



HOLLYWOOD, BIG TECH, AND THE AGGREGATED DATA CAPER

How a stolen screenplay launched a corporate war on America.

[Home](#) [Thanks](#)

Hollywood, Big Tech And THE AGGREGATED DATA CAPER

How A Stolen Screenplay Launched An International Aggregated Data Race, A Secret Corporate Race War, A Data Theft Industry, And Eroded Our Faith In News And Reality.

DISCLAIMER:

Everything written, said or presented on this website or in the article "Hollywood, Big Tech, and the Aggregated Data Caper" is/are just allegations, not necessarily facts. Although I, the owner of this site, whole-heartedly believe these allegations to be true, and although the attached PDF court filings present seemingly overwhelming evidence, everything presented on or connected to this website, no matter how persuasive, is/are just allegations.

- This article/website links to over 150 authentic documents and web articles. Many of these documents are PDFs, which are stored on this website. Some of these documents are stored on external sources (such as the California and Arizona Secretary of State's offices, U.S. Patent Office). The links all ONLY connect to safe documents, and trusted, safe sources.
- In 2017, I, the owner and publisher of this website, wrote a social/political humor book called Moron Don't Ride Harleys. Pages 144-150 of this book lampooned people who believe in conspiracy theories. See [HERE](#). I share the fact that I am openly hostile to conspiracy theories, and share the fact that the following article is substantiated by over 200 verifiable documents, which are ALL linked to this web-article, for you to scrutinize, so you can be certain that every astounding word is true. Conspiracies exists. And many of them can be proven, if you search vigilantly. But, if you are attracted to conspiracies theories that are supported by the refrain, "The government doesn't want us to know," your malleability threatens America. Demand facts and evidence, scrutinize every source, and think critically. Human evolution depends on it.

FOREWORD

My name is Steve Wilson Briggs. In December 2006 I introduced the world to the concept of "Data Aggregation," in a screenplay that presented a sinister vision of how all of the world's data could be aggregated (collected together) and streamed into a massive Earth/universe computer replication (simulation), which could then be sped up, thousands of time faster than the actual world, creating a virtual time machine, capable of predicting and preventing crime and predicting military outcomes. In short, beyond "aggregated data," I conceived the world's first actionable time machine.

Overnight, these ideas would change the world, very much for the worse.

I introduced these plainly evil ideas to show the unparalleled danger of unbridled, hate-based power. But sickeningly, a group of American corporate powerhouses would unlawfully obtain these ideas, and find them "desirable."

The following Data Caper article explains how, in December 2006, U.S. big-tech and big-media industries unlawfully accessed my ideas (using a hacking company named MovieLabs, and while the script was posted on Kevin Spacey's social network for filmmakers "Trigger Street"), then quickly invited over 140 major tech and media executives to meet in Hawaii, in October 2007, for a convention called "The Lobby," to plan secret new US policing and defense systems, based on aggregated data, unauthorized data collection and mass surveillance. Among those in attendance at The

Lobby were Jeff Bezos (Amazon), Mark Zuckerberg (Facebook), Sergey Brin and Larry Page (Google), Evan Williams (Twitter), Peter Thiel (Palantir, PayPal), Jimmy Wales (Wikipedia), and multiple reps from Microsoft and FOX/News Corp and the Big 6 film studios. The Lobby "list" of 140+ invitees was first reported by Matt Marshall, in VentureBeat.com, May 2, 2007, at: <https://venturebeat.com/2007/05/02/the-lobby-are-you-on-the-list/> (or see the pdf [HERE](#)). It is certain that the lower-rank attendees/participants were unaware of the "anti-minority" grand-design of this plan.

This plan was so contrary to our Founding Fathers' intent that it amounted to the unlawful formation of a new nationalist social order. And, inevitably, this plan would connect former U.S. President Donald Trump to 3 Ukrainian/Russian businessmen, and entangle the US Copyright Office in multiple acts of document falsification.

