GlobalResearch
Center for Research on Globalization

Connections Between Michael Hastings, Edward Snowden And Barrett Brown—The War With The Security State

By Christian Stork

Theme: Intelligence

Global Research, August 08, 2013
WhoWhatWhy 7 August 2013

This article was originally published by WhoWhatWhy.

At the time of his death in a mysterious one-car crash and explosion, journalist Michael Hastings was researching a story that threatened to expose powerful entities and government-connected figures. That story intersected with the work of two controversial government critics—the hacker Barrett Brown and the on-the-run surveillance whistleblower Edward Snowden.

Any probe into Hastings's untimely death needs to take into account this complex but essential background.

But First, the Raw Facts

A little over 12 hours before his car was incinerated on an LA straightaway on June 18, 2013, Hastings sent out a short email headed, "FBI Investigation, re: NSA." In it, he said that the FBI had been interviewing his "close friends and associates," and advised the recipients — including colleagues at the website*Buzzfeed* — "[It] may be wise to immediately request legal counsel before any conversations or interviews about our news-gathering practices or related journalism issues." He added, "I'm onto a big story, and need to go off the radat [sic] for a bit."

> From: Michael Hastings
>
> Date: Mon, Jun 17, 2013 at 12:56 PM
>
> Subject: FBI Investigation, re: NSA
>
> To: [REDACTED] [REDACTED] [REDACTED]
>
> Hey [5 REDACTED WORDS] the Feds are interviewing my "close friends and associates." Perhaps if the authorities arrive "Buzzfeed GQ", er HQ, may be wise to immediately request legal counsel before any conversations or interviews about our news-gathering practices or related journalism issues.
>
> Also: I'm onto a big story, and need to go off the radar for a bit.
>
> All the best, and hope to see you all soon.

Michael

The next day, Hastings went “off the radar” permanently.

Here is a video that shows a lateral view of Hastings’s speeding car just before it crashed. (It shows at about 0.07.)

Following publication of the email by KTLA, the FBI quickly denied that the Bureau was ever investigating Hastings.

The Freedom of the Press Foundation and ProjectPM — the research wiki that Brown was involved with — are in the process of filing Freedom of Information Act (FOIA) requests to learn if indeed Hastings was the subject of an FBI probe.

The FBI denial notwithstanding, a number of clues indicate that the proximity of Hastings to Brown and the work of ProjectPM may have been what spawned the purported investigation in the first place.

Deep Background

When the FBI raided the Dallas home of journalist Barrett Brown in March 2012, the travails of the *Vanity Fair* and *Guardian* contributor didn’t get much ink — that is, until Michael Hastings published an exclusive on the Brown raid on *Buzzfeed*.

The story included a copy of the search warrant that revealed why the government was so interested in Brown: Along with colleagues at the research wiki he started, ProjectPM (PPM), Brown was looking into a legion of shadowy cybersecurity firms whose work for the government raised all sorts of questions about privacy and the rule of law.

Since Hastings was familiar with the government contractors listed in the search warrant, he was also potentially culpable in whatever “crimes” the feds believed Brown and PPM were guilty of. Is this why he was being investigated in the days before his fatal crash on June 18, 2013? By then, Hastings had established a reputation as a fearless muckraker, whose stories often stripped the haloes from the powerful and well-connected:

– The besmirched “runaway” Special Forces general Stanley McChrystal, whose career Hastings had dispatched in a 2010 article for*Rolling Stone*

– The saintly General “King” David Petraeus—former commander of Central Command (CENTCOM), International Security Assistance Forces (ISAF) in Afghanistan, and head of the Central Intelligence Agency (CIA)

– Daniel Saunders—a former assistant US attorney for the Central District of California

– Former Secretary of State and presidential hopeful Hillary Clinton, with whose staff Michael had many pointed exchanges regarding State’s Benghazi spin.

