WSJ

Durham Probe Reveals Government Access to Unregulated Data Streams

Special counsel's investigation into origins of FBI's Russia probe points to how cybersecurity researchers and government agencies tap into huge reservoirs of potentially revealing internet data

By Byron Tau, Dustin Volz, and Robert McMillan

Feb. 26, 2022 5:33 am ET

The latest developments in a high-profile criminal probe by special counsel John Durham show the extent to which the world's internet traffic is being monitored by a coterie of network researchers and security experts inside and outside the government.

Mr. Durham has been looking into the origins of the FBI's investigation into alleged ties between the Trump campaign and Russia. Recent court filings in his case against cybersecurity lawyer Michael Sussmann, as well as documents obtained by The Wall Street Journal through public records requests, show how U.S. government entities and private cybersecurity companies are able to monitor the flow of web traffic by tapping into vast quantities of data with little oversight or public awareness. Though such technical data doesn't directly reveal identities or message content, it can at times be reverse-engineered to link online activity back to specific individuals or organizations.

A filing by prosecutors earlier this month said people affiliated with Donald Trump's 2016 Democratic rival for the presidency, Hillary Clinton, worked to exploit nonpublic internet traffic data they had access to in order to establish a narrative tying Mr. Trump to Russia. Mr. Sussmann's lawyers called the allegations misleading and irrelevant.

The monitoring is made possible by little-scrutinized partnerships, both informal and formal, among cybersecurity companies, telecommunications providers and government agencies. The U.S. government is obtaining bulk data about network usage, according to federal contracting documents and people familiar with the matter, and has fought disclosure about such activities. Academic and independent researchers are sometimes tapped to look at data and share any findings with the government without warrants or judicial authorization.

Unlike the disclosures by former intelligence contractor Edward Snowden from nearly a decade ago, which revealed U.S. intelligence programs that relied on covert access to private data streams, the sharing of internet records highlighted by Mr. Durham's probe concerns commercial information that is often being shared with or sold to the government in bulk.

Such data sets can possess enormous intelligence value, according to current and former government officials and cybersecurity experts, especially as the power of computers to derive insights from massive data sets has grown in recent years. Such network data can help governments and companies detect and counter cyberattacks. But that capability also has privacy implications, despite assurances from researchers that most of the data can't be traced back to individuals or organizations, as the traffic associated with Mr. Trump's Manhattan address was.

At issue are several kinds of internet logs showing the connections between computers, typically collected on networking devices such as switches or routers. They are the rough internet equivalent of logs of phone calls—showing which computers are connecting and when, but not necessarily revealing anything about the content of the transmissions. Modern smartphones and computers generate thousands of such logs a day just by browsing the web or using consumer apps.

Academic researchers looking at such computer logs for evidence of cybersecurity threats in 2016 grew concerned about what appeared to be computer-server connections between Mr. Trump's Manhattan tower and a Russian bank. Mr. Trump has denied any ties to Russia.

Mr. Sussmann—whose firm represented the Clinton campaign as well as a tech firm that provided some data for the research—eventually passed the researchers' findings on to the Central Intelligence Agency and the Federal Bureau of Investigation for further investigation. He is charged with lying to the FBI about whom he was representing and has pleaded not guilty. The reason for the computer connection remains unexplained. While some independent internet experts have said the traffic appeared odd, others have offered benign technical explanations.

Julian Sanchez, a senior fellow at the libertarian-leaning Cato Institute who researches privacy and technology issues, said the Durham filing highlighted the obscure ways that pools of data collected or analyzed by third parties—whether cybersecurity researchers or businesses looking to resell personal data—can land in government hands without being subjected to traditional warrant requirements.

"A question worth asking is: Who has access to large pools of telecommunications metadata, such as DNS records, and under what circumstances can those be shared with the government?" Mr. Sanchez said.

The amount of information generated and the use of artificial intelligence tools—combined with less-stringent restrictions than the laws that apply to more-direct wiretapping practices—means this data has become exponentially more valuable in recent years, he said.

