

Pat Ryan worked for a data mining company that faced controversy after its CIA contract was revoked, though it continued to serve an entity controlled by Russian President Vladimir Putin.

Ryan promoted the company Dataminr’s services as early as May 2014 and per his 2017 Congressional Financial Disclosure Report, Ryan earned \$232,150 as Senior Vice President of Dataminr, Inc. in the first nine months of 2017:

- Ryan promoted the value of Dataminr’s services as early as May 2014.



(Pat Ryan, [Twitter](#), 5/19/14)

- Per his 2017 Congressional Financial Disclosure Report, Pat Ryan earned \$232,150 as Senior Vice President of Dataminr, Inc. in the first nine months of 2017.

SCHEDULE C: EARNED INCOME			
Source	Type	Amount Current Year to Filing	Amount Preceding Year
Dataminr, Inc.	Salary	\$232,150.00	\$326,510.35
Greater New York Hospital Association	Spouse Salary	N/A	N/A

(Patrick Ryan: Financial Disclosure Report, [Clerk of the House of Representatives](#), 10/5/17)

SCHEDULE E: POSITIONS	
Position	Name of Organization
Director	Second Front Systems
Director	Young Professionals in Foreign Policy
Senior Vice President	Dataminr, Inc.

(Patrick Ryan: Financial Disclosure Report, [Clerk of the House of Representatives](#), 10/5/17)

Dataminr is a multimillion-dollar startup that mines public Twitter feeds for clients and is one of the few companies authorized to analyze the entire Twitter "firehose," and is “resell the complete stream of tweets”:

- **Dataminr is a multimillion-dollar startup.** “Dataminr, a New York startup that has raised \$50 million and caters to hedge funds to emergency responders, is growing its footprint into media and probably other verticals because it has a knack for alerting customers to actionable tweets in a sea of noise.” (Larry Dignan, “Q&A with Dataminr CEO Ted Bailey: Making Twitter’s firehose actionable,” [ZDNet](#), 5/19/14)
- **Dataminr mines public Twitter feeds for clients and is one of few companies authorized to analyze the entire Twitter "firehose," identifying important information and anomalies.** “As a strategic partner of Twitter, Dataminr has direct access to the company's firehose and finds relevant

information to deliver via alerts on the desktop, email, or in a business system.” (Larry Dignan, “Q&A with Dataminr CEO Ted Bailey: Making Twitter’s firehose actionable,” [ZDNet](#), 5/19/14)

- **Dataminr is “Twitter’s only data partner that is also allowed to resell the complete stream of tweets.”** “As Twitter’s only data partner that is also allowed to resell the complete stream of tweets, Dataminr sells its service to hedge funds, news outlets, large corporations, and government bodies.” (Jen Wieczner, “CIA Director Is ‘Disappointed’ in Twitter and Dataminr,” [Fortune](#), 6/20/16)

Dataminr sold data to the CIA until 2016, when Twitter abruptly revoked the CIA’s access to Dataminr out of apparent concern that its reputation would suffer if it was perceived to be too cozy with the spy agency:

- **This included the CIA until 2016, when Twitter abruptly revoked the CIA’s access to Dataminr out of apparent concern that its reputation would suffer if it was perceived to be too cozy with the spy agency.** “The Wall Street Journal reported last month that Twitter abruptly revoked the CIA’s access to Dataminr out of apparent concern that its reputation would suffer if it was perceived to be too cozy with the spy agency. But critics quickly accused Twitter of being hypocritical in its decision after Russian state-owned news outlet RT said it still had Dataminr access. “Agents of Russia’s Federal Security Service, formerly known as the KGB, have full access via RT to the alerts now being denied to the CIA,” a Journal op/ed columnist wrote.” (Jen Wieczner, “CIA Director Is ‘Disappointed’ in Twitter and Dataminr,” [Fortune](#), 6/20/16)

Twitter owns 5% of Dataminr and the CIA’s venture capital fund owns part of Dataminr:

- **Twitter owns 5% of Dataminr and the CIA’s venture capital fund owns part of Dataminr.** “Dataminr has received investments from both Twitter, which reportedly owns a 5 percent stake in the company, and In-Q-Tel, the CIA’s venture capital fund that exists to spur innovative technologies of interest to the intelligence community.” (Eamon Javers “Why Twitter chose to do battle with the CIA,” [CNBC](#), 5/13/16)