“To Maintain and Cultivate an Enemies List”

In his profile on the blogging consortium *True/Slant*, Hastings confided that his “secret ambition” was “to maintain and cultivate an enemies list.” Such ironic distancing was

Hastings's way of making palatable an inherently cynical view of the world. He knew that power corrupted, and to effect change it was necessary to point out the Emperor's glaringly naked flesh.

In this manner, he was much like his blogging colleague at *True/Slant*, Barrett Brown. So much so, in fact, that the latter approached Hastings to work on a project that would change the way the public viewed the murky world of intelligence contracting in the post-9/11 era.

Michael Hastings interviews General Odierno in Baghdad, Iraq, October 2009

For those unfamiliar with Brown's tale,*WhoWhatWhy* has been chroniclinghis trials since February 2013. He is currently in federal custody in Ft. Worth, Texas, facing *over a hundred years behind bars* for researching 70,000 hacked emails obtained from the cybersecurity firm HBGary Federal and its parent company HBGary. At no point is the government alleging he was involved in the hack itself. His putative "crime" is doing what investigative reporters are supposed to do: digging for the truth about breaches of the public trust.

To do this, Brown pioneered a collaborative wiki where researchers and journalists could sift through these emails and create an encyclopedia from the information contained within. This was known as ProjectPM (PPM).

In 2009, Brown invited Hastings to join forces on PPM, but Hastings's interest was tempered by other commitments. When the two spoke next, Hastings told Brown he was working on something big.

"Not One of Us"

Hastings was referring to his impending 2010 article, "The Runaway General," for *Rolling Stone*, in which he quoted several high-ranking military officials from within Gen. McChrystal's inner circle disparaging their civilian command. The article caused a stir in official Washington, and eventually led to McChrystal being relieved of duty by President Obama.

Amid the fallout from this journalistic coup, an interesting narrative began forming in certain sectors of the press: "Michael Hastings is not one of us." Hastings had broken one of the rules governing Washington's hermetic circle of "access journalism" by quoting his subjects without their express permission. Elsewhere, most working reporters would call this, well, journalism.

Brown was quick to defend Hastings, penning an article for *Vanity Fair* titled, "Why The Hacks Hate Michael Hastings." Later, the two blurbed each other's books, further cementing

their professional relationship.

One thing they shared was a deep discontent with the mainstream media. Indeed, Brown says, they were "obsessed with coming up with ways to change the dynamic."

The busy Hastings never fully immersed himself in the work of PPM. "[Hastings] was an outlet for us to pass things to," says Alan Ross, better known on PPM's Internet relay chat (IRC) as Morpeth. "His relationship was one of talking to Barrett in my experience, rather than direct involvement in PPM." He was "more of an associate than a member."

"Get ready for your mind to be blown."

For Hastings, Brown was clearly a confidential source—the type that flourishes best when kept in the dark and away from other reporters. Yet on January 24, 2013, Hastings tweeted that he was finally beginning to work on the Brown story, telling his interlocutors to "get ready for your mind to be blown."

Kevin Gallagher, the administrator of Brown's legal defense fund atFreeBarrettBrown.org, said Brown and Hastings hadn't been able to talk securely in eight or nine months, but that after a few months of back and forth with Brown's lawyers Hastings finally planned on interviewing him in custody in June.

After whistleblower Snowden's bombshell revelations of dragnet surveillance by the National Security Agency (NSA), Hastings wrote an article on June 7 that referenced Brown for the first time since April 2012. Titled "Why Democrats Love To Spy On Americans," it lambasted supposedly liberal Democrats for their Bush-like surveillance fixation and their unrelenting war on those who seek to expose the operations of the surveillance state:

"Transparency supporters, whistleblowers, and investigative reporters, especially those writers who have aggressively pursued the connections between the corporate defense industry and federal and local authorities involved in domestic surveillance, have been viciously attacked by the Obama administration and its allies in the FBI and DOJ.