Additionally:

- The two or three Blacks that were initially on The Lobby "list" were transferred or released just before the event, and did not attend.
- Two months after The Lobby event (Oct 24-26, 2007), Richard Parson, the only Black CEO in Big 6 history, was fired, allowing the plan to proceed.
- Because Twitter and Trump were both participants in this scheme, Twitter took no effort to restrict or suspend Trump, until after Trump lost re-election, and after insurrectionists assaulted the US Capitol.
- In 2007, under George W. Bush, the US government created two unprecedented computer viruses to facilitate the plan (the "Stuxnet" virus, discovered in 2010 -but launched in 2009, and the ".Trashes" virus, discovered in 2008-09 -but launched in 2007).

The conspirators / participants. The primary participants in this plan were Microsoft, Amazon, Facebook, Google, Twitter, News Corp, the "Big 6" studios (Disney, Warner Bros, Paramount, Sony Pictures, Universal, 20th Century Fox), their parent corporations (WarnerMedia, Comcast, ViacomCBS & Sony), the Motion Picture Association, MovieLabs, Lionsgate, MRC (Media Rights Capital), WME (Williams Morris Endeavor), and the owners of these companies. For brevity, the article refers to these corporations and their owners as "the conspirators" or "the participants."

Amazingly, the facts in the following Data Caper article were only discovered because a wonderful 89-year old attorney named Shirley Potash called me with a tip in March 2018. [Please see my "thank you" to Shirley, on the "Thanks" page, to read the whole story. And read more about Shirley Potash [HERE](#).]

Attached PDFs. The Data Caper article features some filings from the court action Briggs v Cameron (2020). PDFs of these filings are linked in the posts below the article. Some of these filings contain hundred of pages of exhibits. The article relies on numerous filings, rather than just the Briggs v Cameron (BvC) Complaint, because after I filed the Complaint, while researching the defendants' shell companies, I began discovering the disturbing facts that inspired this article; I then filed numerous *motions in limine* and *requests for judicial notice*, to inform the court of these new facts. I have also linked many web-articles, and business registrations, for efficiency and verification. [NOTE: few BvC case details are addressed in the article, because the article is not an attempt to litigate the case in the court of public opinion, it is an effort to warn Americans about extreme National security & aggregated data risks. But some BvC details are addressed, for context.]

EVIDENCE. Virtually all of the attached evidence is FRE (Federal Rules of Evidence) Rule 902 compliant (e.g., business registrations, dated emails, copyright and patent registrations, official publications, newspapers and periodicals, etc.).

SECONDARY POINTS

- Beyond the staggering facts concerning the "aggregated data" and "The Lobby" schemes, secondarily, the "Data Caper" article will explain:
1. Why so many big tech & big media executives resigned between Dec 2019 and Feb 2021 (Bill Gates, Jeff Bezos, Sergey Brin, Larry Page, more...);
 2. How immediately after I introduced "aggregated data," the conspirators formed many fake "shell" companies, to distribute their stolen profits;
 3. How my court filings ended shell companies, on January 1, 2021;
 4. How former President Donald Trump released dozen of demonstrably fake documents, pertaining to "data aggregation," on numerous federal websites, in an effort to help the conspirators steal and backdate this concept;
 5. How 2 months after The Lobby event, the first and only Black CEO of a Big 6 studio was fired;
 6. How, in support of this plan, Ninth Circuit Chief Judge Sidney R Thomas formed 2 shell companies (one, formed in 2006, appears created for payments from film industry participants; the other, formed Jan 2007, just weeks after I introduced "aggregated data," appears intended for payments from big-tech participants). Thomas then, personally, presided over my Briggs v Blomkamp appeal, AND the rehearing petition.
 7. The conspirator's Stuxnet virus' was originally named the "Mr X" virus -named after the film I was working on from late 2007 to 2011. This is confirmed by examining Stuxnet's two driver/install files, both of which start with the MRX prefix ("Mr X"). The nonsensical "Stuxnet" name was given to the virus by Microsoft, over a year after the virus was launched.
 8. How, in 2020, the Ninth Circuit removed 25 of my Briggs v Cameron case filings from its public docket (case filings are public documents which should never be removed from the docket), and did not return my case filings until after I published this website.
 9. How the U.S. Copyright Office produced falsified registrations to help foreign entities steal the intellectual property of an American creator;
 10. How these conspirators used trusted news sources to publish & backdate false web-stories;
 11. How my BvC Complaint helped the Department of Justice stop an aggregated data disaster, in the Spring of 2020;
 12. How in its BvC "motion to dismiss," Google admitted to sabotaging my efforts to market my own films and scripts, by not including my films & online fundraising campaigns in Google's search results, claiming a First Amendment right to do so (read pages 9 & 10, [HERE](#));

