

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT DEPARTMENT

No. _____

SHAWN MUSGRAVE
and NASSER ELEDROOS

Plaintiffs,

v.

CLERK OF THE SUPERIOR COURT FOR
CRIMINAL BUSINESS IN SUFFOLK COUNTY,
in her Official Capacity; THE OFFICE OF THE
ATTORNEY GENERAL, and THE OFFICE OF
THE SUFFOLK COUNTY DISTRICT
ATTORNEY,

Defendants.

AFFIDAVIT OF SHAWN MUSGRAVE

I, Shawn Musgrave, hereby depose and state as follows.

1. I am an investigative journalist, and a plaintiff in the above-captioned matter. I make this affidavit on personal knowledge in support of plaintiffs' Motion to Terminate Impoundment.

2. Attached hereto as Exhibit 1 is a true and correct copy of an order issued by the Superior Court in *In re Administrative Subpoena to Twitter, Inc.*, SUCR2011-11308. Attached to the order is a copy of an administrative subpoena issued by the Office of the District Attorney for Suffolk County to Twitter, Inc.

3. Attached hereto as Exhibit 2 are true and correct copies of news articles regarding the administrative subpoena and a proceeding challenging its enforcement.

4. Attached hereto as Exhibit 3 is an article I wrote for muckrock.com dated April 6, 2015, concerning the monitoring of social media accounts by a Texas police department.

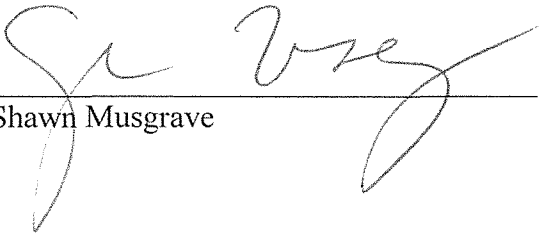
5. Attached hereto as Exhibit 4 is an article I wrote for muckrock.com dated July 13, 2015, concerning a 2008 report commissioned by the Army on terrorism and social media.

6. Attached hereto as Exhibit 5 is an article I wrote for the *Boston Globe* dated February 24, 2016, concerning the use of covert cellphone trackers by the Boston Police Department.

7. Attached hereto as Exhibit 6 is are two articles concerning a recent summons issued by the Department of Homeland Security to Twitter, Inc., seeking the identity of persons behind an account called “@ALT_uscis.”

8. On May 15, 2017, I went to the Criminal Clerk’s Office at the Suffolk Superior Court and asked to view the case file in *In re Administrative Subpoena to Twitter*, 2011-CR-11308. After multiple attempts to locate information on the case, an assistant clerk told me that no case with that docket number exists.

Signed under the pains and penalties of perjury this 26th day of June, 2017,


Shawn Musgrave

1

FILED UNDER SEAL

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, S.S.

SUPERIOR COURT DEPARTMENT
DOCKET NO. SUCR2011-11308

IN RE: ADMINISTRATIVE SUBPOENA TO
TWITTER, INC.
(IMPOUNDED CASE)

EX PARTE ORDER TO SHOW CAUSE

AFTER HEARING,
TWITTER, INC IS ORDERED
TO COMPLY WITH THE

ATTACHED SUBPOENA AS
AMENDED BY 4:00 PM E.S.T.
ON FEBRUARY 28, 2012

TO: Twitter, Inc.
ATTN: Ben Lee — blee@twitter.com
795 Folsom Street, Suite 600
San Francisco, CA 94107
Facsimile: 415-222-9958

James G. McInnis
2-27-2012

Twitter, Inc. is hereby ORDERED to:

Appear in the First Session of the Suffolk Superior Court (Courtroom 704), located at 3 Pemberton Square, Boston, MA 02114 at 9:00 AM February 27, 2012 and SHOW CAUSE why Twitter, Inc. should not be held in contempt for failure to comply with the attached subpoena issued on December 14, 2011 pursuant to G.L. c. 271, § 17B.

~~Pursuant to 18 U.S.C. § 2705(b), Twitter, Inc. is hereby further ORDERED, pending further order of this Court, not to notify any other person, including John Doe (a/k/a Guido Fawkes) and his legal representatives of the existence of this court order~~

SO ORDERED,

James G. McInnis
JUSTICE, SUFFOLK SUPERIOR COURT

February 23, 2012

2-23-12
filed

This Filing (all three pages)
is no longer impounded.

McInnis, J.
2 1 2012



The Commonwealth of Massachusetts

DISTRICT ATTORNEY OF SUFFOLK COUNTY

DANIEL F. CONLEY

Special Prosecutions Unit
One Bulfinch Place
Boston, MA 02114-2997

Telephone: (617) 619-4106
Fax: (617) 619-4100

ADMINISTRATIVE SUBPOENA

December 14, 2011

BY FACSIMILE ONLY — 415-222-9958

Twitter, Inc.
c/o Trust and Safety
795 Folsom Street, Suite 600
San Francisco, CA 94107

Dear Sir or Madam,

Pursuant to an official criminal investigation being conducted by the Suffolk County District Attorney's Office and the Boston Police Department, demand is hereby made pursuant to Massachusetts General Laws Chapter 271, Section 17B and 18 U.S.C. § 2703 that your company furnish within 14 days the following:

All available subscriber information, for the account or accounts associated with the following information, including IP address logs for account creation and for the period **December 8, 2011 to December 13, 2011**:

Guido Fawkes
@p0isAn0N
@OccupyBoston
#BostonPD
#d0xcak3 (z)

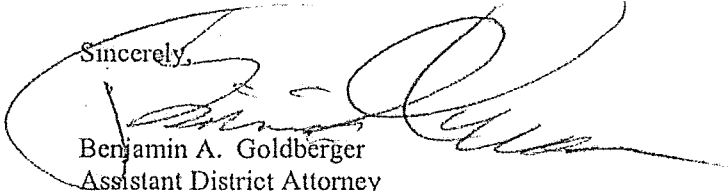
"Subscriber information" is defined by 18 U.S.C. § 2703(c)(1)(E). Please do not send any content of electronic communications in response to this request. Per Massachusetts General Laws Chapter 271, Section 17 B, no common carrier or employee shall be civilly or criminally responsible for furnishing any records or information in compliance with this request.

In order to protect the confidentiality and integrity of the ongoing criminal investigation, this office asks that you not disclose the existence of this request to the subscriber as disclosure could impede the ongoing criminal investigation.