[snip]

Barrett Brown, another investigative journalist who has written for Vanity Fair, among others [sic] publications, exposed the connections between the private contracting firm HB Gary (a government contracting firm that, incidentally, proposed a plan to spy on and ruin the reputation of the Guardian's [Glenn] Greenwald) and who is currently sitting in a Texas prison on trumped up FBI charges regarding his legitimate reportorial inquiry into the political collective known sometimes as Anonymous."

The article ended with "Perhaps more information will soon be forthcoming."

The fact that he planned to interview Brown was corroborated by documentarian Vivien Weisman, who told *WhoWhatWhy* that she spoke to Hastings about it at a Los Angeles book signing for "Dirty Wars" in May 2013. And the editor of *Buzzfeed* reportedly confirmed that Hastings was in the midst of working on the Brown expose at the time of his death.

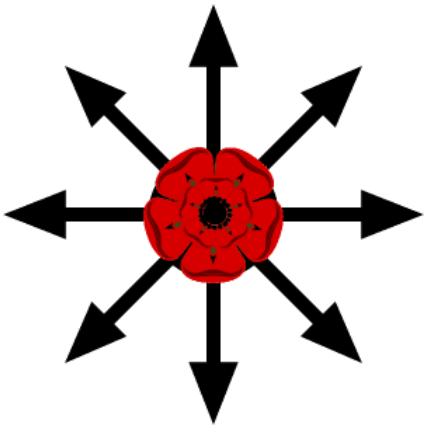
Knowing this prompts the question: what angle of the PPM research was Hastings about to tackle?

The evidence seems to point to another shadowy project revealed in the cache of hacked emails that PPM was sifting through: Romas/COIN.

Your Data Is Mine

Gallagher, who was briefed on the last discussion Hastings had with Brown before the planned interview, says, “Hastings had specifically asked about Romas/COIN.”

Romas/COIN was the name given to a program through which the U.S had been conducting “a secretive and immensely sophisticated campaign of mass surveillance and data mining against the Arab world,” according to emailshacked from the cybersecurity firm HBGary Federal. Evidently, this program allows the intelligence community to “monitor the habits, conversations, and activity of millions of individuals at once.”



ProjectPM logo

Over the course of a year, Aaron Barr, CEO of HBGary Federal, sought out various companies to form a consortium that could wrest control of Romas/COIN from the current contract holder, Northrop Grumman. Eventually the consortium included no less than 12 different firms — ranging from niche software companies to behemoths like Google, Apple, and even Disney.

From the emails, it’s clear that “mobile phone software and applications constitute a major component of the program,” concludes the entry in ProjectPM. Periodic references to “semantic analysis,” “Latent Semantic Indexing,” and “specialized linguistics” indicate that the government agency overseeing the contract was clearly interested in *automated dissection* of spoken or written communication. This is the hallmark of NSA surveillance.

Is it possible that this consortium planned on developing mobile phone software and applications with bugs that would allow the US government to hack into targets’ phones and give it access to all of the communications within?

As detailed by *New York Times* national security reporter Mark Mazzetti, mobile phone intrusion has been par for the course in the military’s signals intelligence work abroad.

Checkmate

Claims of government surveillance capabilities embedded in private-company software are bolstered by recent reporting on the sale of “zero-day exploits” to government agencies.

“Zero-day exploits” refer to security vulnerabilities that are taken advantage of on the same day that the vulnerability becomes known to the victim. As the jargon implies, there are zero days between the time the hole is discovered and the initial attack.

Endgame Systems, one such company cashing in on this new market, was of particular interest to Brown and ProjectPM. Deep in the cache of Aaron Barr’s emails are indications of just how secret the work of Endgame is.

In an email to employee John Farrell, then-Endgame CEO Chris Rouland states: “Please let HBgary know we don’t ever want to see our name in a press release.”