13. How the conspirators hacked into my devices for 2 decades, using Steve Weinstein & his hacking companies MovieLabs & Liberate Technologies;
 14. How I twice, personally, met/encountered Steve Weinstein in 2017-2018 (but didn't know he was hacking me until late 2020);
 15. How MovieLabs patented its method for hacking me and distributing the stolen ideas to the Big 6 studios (see [HERE](#));
 16. How the Internet Archive created fake crawls of the conspirators' fake webpages, while Google modified its browser to display valid URLs of these fake crawls.
 17. How, on Jan 14, 2020, the day I discovered how Google and Internet Archive were falsifying crawls and URLs, I happened to film the hackers (MovieLabs) hack into my laptop;
 18. How the same day that I filmed this hacking, January 14, 2020, the NSA revealed a "serious vulnerability" in Windows 10; this vulnerability allowed the Internet Archive and Google to deceive me for months.
- **REMEMBER:** court PDFs, and many other documents cited in the article, can be found in the PDF section, below the main article.
 - **NOTE:** for continuity, the "**Stuxnet**" and "**.Trashes**" virus details are found at the end of the article.

HOLLYWOOD, BIG TECH, AND THE AGGREGATED DATA CAPER

The Aggregated Data Caper didn't just happen; it was a sequel or threequel—an unexpected product of two smaller capers:

1. **First.** In 1999, after I sent Rupert Murdoch a copy of a short story, Murdoch, Steven Spielberg, Sumner Redstone and Microsoft began using [Liberate Technologies](#) to hack into my computer, to steal screenplays.
2. **Second.** Jan 2006, a defunct company named Zero Gravity Management (ZGM) unlawfully acquired my screenplay; causing the Big 6 to buy multiple ZGM subsidiaries (to keep ZGM quiet). Then, after a federal fraud investigation into Liberate, the Big 6 changed Liberate Technologies' name to MovieLabs—to more discretely steal my ideas.

Confusing? Let's take a brief look at the first two capers.

1. THE FIRST CAPER (February 1999)

In 1999, Rupert Murdoch began using his wealth to spy on private citizens. (See [HERE](#).) These early spying efforts led to the "News International phone-hacking scandal" of 2005-07, which led to Murdoch losing his "News of the World" newspaper. (See [HERE](#).) Around February of that same year, **1999**, I sent Murdoch's "HarperCollins" book company a copy of my short story, "Hot Orange & Honey." Murdoch and Steven Spielberg would steal (infringe) this short to make the TV series "Freaks & Geeks." (To learn more, see Amended Second Declaration, pp 23-37.) Later that year, November 1999, Murdoch's News Corp entered into a "partnership" with Liberate Technologies. (See [HERE](#).) Liberate did not provide the services mentioned in the linked article. The article was published to legitimize payments from News Corp to Liberate.

Steve Weinstein, Liberate's Chief Strategist/Technologist, teaches "Hacking for Defense" to US intelligence prospects at Stanford University (see [HERE](#)) and worked for the prestigious US Naval Research Laboratory—a research think tank that studies everything from artificial intelligence to **electronic warfare**; see [HERE](#). (Also see Third Motion In Limine, pp 1-6; Fifth Motion In Limine, pp 22, 23; Opening Brief, p 3.) In 1996, about the time that Liberate Technologies opened, Steve Weinstein and Liberate Technologies patented his method for hacking. (See [HERE](#).) This is Liberate's earliest patent, and Weinstein's only patent. [More on Weinstein under "Disappearing Webpages" in the "Hacking" section, and read about my strange two personal encounters with Weinstein, near the end of this article.]