Please forward the records to the attention of ADA Benjamin Goldberger / Sgt. Det. Joseph Dahlbeck by email to benjamin.goldberger@state.ma.us and DahlbeckJ.bpd@cityofboston.gov. Records may also be sent by facsimile or regular mail to the above address.

Thank you for your assistance with this matter.

Sincerely,


Benjamin A. Goldberger
Assistant District Attorney

2

U.S. +

Live TV

subpoenaed

By Leigh Remizowski, CNN

🕒 Updated 6:38 PM ET, Thu December 29, 2011

Story highlights

Massachusetts prosecutors seeking Twitter records of Occupy activist

ACLU calls it a violation of the First Amendment

In private hearing, judge impounds all documents pertaining to the case

Prosecution spokesman says he cannot comment

A decision by Massachusetts prosecutors to subpoena the Twitter records of an Occupy Boston activist, as well as records linked to two Twitter hashtags, has free speech advocates up in arms, calling the move a violation of the First Amendment.

Suffolk County prosecutors demanded that Twitter hand over information posted on the social media website by user "Guido Fawkes," whose Twitter handle is @p0isAn0N, as well as information from the user behind @OccupyBoston and those who Tweeted #BostonPD or #d0xcak3, according to the document.

The ACLU gave CNN a copy of the subpoena.

"There is a constitutional right to write things on the Internet," said Peter Krupp, an attorney with the ACLU of Massachusetts who is representing the person using the Twitter handle Guido Fawkes. "There is a constitutional right to do that anonymously."

A Suffolk County Superior judge held a private hearing Thursday and impounded all documents pertaining to the case, according to Krupp, who said he could not divulge what happened during the session.

Krupp said he had requested that the meeting be open to the public.

"Secret court proceedings, particularly proceedings involving First Amendment issues, are troubling as a matter of both law and democracy," said Carol Rose, executive director for the ACLU of Massachusetts, in a statement.

Suffolk County District Attorney spokesman Jake Wark said that, since Thursday's court proceeding was not public, prosecutors could not comment on the hearing.

"We investigate and prosecute criminal acts," Wark said. "We have no interest in investigating political speech or political opinions."

In the subpoena, which was issued on Dec. 14, prosecutors requested that Twitter release to them "all available subscriber information," including IP address logs for the time period between Dec. 8 and Dec. 13 as part of an "official criminal investigation."

Those dates coincide with clashes between protesters and police in Boston's Dewey Square. Dozens of protesters were arrested after refusing to leave the public space after being ordered to do so by Boston's mayor, Thomas Menino.

Wark would not elaborate on the nature of the criminal investigation, but said Thursday that "no charges have been brought against any individual."

U.S. +

Live TV

Subpoenaing Twitter records is becoming more common, according to lawyer Ethan Wall, of the Richman Greer law firm in Miami. Wall, who specializes in intellectual property litigation, said the practice could have "a chilling effect on free speech."

"We are in this information-accessible age where we can post anything and everything from anywhere on any device," Wall said. "Because it's so easy I don't think that people put the thought into how this might affect them personally, professionally or legally."

Henry J. Cittone of Cittone & Lindenbaum LLP, an intellectual property law firm in New York, said the most troubling part of the case is that prosecutors are subpoenaing hashtags, meaning that anyone who Tweeted or re-Tweeted #BostonPD or #d0xcak3 could be exposed during the investigation.

"It looks like authorities are trying to build lists of protestors by using hashtag information, as opposed to going after actual criminals -- which would have been the proper focus of such an investigation," Cittone said.

Krupp called the subpoena "wildly over-broad," pointing out that requesting records of two Twitter handles -- @p0isAn0N and @OccupyBoston -- could affect thousands.

"That's not just subscriber information for those accounts, but presumably followers," he said.

Twitter did not respond to requests for comment. A posting on its website says: "We may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation or legal request; to protect the safety of any person; to address fraud, security or technical issues; or to protect Twitter's rights or property."

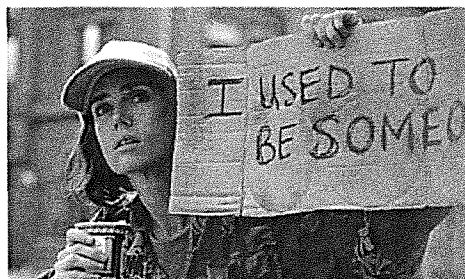
Paid Content

Recommended by



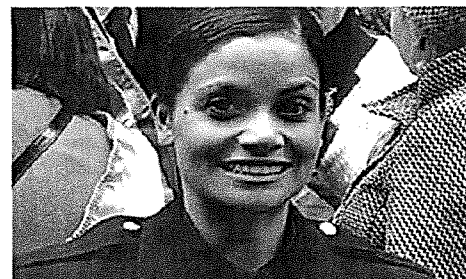
How To Make Sense of SPFs and Sun Safety

The Ohio State University



13 Celebs Now Working Regular Jobs

Post Popular



Female Cop Hid Her Double Life For 7 Years

Wife Wine - Wife It Up



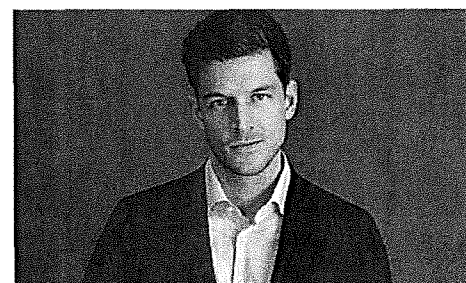
Explore The New Lincoln Navigator

Yahoo! Search



It Seemed Like They Were Alone, But The Deputy Didn't Know There Was A Camera

Scribol



Why This Shirt Company Is Causing so Many Guys to Switch

GQ

U.S. +

Live TV

Angelina Jolie's New Go-To Travel Shoe Is Surprisingly Affordable *Vogue*

Whatever Happened to Debra Jo Rupp After That 70's Show? *Definition*

What's the Secret of These Luxury Sheets' Success? Find Out Here *Brookline*

Rare Historical Photos You Won't Find In History Books *Standard News*

Former NFL WR James Hardy III Found Dead at Age 31

Michael Oher Deletes Instagram Post Appearing to Show Pills 'All...

Convicted sex offender moves next door to his victim. And it's...