Farrell forwarded that note to Barr with the following explanation:

“Chris wanted me to pass this along. We’ve been very careful NOT to have public face on our company. Please ensure Palantir and your other partners understand we’re purposefully trying to maintain a very low profile. Chris [Rouland] is very cautious based on feedback we’ve received from our government clients. If you want to reconsider working with us based on this, we fully understand.”

One look at Endgame’s product line explains a lot about their wariness. Their premier software, “Bonesaw,” shows what a powerful asset the corporation has become to America’s intelligence agencies.

Bonesaw is a targeting application that tracks servers and routers around the world. It maps out all the hardware attached to the Internet. Through these access points, NSA and Cyber Command can hack into or launch attacks against adversaries. The Bonesaw program functions essentially as a user-friendly map.

That map has at its disposal the geolocation and Internet address of every device connected to the Internet around the globe. By designating a country and city — like Beijing, China for example — and the name or address of a target — say, a People’s Liberation Army research facility — a user can find out what software is running on all of the computers inside the facility, what entry points to those computers exist, and a menu of custom exploits that can be used to sneak in.

Sock Puppets and Other Tricks

Other clues as to what ProjectPM-related material may have led the FBI to investigate Michael Hastings can be found in his published work.

Endgame Systems CEO Nathaniel Fick. Formerly of the Center for a New American Security, Fick took over for Endgame in November 2012.

In a May 18, 2012, article on propaganda efforts by the State Department, Hastings referred to a "program being developed by the Pentagon [that] would design software to create "sock puppets" on social media outlets." The HBGary emails are littered with references to this type of "persona management" technology.

Principal among these was a June 2010 United States Air Force (USAF) contract from the 6thContracting Squadron at MacDill Air Force Base in Florida. It sought providers of "persona management software" that would allow 50 users to control up to 500 fictional personae.

These sock puppets were required to be "replete with background, history, supporting details, and cyber presences that are technically, culturally, and geographically consistent." In other words, avatars so convincing they could fool the people with whom they were interacting into believing they were real.

MacDill Air Force Base is home to the United States Special Operations Command (USSOCOM), the section of the military that oversees and coordinates all special-forces activity globally. USSOCOM lists under its "core activities" the employment of psychological operations (PSYOPS) and information operations (IO)—exactly the type of activity this "sockpuppeting" technology would be employed in.

To put it another way: a clone army for future psywars.

Gone With The Mercedes

Given the information currently available it is impossible to know with certainty what angle in the Brown case Michael Hastings was pursuing at the time of his death.

But Hastings's credibility and national security contacts would have served him well in digging deeper into ProjectPM's cache of hacked emails, perhaps exposing to the light of public scrutiny other secretive government contractors in the manner that Brown had begun. (See the "Team Themis" affair.)

With that potential suddenly snuffed out, it's not surprising the Internet is abuzz with speculation over Hastings's death. We've contributed to the investigation surrounding it but, with so few hard facts at hand, now is not the time to speculate about whether foul play was involved. What's clear is that an important voice in the grand tradition of investigative journalism has been silenced.

Hopefully, more information will come to light, and we will know with a fair degree of certainty what Michael Hastings was working on that attracted the government's watchful eye. That is, unless all of his information was incinerated with him in the early hours of that June morning.

GRAPHIC:
http://1.bp.blogspot.com/-ngciGioeQ1A/UQr2ASLxfxI/AAAAAAAAAhU/H0umDPDtbVU/s400/hacker.PNG

https://fbcdn-sphotos-a-a.akamaihd.net/hphotos-ak-frc1/s320x320/388275_248680775201375_268649908_n.jpg

http://trueslant.com/barrettbrown/files/2010/03/PM.png

http://cmsimg.defensenews.com/apps/pbcsi.dll/bilde?Site=M5&Date=20130115&Category=C4ISR01&ArtNo=301150007&Ref=AR&MaxW=300&Border=0&Nathaniel-Fick-Former-CNAS-Chief-Heads-Cyber-Targeting-Firm

The original source of this article is WhoWhatWhy

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Christian Stork