In 2004 a federal investigation accused Liberate of fraud, for using its own funds to create the false appearance of legitimate revenue—by supplying a customer money to make a purchase. Fake companies, that are false fronts for hackers, that make no legitimate product, need to create the appearance of valid income. (See [HERE](#).) (See: Fifth Motion In Limine, p 21.) In April 2005, Liberate closed and sold its assets to Comcast. (See [HERE](#).)

Liberate Technologies hacked into my devices from 1999 to 2005, at the behest of: 1. Rupert Murdoch (News Corp), 2. Steven Spielberg (Dreamworks), 3. Paul Allen (Microsoft), 4. Bill Gates (Microsoft), 5. Sumner Redstone (ViacomCBS). To learn how these parties came together, see Amended Second Declaration, pp 24-25.

2. THE SECOND CAPER (January 20, 2006)

- January 2006, a defunct company named Zero Gravity Management unlawfully acquired my screenplay; causing the Big 6 film Studios to buy multiple ZGM subsidiaries, and change Liberate Technologies' name to "MovieLabs."

In December 2003 or January 2004, I began writing a screenplay originally called "Uberopolis: City of Light." I finished the first draft in May 2005, and emailed it to a few friends and family.

About that same time, Sept 12, 2005, a company named Zero Gravity Management (**ZGM**), owned by Michael Pierce and Mark Williams, went out of business. (See [HERE](#); also see the BvC Complaint, p 20.)

Meanwhile, I continued to revise my script, and emailed a portion of my script, to my brother, on May 12, 2005.

- The first complete script that I emailed out was sent on May 25, 2005. To read a few pages of this emailed script, click [HERE](#).

- By Jan 2006, the script was becoming something unprecedented. To see the first few pages of a version, emailed myself, Jan 16, 2006, click [HERE](#).

Unaware that ZGM was out of business, on January 20, 2006, after seeing a listing on moviebytes.com, stating that ZGM was looking for screenplays to produce, I emailed ZGM to ask if they would like to read my screenplay.

ZGM replied, that same day, via email, permitting me to send them my screenplay. To read that email exchange, click [HERE](#) (scroll down to read complete exchange). I emailed ZGM the script immediately.

Six days after receiving my screenplay, ZGM filed a new California business certificate, and went back in business. (See [HERE](#), and BvC Complaint.) ZGM (Pierce and Williams) never contacted me again.

Pierce & Williams Become Subsidiaries of the Big 6, And Appear on the Avatar Copyright.

Quickly, Pierce and Williams formed many new anonymous shell companies, which became subsidiaries of various Big 6 movie studios. These shells were formed because, in 2006, ZGM (who were friends with 20th Century Fox's VP, Alex Young) tried to market my script to 20th Century Fox. Upon learning that ZGM were aware of my script, Rupert Murdoch (CEO of 20th Cent Fox) arranged to have Pierce & Williams create numerous shells, that Murdoch and the Big 6 would buy from Pierce and Williams, to funnel money to them. (See BvC Complaint pp 19-23, for a more detailed telling of this story).

August 2006, billionaire Stephan H Margolis formed 4 companies with ZGM's Pierce & Williams (Future Service Inc, Future Films USA LLC, Future Films USA 1 LLC, Future Films USA 2 LLC). For Future Films USA, Margolis (a UK citizen) unlawfully used Pierce and Williams' California Address. (See [HERE](#) or [HERE](#).) Pierce and Williams claimed this address on many official documents, at that time. (See [HERE](#) or [HERE](#).)