5 cool things DNA testing can do

Recommended by



Trinidad: History, geography, and condiments

0 comments

Sign in

Newest | Oldest | Hot Threads

Powered by Livefyre

U.S. +

Live TV

QUINN NORTON SECURITY 12.30.11 4:00 PM

BOSTON D.A. SUBPOENAS TWITTER OVER OCCUPY BOSTON, ANONYMOUS



@p0isan0n's Twitter icon, the Antisec oenophile

ON DECEMBER 14, Twitter received a bizarre subpoena from the District Attorney of Suffolk County, which includes Boston.

It requested "All available subscriber information, for the account or accounts associated with the following information, including IP address logs for account creation and for the period December 8, 2011 to December 13, 2011." The named targets included two hashtags, two accounts, and one proper name:

Guido Fawkes
@p0isAn0N
@OccupyBoston
#BostonPD
#d0xcak3

That subpoena, as written, ostensibly asks for whatever identifying information Twitter has on anyone who used the hashtags #bostonpd and #d0xcak3 from 12/8/2011 to 12/14/2011, which could number in the thousands.

[bug id="occupy"]It's unclear if that's what the Boston police meant to do, or if they are unfamiliar with Twitter. It seems likely the latter, given that the @occupyboston account is a year-and-a-half old fallow account with four tweets. The quasi-official Twitter account for the Occupy Boston movement that was evicted in this time frame is @occupy_boston.

@p0isan0n purports to be a participant in Antisec, the blackhat wing of Anonymous, which has targeted the Boston Police several times in document releases that have included online logins, physical addresses, and most recently, payroll information for 40 senior officers. The subpoena may also be related to the d0xing, or document publication, of Boston Mayor Tom Menino on December 9th, as tweeted by @youranonnews:

"Boston Mayor Tom Menino d0x'd, courtesy of @DoxCak3 —
<http://pastebin.com/JtFqDr7G> #OccupyBoston << someone order the man a pizza, stat!"

If so, the district attorney's office mixed up their # and @ symbols.

The subpoena also includes a request for confidentiality from the Special Prosecutions Unit, but had no actual legal gag order. Without legal orders, the request for

confidentially had no more enforceability than if Assistant District Attorney Benjamin Goldberger had also asked Twitter to send him a cupcake.

It's Twitter's policy to forward a subpoena to its target in order to give the user a chance to fight it, unless the company is specifically gagged. It appears that @p0isan0n received a copy from Twitter and posted it to Scribd.

ACLU attorney Peter Krupp, who is representing user @p0isan0n, filed a motion to quash the subpoena on First Amendment grounds. But Thursday, the ACLU seemed to be dealt a defeat when Suffolk Superior Court Judge Carol Ball issued an impoundment order after hearing the case in whispers at the bench.

This barred anyone in the case from talking about the arguments on either side, or about why the motion to dismiss the subpoena was likely rejected. Impoundment is an extraordinary measure that can be requested by one side of a case, and is generally granted only in cases involving sensitive security issues, investigative issues, witness intimidation, or the possibility of the suspect running.

"I think none (of these reasons) are valid in this instance," said Krupp.

For its part, the Boston Police told Boston local publication BostInno that the "Boston Police Department is investigating serious threats directed at department personnel. The department will not disclose the specific nature of the intelligence gathered relative to this matter."

But what does it mean to subpoena a hashtag?

Krupp has a scary interpretation: "Presumably that means the IP address of anyone that uses that hashtag. It's all IP address logs associated with that Twitter address."

That would mean Twitter would be required to turn over the IP addresses and e-mail addresses of anyone who used the hashtag #BostonPD from December 12 to 14, a time period covering the widely followed eviction of Occupy Boston from Dewey park.

Krupp also sees a fishing expedition in the phrasing of "for the account or accounts associated with the following information". That, he believes, could mean anyone that's a follower of that account.

"In my view the statute... doesn't go nearly so far in permitting an administrative subpoena to get that information," Krupp said. "You have to go to a court and prove you're entitled to that stuff."

If the D.A. has this liberal interpretation of the subpoena, your humble Wired reporter is included for the incriminating act of following someone on Twitter.

Photo: floordje/Flickr

Correction: The story was updated to reflect that the hearing was comprised mostly of attorneys conferring with the judge.

**Breaking** ^{Comments} Live: Verdict in Bella Bond trial

Twitter gives Boston police, prosecutors data in hacking probe



0

By John R. Ellement | GLOBE STAFF MARCH 01, 2012

Social media giant Twitter handed over subscriber information today for one Twitter account indirectly tied to the Occupy Boston protest, ending a court battle fought behind closed doors as Boston law enforcement investigated hacking attacks on the Boston police and a police union.

The administrative subpoena was first sent to Twitter last December requesting information on the following Twitter subscriber accounts and hashtags: Guido Fawkes, @pOisAnON, @OccupyBoston, #BostonPD and #dOxcak3.

In the Dec. 14 letter, a prosecutor in Suffolk District Attorney Daniel F. Conley's office told Twitter the information was needed to assist law enforcement in an "official criminal investigation."

According to Twitter spokesman Matt Graves, the company provided the subscriber information for @pOisAnON, an account that is associated with the name of Guido Fawkes. “We provided information on a single user,” Graves said in a telephone interview today.

Get **Fast Forward** in your inbox:

Forget yesterday's news. Get what you need today in this early-morning email.

Enter email address

Sign Up

Graves declined comment when asked how Twitter responded to the court's order requiring the company to hand over information linked to hashtags and @OccupyBoston.

But Jake Wark, spokesman for Suffolk District Attorney Daniel F. Conley, said prosecutors are satisfied with Twitter's response to the court order.

“Twitter's recent communication with our office gave both parties a clear understanding of what information was relevant to our probe. We

requested and received only that information,” Wark said in an email. “This is a focused investigation, not a fishing expedition.”

Attorney Peter Krupp and the American Civil Liberties Union have fought the request by prosecutors in Suffolk Superior Court, where court records were impounded and court hearings were held out of earshot of the public in recent weeks.

But Superior Court Judge Frances McIntyre last week ruled against the ACLU’s efforts. She ordered Twitter to hand over the information this week, and Twitter has complied with the judge’s instructions.

Speaking for the ACLU, Krupp said yesterday they continue to believe that the constitutional rights of their client, who uses the Twitter name of Guido Fawkes, are being violated. The ACLU also wants the entire case file to be made available to the public; only McIntyre’s order and the subpoena have been unsealed.

“We continue to believe that our client has a constitutional right to speak, and to speak anonymously,” Krupp said, adding that the request by prosecutors “infringed our client’s rights under the First

He said there will be no more legal fights on behalf of Guido Fawkes because Twitter has provided the information to law enforcement officials.