"Surveillance takes the path of least resistance," Mr. Sanchez said. Today, he said, "you have enough data and computing power that you can generate intrusive insights from data that is fairly unregulated."

Internet traffic from Mr. Trump's Manhattan address was part of bulk data being used by academic researchers funded in part by U.S. Defense Department grants from Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory, according to documents and interviews with people familiar with the project. Manos Antonakakis, a Georgia

Tech professor and the lead researcher on the project, had put together a team of experts and academics to work on hunting for cyber threats in 2016.

The grant proposals and contract documents viewed by The Wall Street Journal show that the Pentagon-funded work wasn't related to Mr. Trump. However, according to emails released to the Journal under Georgia's public-records law, the same team of researchers had begun work, before the official start date of the DARPA project, on a project with potential political implications.

The Georgia Tech team partnered with Neustar—a Washington-area technology and telecommunications company—to get internet logs for the DARPA project, the emails show. The DARPA funding wasn't scheduled to begin until November 2016, but Neustar began transferring data to the Georgia Tech researchers in late July.

DARPA, through a spokesman, denied any links to the research that was turned over to federal authorities regarding Mr. Trump's computer servers, saying any data acquired before the official start of government funding was done of Georgia Tech's own accord.

Neustar declined to answer a detailed list of questions about its participation in the project. Georgia Tech didn't respond to a request for comment.

At the center of the data transfers from Neustar was Rodney Joffe, a South African-born tech executive with ties to the intelligence community and the Defense Department who got his start in the direct-mail and marketing business before becoming a prominent anti-spam and cybersecurity expert. His lawyers declined to comment beyond saying he had "decades of service to the U.S. government" and the data he provided was legally acquired.

At the time of his contact with the Georgia Tech researchers, Mr. Joffe was a senior vice president and chief technology officer at Neustar, and had ties to other companies that work with government on technology-related matters.

Mr. Joffe is the owner, for instance, of Packet Forensics, a small technology firm that has a $35 million contract with DARPA, according to federal contracting records. In 2010, the company was marketing a device to foreign and U.S. government entities that allowed them to intercept people's internet traffic by forging security certificates. The company also offers numerous other technical services for government entities, according to its website.

According to people familiar with the matter, Mr. Joffe has long been involved in various government intelligence and cybersecurity efforts—including sometimes procuring or facilitating the acquisition of data or technological capabilities. In a 2015 interview with a Neustar employee after receiving a trade-association award, Mr. Joffe said: "I'm not the smart guy in the room. I'm really the dumb guy that carries the bags. But fortunately in those bags, I have a lot of money. So my role has really been carrying the bags of money to help whenever I can whenever folks in the community want things."

While online, users as they move around the web generate several kinds of internet metadata of the sort used to identify communications to and from Mr. Trump's Manhattan address. To access

most sites and services, users must connect between their computer and a server. Logs called "netflow" data provide information about where and when computers connect on the internet. And another kind of internet data called DNS data acts as a phone book for the internet—converting URLs like wsj.com into numerical IP addresses readable by computer servers.

Together, these two kinds of network data are used for widespread digital monitoring and highlight the government's ability to look very precisely at computer connections that can sometimes be traced back to individuals or companies.

For example, an American working in China described to the Journal how the FBI warned his U.S.-based private-sector employer in 2020 about a potential cyberattack—mistaking his legitimate network connection to his company's U.S. server as potentially nefarious. The approach occurred during the 2020 election campaign, when U.S. officials were scouring the web for potential trouble.

Jody Westby, a lawyer and cybersecurity expert representing one of the Georgia Tech researchers, said that the indictment of Mr. Sussmann would have a chilling effect on decades of constructive cooperation between private cybersecurity researchers and government.

"Because of the way the government and Durham has handled this, the cybersecurity community now is afraid to take anything to law enforcement," Ms. Westby said. "The whole nation is at a higher risk level."