September 2006, Pierce, Williams and Margolis formed their new company, Future Service Inc, which would appear on many Avatar movie copyright registrations. Avatar is one of 2 films at the center of the Briggs v Cameron. Future Service Inc immediately became a subsidiary of Murdoch's News Corp and 20th Century Fox (now Disney). (See [HERE](#) ; also see BvC Complaint pp 15-23, 53.)

December 2006, Mark Williams formed Williams Productions LLC, (see [HERE](#) ; also Amended Motion In Limine, pp 8-9.) which became a subsidiary of NBCUniversal, although the company is located in **a towing yard** (see [HERE](#)).

The Motion Picture Association (MPA)

The "Big 6" are the six most powerful studios in the US (Disney, Warner Bros, Sony Pictures, Paramount, Universal, Netflix*). The Big 6 own the Motion Picture Association (MPA). November 2005, seven months after Liberate Technologies closed, the Big 6 & the MPA filed a California business registration for Motion Pictures Laboratories, Inc (MovieLabs); see [HERE](#).

- Netflix replaced 20th Century Fox in the Big 6 in 2019, after Disney purchased 20th Century Fox.

MOVIELABS: PART 1

The MPA would not announce MovieLabs' formation until July 2006. (See [HERE](#).)

Thus, six months after ZGM acquired my screenplay, the MPA (which had been in existence for 84 years) created its first and only known subsidiary, MovieLabs, and appointed Steve Weinstein as MovieLabs' first CEO. Weinstein and the other "executives" (hackers) at defunct Liberate Technologies (Raymond Drewry, Craig Seidel, Jim Helman) all moved to MovieLabs. (Click [HERE](#); also see Third Motion In Limine, pp 1-6; Amended Second Declaration, pp 39, 40; Fifth Motion In Limine, pp 22, 23.) MovieLabs claims to be located in **Palo Alto, CA** (near **Stanford University**).

MovieLabs was created to hack into my computer and phone, full time, and steal my screenplays, books, shorts, email—even my conversations.

Liberate Technologies' failed because its owners made it a public company, which invited government scrutiny. So the Big 6 & the MPA were careful to make MovieLabs a private company, which they alleged derived its income from a few private clients. [NOTE: All of the hacking companies that the conspirators have used over the years (Liberate Technologies, MovieLabs, EFI) claim(ed) that they work for a few private clients, and produce some sort of software for computers or TV boxes or printers—because software is not tangible; thus, they never have to show a product—because these are fake company fronts, for hackers, who don't produce anything.]

- The complete facts about MovieLabs are lengthy; so I have moved the remaining facts toward the end of this article, under "MOVIELABS - PART 2". These facts show: 1. MovieLabs has only produced 3 (very questionable) patents in 15 years, including a patent for hacking me; 2. MovieLabs does not derive any legitimate income.

• 3. THE AGGREGATED DATA CAPER BEGINS

The Revision

Around June 2006, I changed my screenplay's name, from "Uberopolis: City of Light" to "Butterfly Driver," and substantially revised it. In addition to the dozen original ideas found in the prior versions, I added an arch about the importance of hope (this has since been infringed dozens of times).

But in December 2006, I revised the script again, to add four revolutionary concepts, which would inspire new industries (such as: aggregated data collection and distribution, aggregated data based defense systems, biometric data collection and cyber imaging, neurological electromagnetic imaging...). The four revolutionary ideas contained in the revised December 2006 screenplay were:

1. Data aggregation: collecting all available data (surveillance cams, GPS, traffic, telephone, meteorological, nautical, astronomical, internet activity, commerce...), then aggregating (combining) all of that data into a giant computer data center;
 2. Using an advanced MRI scanner to make perfect digital/cyber reproductions (neurogens) of human brains, bodies and souls, which look, act and think just like the original human. These neurogens could then be inserted into...
 3. A massive computerized replication (simulation) of Earth and the known universe (called the "GenLab," "The Accelerator," or "Soul Machine");
 4. By inserting all known living persons' "neurogens" into the Accelerator, and by inserting all available data into the Accelerator, the Accelerator could then be sped up, thousands of times faster than the real world, to prevent and predict crime (and military outcomes) up to 4 hour into the future, with 99.98% accuracy.
- NOTE: Google is currently very involved in creating computer reproductions of brain scans. (See [HERE](#).)