Prosecutors and Boston police have not publicly disclosed the focus of the criminal inquiry.

Wark said that prosecutors are not targeting those who participated in the Occupy Boston takeover of Dewey Square, some of whom were arrested by police when the makeshift campground was shut down in December.

“The relationship between this investigation and Occupy Boston is tangential at best,” Wark said. “The charges arising out of the Dewey Square protest have already been addressed by the court. [Any media report] that links this investigation to the protest movement has been, and will continue to be, completely erroneous.”

During the past several months, the main police website and the website for the Boston Police Patrolmen’s Association have been targeted by computer hackers, some of whom claimed to have acted on behalf of Occupy Boston protesters.

John R. Ellement can be reached at element@globe.com.

0 COMMENTS

Twitter Share 0

3



Sign Up

Log In

Newsletter

Want the latest investigative and FOIA news?

email address

Subscribe



April 6, 2015

Share

Police in Texas regularly monitor social media - with no policies to limit its use

"I found this on one of the guys I monitor on Facebook ... Think you know anyone we could get it to?"

Written by Shawn Musgrave

Edited by JPat Brown

One morning last September, Officer Evan Ratcliff of the Round Rock Police Department in the Austin suburbs found something online that he wasn't quite sure what to do with.

From: Evan Ratcliff [mailto:eratcliff@roundrocktexas.gov]
Sent: Wednesday, September 03, 2014 11:36 AM
To: Pearson, Amber
Subject: RE: It's meeeeeeeee

I found this on one of the guys I monitor on Facebook. I called Garland and they have no record of a shooting. Think you know anyone we could get it to?

<https://www.facebook.com/██████████>

TAGS

agency manual

social media monitoring

texas

RELATED REQUESTS

Completed

152 files

Austin Regional Intelligence Center documents referencing ISACs

Evan Anderson sent this request to the Austin Regional Intelligence Center of Texas

[Sign Up](#)[Log In](#)

have no record of a shooting. Think you know anyone we could get it to?”

Ratcliff then pasted a link to the man’s Facebook profile at the bottom of his email.

The Austin Police Department provided the email — including the full Facebook URL — in response to a records request submitted by MuckRock user Evan Anderson. We have redacted the URL above and in documents posted online.

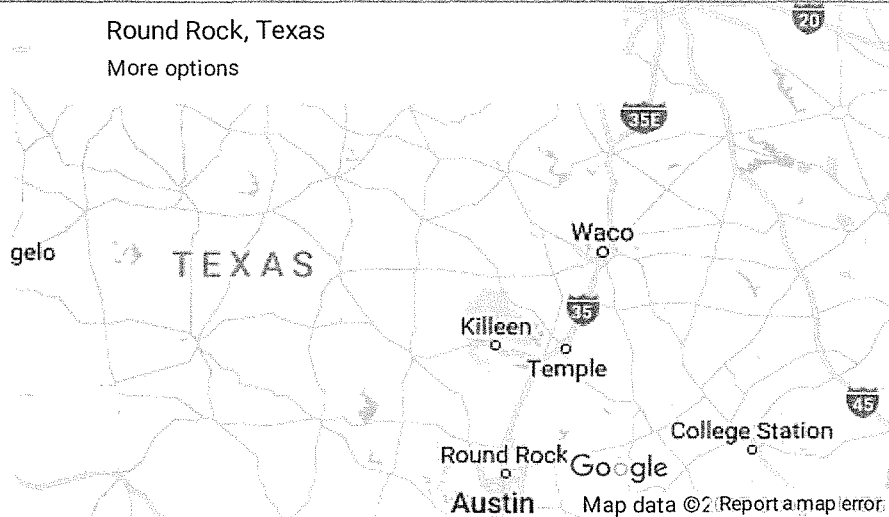
This casual email exchange between two police officials gives a rare look into the role that social media can play in modern policing. Barring restrictive privacy settings, there are few legal or practical limitations on monitoring an individual’s social media posts or retaining such information for future investigations.

But it’s unclear how this particular man’s online postings came to be monitored in the first place. For those less familiar with Texas geography, approximately two hundred miles separate Round Rock from Garland, where the man lived at the time of Ratcliff’s email.

Officer Ratcliff didn’t include the photo or post that caught his eye, nor did he respond to questions regarding how many individuals he monitors via Facebook.

A spokesperson for Round Rock Police Department defended monitoring the man’s account, saying that he “was known in our area for criminal activity and actively posted pictures of firearms and other illegal items.”

The spokesperson declined to provide further details of such illegal items, or how officers could tell whether firearms in the man’s photos were illegally obtained. Texas has no registration requirement for firearms, although its gun laws do require a permit to carry concealed handguns. (Also, a few million people post about guns on Facebook, and a few of them must live within a two-hundred mile radius of Greater Austin.)

[Sign Up](#)[Log In](#)

“Our top priority is ensuring officer safety and above all the safety of the public,” explains Angelique Myers of RRPD. “By using social media, we are able to learn more about possibly dangerous individuals we could potentially encounter and how to best prepare when that occurs.”

A patrol officer with RRPD since 2008, Ratcliff is also a SWAT member and the coordinator for his department’s automated license plate recognition (ALPR) program. On his LinkedIn, Ratcliff describes his approach as “intelligence-based policing.”

But neither Ratcliff or his Austin correspondent knew where to call next with this particular Facebook finding.

“I don’t have a personal contact up there, but this is a list of all of the fusion centers,” Amber Pearson wrote back. As promised, she attached the contact information for all fusion centers nationwide. Pearson’s list includes the Austin Regional Intelligence Center (ARIC) and the Dallas Fusion Center, the one nearest to Garland.

[Sign Up](#)[Log In](#)

MuckRock received no response from the man himself. A review of his public Facebook profile — which has limited privacy restrictions — did not uncover any posts related to a shooting.

Combing over public posts does, however, reveal a wealth of information about this man's whereabouts, his relationships and off-handed thoughts. Together, these give a detailed glimpse into his day-to-day and personality alike.

In the past six months since Officer Ratcliff emailed his profile link, the man posted photos of adorable children alongside a location-tagged video of himself making "purple drank."



Sign Up

Log In



He also posted location-tagged updates from a courthouse, the gym, a smoke shop and a friend's home.

Anyone — civilian or law enforcement alike — could piece together these incredibly personal details. As this information is available to anyone who knows this man's profile is public, some law enforcement agencies see no need to restrict how agents collect it.

"We do not have a current policy that details the use of social media in investigations," replied RRPD's spokesperson, "due to the fact that it is public information that is freely accessible."