In May 2016, Twitter cut off U.S. intelligence agencies from access to Dataminr’s service:

- **In May 2016, Twitter cut off U.S. intelligence agencies from access to Dataminr’s service.** “Twitter Inc. TWTR +0.56% cut off U.S. intelligence agencies from access to a service that sifts through the entire output of its social-media postings, the latest example of tension between Silicon Valley and the federal government over terrorism and privacy. The move, which hasn’t been publicly announced, was confirmed by a senior U.S. intelligence official and other people familiar with the matter. The service—which sends out alerts of unfolding terror attacks, political unrest and other potentially important events—isn’t directly provided by Twitter, but instead by Dataminr Inc., a private company that mines public Twitter feeds for clients. Twitter owns about a 5% stake in Dataminr, the only company it authorizes both to access its entire real-time stream of public tweets and sell it to clients.” (Christopher S. Stewart and Mark Maremont, “Twitter Bars Intelligence Agencies From Using Analytics Service,” [The Wall Street Journal](#), 5/8/16)

Controversy arose when Dataminr stopped serving the CIA as a client, but continued to serve Vladimir Putin’s RT broadcaster, which provides access to Russia’s Federal Security Service, formerly known as the KGB:

- Controversy arose when Dataminr stopped serving the CIA as a client, but continued to serve Vladimir Putin’s RT broadcaster, which provides access to Russia’s Federal Security Service, formerly known as the KGB. “Silicon Valley’s hostility to U.S. intelligence and law enforcement reached a new low last week when Twitter rejected the Central Intelligence Agency as a customer for data based on its tweets—while continuing to serve an entity controlled by Vladimir Putin. The Wall Street Journal broke the news that Twitter decided U.S. intelligence services could no longer buy services from Dataminr, which has a unique relationship with Twitter. Dataminr is the only company Twitter allows to have access to its full stream of hundreds of millions of daily tweets and sell the resulting intelligence to customers. ... Among the customers still getting the Dataminr alerts is RT, the broadcaster created and funded by the Russian government. Vladimir Putin has said that the government runs RT to ‘try to break the Anglo-Saxon monopoly on the global information streams.’ RT disclosed it is a Dataminr customer in its news account of Twitter barring the CIA. Agents of Russia’s Federal Security Service, formerly known as the KGB, have full access via RT to the alerts now being denied to the CIA.” (L. Gordon Crovitz, Op-ed, “Twitter Picks Russia Over the U.S.,” [The Wall Street Journal](#), 5/15/16)
- RT was one of Dataminr’s clients. “RT is one of Dataminr’s clients.” (“Twitter bans US intelligence access to Dataminr analytics - report,” [RT](#), 5/9/16)

Despite Ryan’s data firm prohibiting access to U.S. intelligence while serving Russian intelligence, Ryan was “gravely concerned that a foreign adversary like Russia was actively trying to influence our election and undermine our democracy:”

- In 2017, Ryan posted on Facebook that he was “gravely concerned that a foreign adversary like Russia was actively trying to influence our election and undermine our democracy.”



(Pat Ryan for Congress, [Facebook](#), 6/8/17)



(Pat Ryan for Congress, Facebook, 7/10/17)

Even after Ryan’s data firm was supposed to cut off its service from U.S. intelligence agencies, it ran into trouble for servicing domestic spy centers and had to be forced to stop:

- **In May 2016, Twitter cut off U.S. intelligence agencies from access to Dataminr’s service.** “Twitter Inc. TWTR +0.56% cut off U.S. intelligence agencies from access to a service that sifts through the entire output of its social-media postings, the latest example of tension between Silicon Valley and the federal government over terrorism and privacy. The move, which hasn’t been publicly announced, was confirmed by a senior U.S. intelligence official and other people familiar with the matter. The service—which sends out alerts of unfolding terror attacks, political unrest and other potentially important events—isn’t directly provided by Twitter, but instead by Dataminr Inc., a private company that mines public Twitter feeds for clients. Twitter owns about a 5% stake in Dataminr, the only company it authorizes both to access its entire real-time stream of public tweets and sell it to clients.” (Christopher S. Stewart and Mark Maremont, “Twitter Bars Intelligence Agencies From Using Analytics Service,” [The Wall Street Journal](#), 5/8/16)
- **In December 2016, Dataminr was under fire by the ACLU for servicing domestic spy centers, also known as fusion centers.** “As of this week, Twitter has made sure that federally funded fusion centers can no longer use a powerful social media monitoring tool to spy on users. After the ACLU of California discovered the domestic spy centers had access to this tool, provided by Dataminr (a company partly owned by Twitter), Dataminr was forced to comply with Twitter’s clear rule prohibiting use of data for surveillance.” (Nicole Ozer, “Twitter Cuts Off Fusion Spy Centers’ Access to Social Media Surveillance Tool,” [ACLU of California](#), 12/15/16)