I then posted this new version of my script on Kevin Spacey's screenwriter and filmmaker social network, Trigger Street (at www.TriggerStreet.com) for 3-6 weeks, in December 2006. Although the conspirators may have accessed the script on Trigger Street, I believe they used Steve Weinstein and MovieLabs to hack into my computer, and watched me write it in real time. Once they saw that advanced policing and military systems, and a virtual time machine, were possible, using aggregated data, they set out to make this a reality.

THE LOBBY

The Conspirators' New Government of Terror

May 2007, roughly six months after the conspirators accessed my revised screenplay, Google, Microsoft, Amazon, Facebook, the Big 6 film studios, and over 140 executives of powerful tech, film, media and financial corporations, agreed to participate in an exclusive convention, called "The Lobby," to be held in late October 2007, at The Fairmont Orchid, on the Big Island, in Hawaii. (See [HERE](#); also Fifth Motion In Limine, pp 22, 23; and Opening Brief, pp 6-8.)

While the big-tech companies were interested in aggregating data to predict markets, crime and military outcomes, and selling these ideas to the US military, the film industry was simply interested in the entertainment value of my ideas.

"The Lobby" convention was intended to get all of these major companies on board with secretly collecting as much real-time data on users as possible, to create a predictive, data-based marketing system, to anticipate the wants and needs of the participants' customers. But the larger plan, which many Lobby invitees were likely unaware of, was to collect the data from ALL of The Lobby participants, then use that unrelated aggregated data to create predictive policing and defense systems.

There was no official announcement about The Lobby, because it was a private event. On May 2nd, 2007, Matt Marshall published the only known blurb (8 sentences) about the event, which included a "list" of all of the invitees' names. Inexplicably, on this list, amid the many powerhouse corporations, was Steve Weinstein, CEO of MovieLabs (a company that was only a year old, with no known product or income). The Lobby occurred October 24 to 26, 2007.

10 days after The Lobby convention, November 6, 2007, Facebook would launch its "Beacon" data collection program. Facebook's Beacon program was quickly sued (Lane v Facebook, Inc). This lawsuit proved that Facebook was collecting real-time user data, without consent, and while users were not logged on, and they continued to collect data after users "opted out". Beacon ended in September 2009.

Government By Hatred,

Dehumanization & Surveillance

Demographically, "The Lobby" invitees were disproportionately White, disproportionately Jewish, with a higher representation of Asians and South Asians than are demographically present in America.* Latinos were under-represented. No Blacks attended the "The Lobby" —although a few were initially invited, they were reassigned or promoted before The Lobby took place—making them conveniently unable to attend. (For example, Denmark West of MTV was on the Lobby list, but July 19, 2007, two months after The Lobby list was published (but 3 months before the actual event) West was transferred to BET; see [HERE](#), or pdf [HERE](#).) Renown Black powerhouses, like David Steward, Oprah Winfrey, Robert Smith, Jay-Z and Tyler Perry (who were more established and more powerful than many of the invitees) were conspicuously excluded.

The Lobby catalyzed after a group of powerful White men stole the intellectual property of a Black (bi-racial) American (myself), then used the stolen ideas to create military and policing systems that negatively target Blacks (Amazon's Rekognition and Clearview AI's facial recognition software, which are behind most American police surveillance systems, have been found to discriminate against Blacks). Therefore, The Lobby must be called what it was: a secret racist retreat to plan to use aggregated data, aggressive surveillance and disinformation to subjugate, brutalize and dehumanize Blacks and darker-skinned minorities.