The department's lack of a policy raises questions about privacy protections and the need for clear guidelines around how law enforcement are able to access, retain and aggregate information posted on the open web. In coming weeks, MuckRock will ask agencies nationwide regarding their own policies and procedures for using social media as an investigative tool.

4



Sign Up

Log In

Newsletter

Want the latest investigative and FOIA news?

email address

Subscribe



July 13, 2015

Share

2008 report warned of MySpace and Second Life as jihadist recruitment tools

TAGS

internet isis myspace terrorism

“How a Boy Becomes a Martyr: The Dangers of Web 2.0 Technology”

Written by Shawn Musgrave

Edited by JPat Brown

Terrorism analysts have noted how savvy the Islamic State is on social media. The White House and think tanks alike point to Twitter support for ISIS as a key metric for the group's strength. Similar worries once swirled around MySpace and Second Life as platforms for recruiting homegrown jihadists.

A 2008 report commissioned by the Army envisions how a mastermind halfway around the world might leverage social networks for terrorism. In the fictional case study, a jihadist targets a lonely Detroit teenager via MySpace, connects the boy with a sleeper cell, trains him on Second Life for weeks, and orchestrates a suicide attack that kills dozens of people.

RELATED REQUESTS

No Responsive Documents

1 file

Urban Warfare Analysis Center (UWAC) contracts — DCMA

Shawn Musgrave sent this request to the Defense Contract Management Agency of the United States of America

No Responsive Documents

5 files

Urban Warfare Analysis Center (UWAC) reports

[Sign Up](#)[Log In](#)

United States or America

Scope Note

The following report is a fictitious account of how a young person in America could become a suicide bomber for an Islamic extremist group. It is the fifth in a series of reports on Web 2.0 technology and future urban warfare. All references to people, groups, and products are intended for illustrative purposes only. As such, the authors do not suggest that any of the products or organizations listed condone or support extremist activities.

Pete is a 16-year-old boy in Detroit who is moody and depressed. He lacks a stable home life, is socially awkward at school, and has no clear direction in life. Like many teens around the world, he finds solace in friendships made online through social networking sites.

The report, "How a Boy Becomes a Martyr: The Dangers of Web 2.0 Technology", was posted online in 2010 by the Public Intelligence website. It was compiled by the Urban Warfare Analysis Center, a now-defunct "dedicated center of excellence" sponsored by the U.S. Army Research Laboratory and run by a military contractor.

Notably, the report came out four months after Facebook overtook MySpace as the top social network worldwide.

To print the document, click the "Original Document" link to open the original PDF. At this time it is not possible to print the document with annotations.

[Sign Up](#)[Log In](#)

Its six pages spin a wildly improbable yarn about technology's appropriation by murderous zealots. The report proposes no solutions or assessment as to its feasibility, but offers only "a fictitious account of how a young person in America could become a suicide bomber for an Islamic extremist group."

We open on Pete, a 16-year-old in Detroit who is "socially awkward" and in need of a father figure. Jafar, a jihadist living in Lebanon, sends Pete a friend request from his own MySpace account and several fake ones, and introduces the young man to Islam. Unbeknownst to his friends and family, Pete is soon spending hours online socializing with Jafar and a global Muslim community.

The report neglects to note whether Jafar makes Pete's top 8. We quickly pivot from MySpace to Second Life, where Pete creates an avatar "with dark skin and stylish clothes" to make himself appear Middle Eastern. Jafar steers Pete toward Muslim spaces within Second Life, and encourages his moldable protege to make the Virtual Hajj to the replicated Mecca.

Pete is unaware that Jafar controls many of the avatars he meets inside Second Life. The terrorist mentor stages a conversation on the topic of jihad within earshot of Pete, and soon puts the teenager in touch with a band of radical jihadists living just outside Detroit. Now radicalized himself, Pete resolves to carry out an attack.

"Pete feels like a champion," the report summarizes of Pete's excitement at being chosen for jihad. "He finally won at something."



Sign Up

Log In

of 1,000 new Muslims. "You even express disappointment that he was not picked because he has been trying for many years. Pete feels like a champion. He finally won at something."

Meanwhile, the local professional basketball team is winning many games and attracting large crowds. Their schedule is also posted on the team's website. The target for the attack is now selected: a packed house at an upcoming home game.

UWAC © 2008. All Rights Reserved. For Official Use Only. 4

Jafar settles on the stadium for "the local professional basketball team" as the target. (Note that the report cites MySpace and Second Life by name, but not the Pistons. Even I know the Pistons play in Detroit.)

Second Life facilitates Pete's training and prep for the attack, from "an exact three-dimensional virtual blueprint" of the arena constructed by rabid fans of "local professional basketball" for training to "a virtual ticket booth" to purchase tickets. Pete rehearses the attack over 200 times on a private virtual island inside the game.

On the fateful day, Jafar leads Pete to a secret location inside Second Life, where he "is welcomed as a champion by what seems like thousands of Muslims." Once again, all of these adoring fans are bots controlled by Jafar as part of the plot.

Pete straps up with a martyr vest, sneaks inside the arena according to plan, and takes his seat at midcourt. He stands and detonates just after opening tip off while screaming "Allahu Akbar!"

Other blasts go off simultaneously, each planted by coordinated teams who were also trained inside Second Life without ever having met each other.

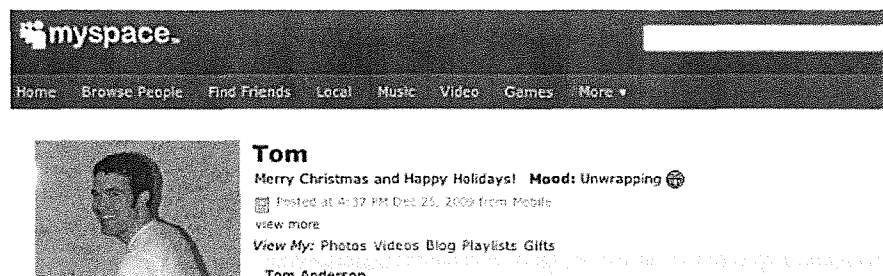
"Only Jafar knew the entire plan," the report emphasizes.

UWAC © 2008. All Rights Reserved. For Official Use Only. UNCLASSIFIED

One week later, Jafar and several associates meet inside Second Life to review all stages of the attack. They study many hours of film footage on police actions provided by national news stations. At the same time, Jafar notices a new avatar in Second Life that has taken a particular interest in Pete's story. His MySpace profile states that he is a 15-year-old male from California named Tom...