The CA-ACLU of California discovered that an LA-area fusion center, was using Dataminr and had access to the company’s powerful Geospatial Analysis Application that enables keyword searches and location-based tracking and emphasized it is more “important than ever to protect against an expanding web of surveillance”:

- **The Guardian:** “ACLU investigation revealed fusion centers could access monitoring tech to target activists and journalists while racially profiling people deemed ‘suspicious’” (Sam Levin, “Twitter blocks government ‘spy centers’ from accessing user data,” [The Guardian](#), 12/15/16)
- **Dataminr was “clearly violating Twitter’s policy prohibiting the use of its data for surveillance, according to the ACLU” by giving government agencies access to these tools.** “By giving

government agencies access to these tools, Dataminr was also clearly violating Twitter’s policy prohibiting the use of its data for surveillance, according to the ACLU.” (Sam Levin, “Twitter blocks government ‘spy centers’ from accessing user data,” *The Guardian*, 12/15/16)

- **ACLU:** “These domestic spy centers—local-state-federal partnerships that aim to collect and analyze vast amounts of information to connect the dots about ‘threats’—have a history of sweeping in constitutionally protected political, religious, and artistic activity.” (Nicole Ozer, “Twitter Cuts Off Fusion Spy Centers’ Access to Social Media Surveillance Tool,” [ACLU of California](#), 12/15/16)
- **ACLU:** “These spy centers also gather information about innocent people deemed ‘suspicious’ by law enforcement – people like ACLU client Tariq Razak, a ‘male of Middle Eastern’ descent who was waiting in a train station for his mother to use the restroom.” (Nicole Ozer, “Twitter Cuts Off Fusion Spy Centers’ Access to Social Media Surveillance Tool,” [ACLU of California](#), 12/15/16)
- **New York Post:** “In addition to location-based tracking, Dataminr had been enabling law enforcement since March to do keyword searches to monitor specific demographics and organizations, the ACLU found.” (Post Staff Report, “Twitter yanks spy agencies’ access to Dataminr,” [New York Post](#), 12/16/16)

In response to the ACLU’s criticism, Twitter ensured that federally funded fusion centers could “no longer use a powerful social media monitoring tool to spy on users”:

- **In response to the ACLU’s criticism, Twitter ensured that federally funded fusion centers could “no longer use a powerful social media monitoring tool to spy on users.”** “As of this week, Twitter has made sure that federally funded fusion centers can no longer use a powerful social media monitoring tool to spy on users.” (Nicole Ozer, “Twitter Cuts Off Fusion Spy Centers’ Access to Social Media Surveillance Tool,” [ACLU of California](#), 12/15/16)
 - “After the ACLU of California discovered the domestic spy centers had access to this tool, provided by Dataminr (a company partly owned by Twitter), Dataminr was forced to comply with Twitter’s clear rule prohibiting use of data for surveillance.” (Nicole Ozer, “Twitter Cuts Off Fusion Spy Centers’ Access to Social Media Surveillance Tool,” [ACLU of California](#), 12/15/16)
 - “...our long-standing position has been that the use of Twitter data for surveillance is strictly prohibited, and we continue to expand our enforcement efforts.” (Letter from Colin Crowell, Vice President, Global Public Policy, [Twitter](#), 12/12/16)
 - “We have shared our concerns with Dataminr regarding fusion centers. In light of these concerns, Dataminr will no longer support direct access by fusion centers, and has informed us that any accounts accessible by fusion center email addresses have been notified that their access is now terminated.” (Letter from Colin Crowell, Vice President, Global Public Policy, [Twitter](#), 12/12/16)