I suspect the Lobby's organizers were Rupert Murdoch, Larry Ellison, Jeff Bezos, Bill Gates, Larry Page, Sergey Brin and Mark Zuckerberg. Rupert Murdoch's anti-Black views are expressed in FOX News' anti-Black bias. The anti-Black sentiment of Bezos, Gates, Ellison, Page, Brin and Zuckerberg

can be seen in their companies' terrible records of hiring Blacks and Latinos, prior to 2020. (See The Opening Brief pp 6-8; Fifth Motion In Limine, pp 22, 23; Amended Second Declaration, pp 41-49).

The Lobby Connects To Fraud at the US Copyright Office; The Trump-Russian Connection,

While checking the copyright registrations of a few works that infringe my screenplays, I found several shameless examples of the US Copyright Office producing demonstrably falsified documents, and most of these documents were for foreign entities (Japan and the UK). (See the Amended Second Declaration, pp 10-14, and 7, 8, and Second Request for Judicial Notice, and Fifth Motion In Limine, pp 15-20).

But the sickest example of fraud at the Copyright Office is related to Sony Pictures' and MRC's 2017 film "Baby Driver," which the Copyright office went grossly out of date and grossly out sequence to give the film a registration ending in "44444". (See [HERE](#).) The Copyright Office fraud related to this registration is extensive, fully explained in the Amended Second Declaration, p 9-15 (read that section [HERE](#); this section also explains the meaning of the number 44444). Worse than the date and sequencing fraud, "Baby Driver" infringes my screenplay "Cyclones," which I copyrighted in 1992, which **Ari Emanuel, Sony, Media Rights Capital** and **WME** could have only accessed through a connection at the US Copyright Office. (The name "Baby Driver" was selected to mock "Butterfly Driver," and to send a message: "we can steal whatever we want from you.") All of this prompted me to look into the leadership of the US Copyright Office.

I quickly learned that Karyn Temple, who was the Register of Copyrights at the time of much of the document falsification, left the Copyright Office in January 2020, and took a new job with the Motion Picture Association (MPA). (See [HERE](#); also Third Request For Judicial Notice.) Again, the MPA is owned by the Big 6 studios, and the MPA owns MovieLabs.

I then found Carla Hayden (the U.S. Librarian of Congress, who presides over the US Copyright Office) featured on the "Speakers" website of All American Entertainment (**AAE**). (See Fifth Motion In Limine, pp 4, 8.)

Although I had never heard of AAE, on the AAE "Speakers" website (www.AllAmericanSpeakers.com), I found web pages for the biggest actors in the world (although I found no Black actors, other than Hayden, on this site). I soon found all of the primary conspirators, named on "The Lobby" announcement, listed on the AAE "Speakers" website: Gates, Bezos, Zuckerberg, Spielberg, Iger, Thiel, Page, Brin, Reed Hasting, Ari Emanuel.... Click [HERE](#). Somewhere along the way I found **Eric Trump**, son of **former US President Donald Trump**. (See Fifth Motion In Limine, exhibit E.) This prompted me to go to OpenCorporates.com, to investigate AAE. I soon learned:

1. All American Entertainment Inc (AAE) is based in Deerfield Beach, FL, 29 miles from Trump's Mar-a-Lago home (Fifth Motion In Limine, p 12);
2. All American Entertainment is sponsored by Microsoft, Google, and others (Fifth Motion In Limine, p 8);
3. All American Entertainment is connected to 3 Ukranian/Russian businessmen, through a man named Robert Chmielinski (see Fifth Motion In Limine, pp 13, 14).
4. In May and July, 2008, Robert Chmielinski opened two companies, which appear to be involved in biometric imaging—the technology necessary for 3D cyber images of human bodies or brains: 1. Imaging Equipment International, LTD; 2. IT - Innovation Technologies, Inc.
- Any ties Trump has to these Russians is hidden by Trump's 500 shell LLCs; see [HERE](#).
- After I filed my Opening Brief with the 9th Circuit (in which I commented that I found no Blacks on the AAE speaker website), AAE began prominently displaying Black artists on its Speakers homepage.
- After I filed my Fifth Motion In Limine, the Internet Archive stopped legitimately archiving its crawls of www.AllAmericanEntertainment.com. Now, when one enters "www.allamericanentertainment.com" into the Internet Archive app, the app's URL directs to: https://web.archive.org/web/2020*/https://www.allamericanentertainment.com/; when it should direct to: https://web.archive.org/web/*/https://www.allamericanentertainment.com.