[Sign Up](#)[Log In](#)

year-old in California, who of course, just happens to be named Tom.



This is just one of several reports produced by the Urban Warfare Analysis Center on government contract. Other UWAC titles include:

- “Cell Phone Use by Insurgents in Iraq”
- “Threat Analysis: Hamas and Hezbollah Sleeper Cells in the United States”
- “Web 2.0 and Enemy Recruitment”
- “Virtual Worlds and their Implications for Urban Warfare”
- “Virtual Worlds and Terrorist Attack Planning”

MuckRock has requested all UWAC reports, as well as contracts between the UWAC contractor and the Army.

Where policy experts, military officials and community leaders are now tackling Twitter as a terrorist tool and a powerful means of countering extremist ideologies, there is scant evidence that earlier social networks aided jihadists in training.

Related Stories

5



Comments
Breaking: Supreme Court to review Trump travel ban

Public kept in the dark about BPD's use of covert cell trackers

Deployment of devices that intercept signals raises concerns

57

By Shawn Musgrave | NEW ENGLAND CENTER FOR INVESTIGATIVE REPORTING FEBRUARY 24, 2016

The Boston Police Department is keeping the public largely in the dark about how it uses covert cellphone trackers — devices that have raised civil liberties questions across the country.

The department declined to provide details about how the trackers are used in the field, saying that disclosing protocols or the types of cases that they are being used for would endanger lives. The trackers allow police to identify all phones at a given locale and to log the movements of handsets over time.

Other law enforcement agencies have provided details of tracker usage,

Tweet Share

57

to the New York Civil Liberties Union
that were made public this month. The documents showed that the NYPD had used the trackers at least 1,000 times since 2008, for investigations ranging from homicide and rape to identity theft and missing-person searches.

Documents obtained by the New England Center for Investigative Reporting under the state Public Records Law show the Police Department and the Suffolk district attorney's office have agreements with the Federal Bureau of Investigation not to disclose information about the trackers. The devices are also known as StingRays, the brand name of the most widely used models.

Get **Fast Forward** in your inbox:

Forget yesterday's news. Get what you need today in this early-morning email.

Enter email address

Sign Up

Under the pacts, police and prosecutors agreed not to provide information about the devices, even in court proceedings, without prior approval of the FBI. They also agreed to seek dismissal of a case, at the

FBI's request, rather than disclose sensitive information about them in court.

The US public defender's office in Boston, which represents indigent defendants in federal prosecutions, says that prior to a New England Center for Investigative Reporting story in November, it was unaware that any such agreement existed. The center revealed the Boston Police Department's use of the devices.

"The danger is that nondisclosure agreements foster mischief," said William Fick, an assistant US public defender. He said such agreements "create perverse incentives" for law enforcement and prosecutors to omit or misrepresent how they obtained information.

The Boston Police Department says it typically obtains search warrants to monitor cellphones. But detectives are not required to spell out in a warrant application that they intend to use a tracker in their search, a police spokesperson said.

Civil liberties advocates have argued that without knowledge that a tracker will be used, judges are less likely to put limits on warrants to keep police from gathering cellphone

The trackers are called cell-site simulators because they monitor mobile devices by mimicking cell towers. When the tracker is turned on, all cellular phones within range connect to it and transmit their location.

“Unless the use of a cell-site simulator is disclosed, a defendant cannot raise a legal or constitutional challenge seeking to suppress evidence on that basis,” Fick said.

Prosecutors “weighed both the public safety potential and the practical realities of the technology” before agreeing to the nondisclosure terms, said Jake Wark, a spokesman for the Suffolk district attorney. “There is an obvious public safety benefit to be able to quickly and accurately locate a person who is in danger or poses a threat.”

The agreement requires prosecutors and police to notify the FBI if any court proceeding might disclose sensitive information about the capabilities of cellphone trackers. Both parties agreed to seek dismissal of such cases at the FBI’s request.

Neither the police nor the district attorney has sought to dismiss a case on these grounds, Wark said.

The trackers don’t come cheap. Documents released to the New England Center for Investigative Reporting in early February include an

“

‘Unless the use of a cell-site simulator is disclosed, a defendant cannot raise a

April 2014 cost estimate for purchasing a variety of components from Harris Corp., the Florida-based manufacturer of StingRays.

challenge seeking to suppress evidence on that basis.'

William Fick, assistant US public defender

The \$333,910 price quote matches the sum of a series of entries in the city's online checkbook for police expenditures on July 8, 2014.

The Boston Police Department confirmed that it acquired the equipment in July 2014.

But the department has not answered inquiries about the particular device and possible components it purchased. The model number provided by the Police Department corresponds to the KingFish, a hand-held version of the StingRay tracker, made by Harris Corp.

Police purchased the equipment using a portion of an \$8.6 million grant from the Department of Homeland Security, according to Laura Oggeri, a spokeswoman for the Boston mayor's office.

Edward Callahan, head of the Police Department's technology bureau, told Boston City Councilor Ayanna Pressley in May that use of the trackers was subject to obtaining a warrant. They may be used without warrants when "exigent circumstances exist that require immediate law enforcement action." Callahan wrote in a letter to Pressley.

In 2015, Washington enacted a law that requires explicit search warrants for tracker use and includes provisions for police to minimize data collection from bystanders' cellphones. Similar laws have been enacted in Virginia, Minnesota, Wisconsin, and Utah.

The Justice Department amended its protocol in September to require a search warrant to track phones via cell-site simulators, instead of vague court orders. The Department of Homeland Security followed suit in October. Both policies now require federal agents to be explicit about what technology will be used in the search.

Judges may not have the same clarity when reviewing Boston police warrant requests. Lieutenant Michael McCarthy, a spokesman for the Police Department, said "there is no requirement" that affidavits in support of such requests "specifically indicate" that the trackers will be used.

He said he couldn't provide examples of cellphone tracking warrants.

Police must be explicit about how and when "they intend to conduct invasive electronic monitoring" to make sure people who aren't targets "aren't swept up in police spying operations," said Kade Crockford, who researches surveillance issues for the American Civil Liberties Union of Massachusetts.

The Suffolk district attorney's office has described cellphone trackers as a "tool that can protect and save lives by apprehending a violent fugitive or rescuing a kidnap victim."

But the local ACLU chapter says it's worried that police may be using trackers on routine criminal investigations.

Police officers in Baltimore used trackers in probes of murders and armed robberies, but also in low-level theft and harassment cases, according to a surveillance log released last year.

