign Intelligence Surveillance Act (FISA) application to the FISA court and obtained a warrant to surveil former Trump campaign advisor Carter Page.

The DOJ later submitted three renewal applications to the FISA court, again relying heavily on the Steele dossier, even though agents were

unable to confirm any of the non-public "intel" of relevance and after discovering numerous problems with Steele's reporting. The Department of Justice's Office of Inspector General or OIG later found that the FISA applications targeting Page contained 17 "significant inaccuracies and omissions."

Soon after, the then-presiding judge of the FISA court, Rosemary Collyer, blasted the FBI for its handling of the Page FISA applications. She also stressed "the frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable."

The FISA abuse seen in the Page case exposed the DOJ and FBI's sloppiness, disregard for the law, incompetence, and political bias, casting doubt on the entire FISA process. Similarly, the revelation last week that no one from the FBI asked Sussmann for the source of the Alfa Bank data and whitepapers suggests these same problems broadly infect federal law enforcement and intelligence agencies.

Relying on Obviously Suspect Information

With Steele, the feds believed the unbelievable in part because of Steele's pedigree as a former MI6 agent. Here the FBI relied unquestioningly on Sussmann and the data and white papers he provided from "various cyber experts" to open an investigation into the supposed Alfa Bank-Trump communications network.

While Sussmann's attorney posited that the FBI unquestioningly accepted the data and white papers because the source of the

information was irrelevant, the more likely explanation is that the law enforcement and intelligence communities worked regularly with Sussmann, tech companies, and cyber experts, and placed unwavering trust in those sources.

Sussmann's congressional testimony confirmed that he had "various contacts with members of law enforcement and the intelligence community on behalf of a number of different clients" since leaving the Department of Justice. He had served as "a prosecutor in the {DOJ's] Computer Crime and Intellectual Property Section" before joining Perkins Coie.

Sussmann likewise revealed in court filings that Joffe, "far from being a stranger to the FBI—was someone with whom the FBI had a long-standing professional relationship of trust and who was one of the world's leading experts regarding the kinds of information that Mr. Sussmann provided to the FBI."

There's a Whole Lot of This Going On

It was also not merely Sussmann and Joffe with whom the FBI and intelligence agencies held close contact. Rather, documents obtained from right-to-know requests to Georgia Tech reveal extensive coordination between the Department of Defense's Defense Advanced Research Projects Agency (DARPA), the FBI, and cybersecurity experts.

Some of this coordination came through private organizations such as Ops-Trust, a self-described "highly vetted community of security professionals focused on the operational robustness, integrity, and security of the Internet" that includes both law enforcement and private cybersecurity experts. The National Cyber Forensics and Training

Alliance, or NCFTA, likewise "facilitates collaboration and information sharing between private industry, academia, and the law enforcement/intelligence community" with the FBI having an agent "collocated" at the NCFTA.

Emails reviewed by The Federalist show regular communication between the FBI and members of the NCFTA listserv discussing investigative matters, including requests by the FBI for "law enforcement friendly contacts" at tech companies. No wonder, then, that the FBI was "lulled" into opening an investigation into the supposed Trump-Alfa Bank connection based on Sussmann's word that the data and white papers originated with cyber experts.

Just Consider One Other Georgia Tech Researcher

While the documents publicly available remain limited mainly to those accessible from Georgia Tech, that material still provides a glimpse at the deep connection between private cybersecurity experts and members of federal law enforcement and intelligence agencies.

Emails show, for instance, that Manos Antonakakis, the Georgia Tech researcher who reviewed one of the white papers Sussmann later provided to Baker, worked for years with FBI agents, communicated with DARPA about various requests to assist with FBI or DOJ investigations, and provided analyses used in various criminal matters. Antonakakis also provided an analysis for the federal government of hackers believed to be working for the Russian military intelligence agency GRU, known publicly by the nickname "Fancy Bear."

Other documents show that as part of Antonakakis' work with DARPA

and the $17 million contract awarded Georgia Tech researchers to "identify the virtual actors responsible for cyberattacks, a technique known as 'attribution,'" Antonakakis conducted attribution analysis for the federal government, including with data provided by Joffe.

A Situation Ripe for Setups

This collaboration between government entities and private cybersecurity experts is, as the Wall Street Journal recently reported, of "enormous intelligence value" and "can help governments and companies detect and counter cyberattacks." The Journal's coverage, however, missed the mark when it then noted that "the monitoring of web traffic flow by government entities and private cybersecurity experts" raises "privacy implications."

This analysis missed the larger and more serious scandal: Individuals with wide access to sensitive government and proprietary data can exploit that data to target a political opponent. They can draft misleading "white papers," present the data and white paper to the FBI and CIA with whom they hold a trusted relationship, and thereby trigger a criminal (or national security) investigation.