McCarthy said the Police Department has no list of tracker cases to provide, and declined to give any examples of their use.

"The types of cases can vary and the decisions to apply for its use are based on the circumstances of each individual case," McCarthy said.

The New England Center for Investigative Reporting (www.necir.org) is a nonprofit news outlet based at Boston University and WGBH (PBS/NPR) in Boston. New England Center for Investigative Reporting intern Amanda Lucidi also contributed to this report.

SHOW 57 COMMENTS

Stay updated, right in your news feed.

Like 482K

Top 10 Trending Articles

Twitter Share

57

- Could artists revive this fading Maine town?

Comments
- As a real estate rookie, Jared Kushner snapped up Somerville properties but also made mistakes
- MBTA to propose changes to retirement benefits
- Short-term corporate apartments adding to the strain on Boston’s housing market
- A lawsuit helps muzzle John Oliver — sort of
- It’s tourist season, and here come the monks
- 15 ways Harry Potter has changed culture since the first book was published 20 years ago
- Should these women be forced to call themselves 'selectmen'?
- Two Brighton homes, listed for \$1 apiece but lacking buyers, face demolition
- A teen falls 25 feet off a Six Flags ride — and a crowd catches her

My Account	Contact
Logout	Help
Manage my Account	FAQs
Mobile Customer Service	Globe newsroom
Sign Up For Newsletters	Advertise
Social	More
Facebook	ePaper
Twitter	News in Education

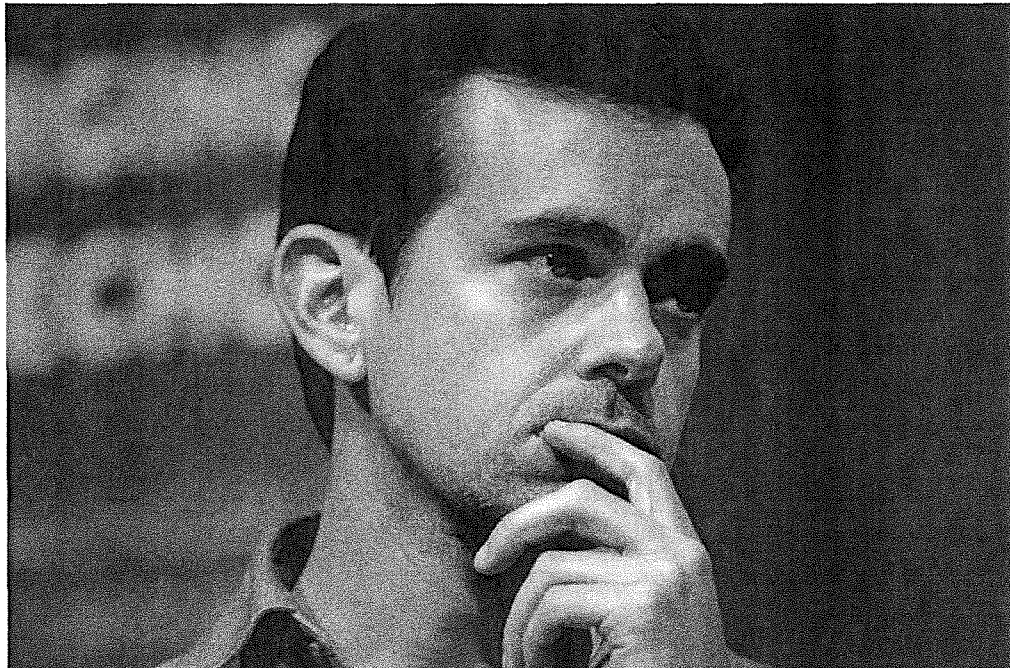
6

TWITTER

Twitter is suing the government for trying to unmask an anti-Trump account

The lawsuit filed Thursday contends the government is threatening free speech.

BY TONY ROMM | @TONYROMM | APR 6, 2017, 3:55PM EDT



Bill Pugliano / Getty

Twitter is suing the Trump administration after it tried to compel the social media site to reveal the identity of an account that had been tweeting criticism of the president.

In a lawsuit filed in the U.S. District Court in the Northern District of California, Twitter revealed that the Department of Homeland Security in March had demanded that the company reveal who is behind @ALT_USCIS, an anonymous account that has been raising alarms about U.S. Citizenship and Immigration Services and Trump's immigration policies.

Twitter contends the request amounts to an “unlawful” use of the government’s investigative powers, as the rules that allow customs and border officials to issue summonses generally relate to the import of merchandise, including counterfeit goods — not information involving online accounts.

In seeking to unmask that user anyway, though, Twitter says the government’s request “would have a grave chilling effect on the speech of that account in particular and on the many other ‘alternative agency’ accounts that have been created to voice dissent to government policies.”

A spokesman for DHS declined to comment, citing the fact it is pending litigation. Spokespeople for the Justice Department and White House also declined to offer their views on the case.

FROM OUR SPONSOR CONTINUE FOR MORE CONTENT



But Democratic Sen. Ron Wyden, an ally of Silicon Valley in Congress, blasted the Trump administration Thursday for its conduct. “The Department of Homeland Security appears to have abused its authority and wasted taxpayer resources, all to

uncover an anonymous critic on Twitter,” the Oregon lawmaker told **Recode** in a statement. He said the agency’s inspector general -- a watchdog that reviews for abuse — should “investigate to determine who directed this witch hunt.”

Since Trump has taken office, a number of “alt-agency” accounts — unofficial deviations from federal agencies’ verified online Twitter profiles — have started firing 140-character salvos at the new administration.

There are accounts for the Environmental Protection Agency and the Labor Department, for example, which have targeted Trump for his climate and employment policies. Some “rogue” staffers at the National Park Service even hijacked their official account to tweet criticism of the president around his inauguration, though NPS quickly reclaimed it.

In many cases, though, the authors of these accounts are not clear. “The users appear to view and depend on preservation of their anonymity as crucial to their ability to express information and ideas that are contrary to the policies and objectives of the Administration and its agencies,” as Twitter explains in its court briefing.

The @ALT_USCIS account arrived in late January, according to Twitter’s complaint, purporting to be the site of the “[o]fficial inside resistance” of USCIS. It began tweeting sharp rebukes of Trump’s immigration policies, including his support for a wall along the U.S.-Mexican border. And it soon alleged rampant mismanagement at the USCIS, pointing out a potential instance of lost green cards and poor behavior by customs agents.

On March 14, Twitter said an agent for the USCIS “transmitted to Twitter by fax a summons” that ordered it to produce records related to the alt-agency account. That information included names, addresses and phone numbers, Twitter said, along with a threat of additional sanctions if the company did not comply.

In the days to follow, Twitter said it informed the @ALT_USCIS accountholder of the government’s request — and the Trump administration of its plans to challenge the summons in court.

And on Thursday, the @ALT_USCIS also fired back:

Constitution of United States of America 1789 (rev. 1992)

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.



ALT Immigration
@ALT_uscis

Follow

3:52 PM - 6 Apr 2017

3,261 7,163

Twitter has a long history of defending free speech on its platform, sometimes to a fault (hence its issues around abuse and harassment). Late last year, Twitter reminded everyone that it's against the company's guidelines to use Twitter for surveillance purposes, claiming a "commitment to social justice is core to our mission."

Additional reporting by Kurt Wagner.



Subscribe to the Recode newsletter

Sign up for our Recode Daily newsletter to get the top tech and business news stories delivered to your inbox.

Your email

GO

By signing up you agree to our [terms of use](#).

BREAKING NEWS: Supreme Court grants Trump emergency request allowing parts of refugee ban to go into effect [view more](#)

EDITION: UNITED STATES

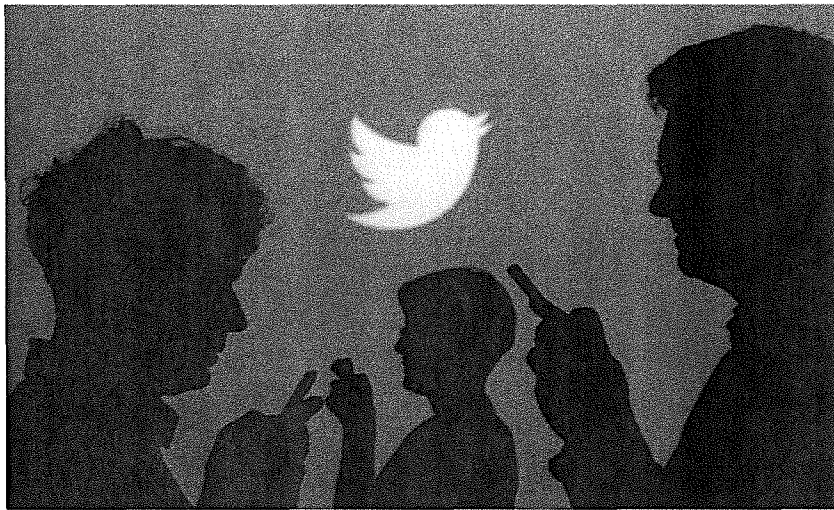
[Business](#) [Markets](#) [World](#) [Politics](#) [Tech](#) [Commentary](#) [Breakingviews](#) [Money](#) [Life](#)

Latest Venture Capital News

Malaysian Real Estate Portal The Edge Property Secures US\$14 million to customize user experience

TECHNOLOGY NEWS | Fri Apr 21, 2017 | 8:53pm EDT

U.S. Homeland Security probes possible abuse in Twitter summons case



FILE PHOTO: People holding mobile phones are silhouetted against a backdrop projected with the Twitter logo in this illustration picture taken September 27, 2013. REUTERS/Kacper Pempel/Illustration/File Photo

TRENDING STORIES

- 1 Exclusive: U.S. warship stayed on deadly collision course despite warning - container ship captain
- 2 Special Report: How the Federal Reserve serves U.S. foreign intelligence
- 3 Asylum seekers in Canada who fled Trump now trapped in legal limbo

BREAKING NEWS: Supreme Court grants Trump emergency request allowing parts of refugee ban to go into effect [view more](#)

The U.S. Homeland Security Department's inspector general said on Friday he was investigating possible abuse of authority in a case that triggered a lawsuit against the department by Twitter Inc ([TWTR.N](#)).

Inspector General John Roth described the probe in a letter to Senator Ron Wyden, an Oregon Democrat who had asked for an investigation due to concerns about free speech protections.

In a lawsuit on April 6, Twitter disclosed that it received a summons in March from the U.S. Bureau of Customs and Border Protection, an agency within Homeland Security, demanding records about an account on the social media platform identified by the handle @ALT_uscis.

The account has featured posts critical of President Donald Trump's immigration policies, leading Twitter to complain in its lawsuit that the summons was an unlawful attempt to suppress dissent.

The agency dropped its demand of Twitter the day after the suit was filed.

Customs bureau spokesman Mike Friel said on Friday that the bureau requested the inspector general's review and will fully support it.

The people behind the Twitter account have not disclosed their identities, but the use of "ALT" with a government agency acronym has led many to assume government employees were behind the tweets critical of Trump.

The lawsuit said the account "claims to be" the work of at least one federal immigration employee. USCIS is the acronym of United States Citizenship and Immigration Services, a component of Homeland Security.

ALSO IN TECHNOLOGY NEWS

Short of IT workers at home, Israeli startups recruit elsewhere

Facebook in talks to produce original TV-quality shows: WSJ

Roth's office is charged with investigating waste, fraud and abuse within Homeland Security. He wrote in his letter that he was looking at whether the summons to Twitter "was improper in any way, including whether CBP abused its authority."

"DHS OIG is also reviewing potential broader misuse of summons authority at the department," he added.

Wyden's office posted the letter online. A representative for Roth could not immediately be reached for comment. A Twitter spokeswoman declined to comment.

(Reporting by David Ingram; Editing by Tom Brown and Diane Craft)

Our Standards: [The Thomson Reuters Trust Principles](#)

NEXT IN TECHNOLOGY NEWS

Western Digital objects to SK Hynix participation in Toshiba chip unit sale



TOKYO Western Digital Corp has told Toshiba Corp that it will not agree to a sale of the Japanese conglomerate's prized memory chip unit to a preferred bidding consortium that includes rival chipmaker SK Hynix Inc.

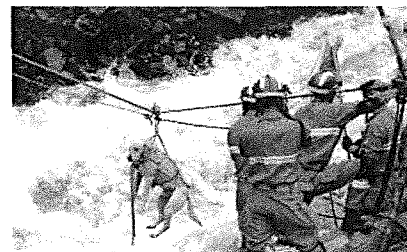
MORE FROM REUTERS

SPONSORED CONTENT

4 **rush to record output**

5 **'Pharma bro' Martin Shkreli heads into fraud trial**

PICTURES



Photos of the day