The Sussmann indictment and other documents filed in his criminal case allege this exact scenario, with one cyber expert called merely the "Originator" but since identified as April Lorenzen creating a dataset purporting to show the Trump-Alfa Bank connection. She shared her data with Joffe, who tasked Antonakakis, Dave Dagon, and employees working at technology companies connected to Joffe "to mine Internet data to establish 'an inference' and 'narrative' tying then-candidate Trump to Russia."

Apparently Fabricating Allegations Out of Spite

Joffe would later present to other researchers a "white paper" that purported to explain the basis for the Trump-Alfa Bank theory, asking for their feedback. While Antonakakis did not support the paper and thought it "was not great," privately he told Joffe that while "a DNS expert would poke several holes to this hypothesis (primarily around visibility," "very smartly you do not talk about" that. "That being said," Antonakakis added, "I do not think even the top security (non-DNS) researcher can refute your statements. Nice!"

Knowing the deficiencies in the white paper, Joffe nonetheless allegedly had Sussmann hand it off to the FBI's general counsel, which then triggered a federal investigation into the supposed Trump-Alfa Bank connection. The Clinton campaign also pushed the Alfa Bank hoax to the media, directing reporters to talk to Georgia Tech's Dagon about the analysis.

Sussmann also presented a second set of data to the CIA that allegedly consisted of internet traffic exploited by Joffe, Dagon, and Lorenzen related to, among other locales, the Trump Tower, Donald Trump's Central Park West apartment building, and the Executive Office of the President of the United States. In providing this data to the CIA, the "trusted" Sussmann told agents, the data "demonstrated that Trump and/or his associates were using supposedly rare, Russian-made [Yota] wireless phones in the vicinity of the White House and other locations."

Not only was there "no support for these allegations," according to the special counsel, the data provided to the CIA was cherry-picked to create the appearance of a Trump-Russia connection, while additional data compiled by the researchers but not shared with the CIA

conflicted with the Yota cell phone theory.

Weaponizing National Security Against Political Targets

These allegations indicate that, as with the Steele dossier, politically motivated actors presented false or misleading information to federal agents to prompt an investigation into Trump. As in the case of Steele's intel, the Crossfire Hurricane team took the data seriously, in part because it came from supposedly trusted sources.

Just as the implications of the FISA abuse extended beyond Page's case and raise concerns about the entire FISA system, the implications of cybersecurity experts allegedly exploiting nonpublic internet traffic to frame a political enemy reach beyond Trump. If cybersecurity experts could trigger an investigation into Trump for political reasons, they can prompt an investigation of anyone, for any reason. Maybe they already have.

Lorenzen, Dagon, Joffe, and Sussmann allegedly culled data to fit a narrative and possibly draft misleading "white papers" that Sussmann, on behalf of Joffe, then presented to the FBI and CIA for political ends. This destroys the public's trust in cybersecurity experts. The FBI's failure to ask even the most basic questions when it received the data and unsigned "white papers" from Sussmann renders them likewise suspect.

Yet Dagon's attorney has the chutzpah to claim, as the Wall Street Journal put it, "that the indictment of Mr. Sussmann would have a chilling effect on decades of constructive cooperation between private cybersecurity researchers and government." "Because the way the

government and Durham has handled this, the cybersecurity community now is afraid to take anything to law enforcement," Jody Westby told the paper. As a result, "the whole nation is at a higher risk level," Westby warned.

On this latter point, Westby is correct: Our nation is at higher risk of cyber-attack. But the blame for that firmly lies with the cybersecurity experts who abused the great power entrusted to them to hurt Trump.

It is not merely those who prepared the material or presented it to the FBI or CIA who hold responsibility. Every cybersecurity expert who bolstered the Alfa Bank hoax, defended a theory that a "DNS expert" could easily poke several holes in, refused to reveal those deficiencies, failed to call out colleagues for abusing the government and public's trust, and instead blamed the special counsel's office for revealing the sham, shares in the blame.

The work private cybersecurity experts do, and the help they provide the FBI and intelligence agencies, is of vital importance to our country and its national security. It is precisely because of this that the Alfa Bank and Yota cell phone hoaxes are so scandalous.

Margot Cleveland is The Federalist's senior legal correspondent. She is also a contributor to National Review Online, the Washington Examiner, Aleteia, and Townhall.com, and has been published in the Wall Street Journal and USA Today. Cleveland is a lawyer and a graduate of the Notre Dame Law School, where she earned the Hoynes Prize—the law school's highest honor. She later served for nearly 25 years as a permanent law clerk for a federal appellate judge on the Seventh Circuit Court of Appeals. Cleveland is a former full-time university

faculty member and now teaches as an adjunct from time to time. As a stay-at-home homeschooling mom of a young son with cystic fibrosis, Cleveland frequently writes on cultural issues related to parenting and special-needs children. Cleveland is on Twitter at @ProfMJCleveland. The views expressed here are those of Cleveland in her private capacity.