Click the last link, to see this. The fake element in the URL that the link redirects to, is the "2020" near the center of the URL, adjacent to the asterisk (*). This Internet Archive fake URL scheme is explained in the BvC Complaint, pp 96-108, and later in this article.

Business Formation Connections

2006

After the conspirators obtained my script from ZGM, the following businesses (owned by the infringers of my work, or parties connected with the infringement) formed between Jan 26, 2006 and Dec 31, 2006:

1. Zero Gravity Management LLC, went back in business, January 26, 2006.
2. Dune Entertainment II LLC, the first "Dune" company, owned by US Treasury Secretary Stephen Mnuchin, was formed March 14, 2006. [Dune Entertainment III LLC, which appears on the Avatar movie copyright, was formed June 2007.] See [HERE](#). (NOTE: Steven Mnuchin was the Executive V.P. of Goldman Sachs from 2001 to 2002.)
3. The same day that Mnuchin's company was formed, Mar 14, 2006, All American Entertainment Inc was formed ([HERE](#); 5th Motion In Limine, p 10).
4. July 2006, the Motion Picture Association (owned by the Big 6) opened a new subsidiary: MovieLabs. (See [HERE](#); also Third Motion In Limine, p 4.)
5. August 2006, Stephen Margolis and ZGM formed 4 shell companies: Future Service Inc, Future Films USA LLC, Future Films USA 1 LLC, Future Films USA 1 LLC. (See [HERE](#).)

6. Sept 7, 2006, a man named Sidney R. Thomas (the Chief Judge of the 9th Circuit) formed "Thomas-Hume Holdings, LLC". (See [HERE](#).) This AZ business filing appears falsified (explained later in this article). Chief Judge Thomas presided over the Briggs v Blomkamp appeal, 2018, AND the rehearing petition.
7. Sept 20, 2006, Pierce and Williams (ZGM) formed Future Service Inc, which appears on the Avatar copyright and became a 20th Century Fox subsidiary. See [HERE](#).
8. Jeff Bezos formed his company Blue Origins in September 29, 2006; see [HERE](#). Bezos abused lax US business oversight to fraudulently backdate the company to 2000. (See Amended Second Declaration, pp 44 and 45.)
9. Media Rights Capital (producer of Elysium), formed on November 30, 2006. See [HERE](#).
10. Dec 2006, Mark Williams (ZGM) opened a new shell, Williams Productions LLC, which became a subsidiary of Universal Pictures (NBCU) in 2007.
11. June 13, 2006, former US President Donald J Trump formed "TIHM Member Corp." See [HERE](#).
 - Twitter was also formed during this time, on March 21, 2006. But I don't think Twitter joined the conspirators until around January 2007.

2007

After I published the revised script (containing the "aggregated data" concept, the GenLab/Accelerator, etc), in December 2006, the following businesses (related to the infringement of my work) began forming:

1. January 11, 2007, Sidney R. Thomas, Chief Judge of the Ninth Circuit, formed Trinity Property Development, LLC, with Chris Jaska and Randy White. Judge Thomas presided over the Briggs v Blomkamp appeal in 2018. This business filing shows many signs of fraud (explained later in this article). See [HERE](#). Thomas' business partner, Chris Jaska, is an advanced laser "imaging" engineer.
2. May 2, 2007, VentureBeat.com announced the Lobby convention, to be held in Hawaii, in October, 2007. (See [HERE](#).)
3. Mnuchin's company Dune Entertainment III LLC, was formed June 2007. (See [HERE](#).)
4. July 2008, Pierce (ZGM) formed 212 Degrees Fahrenheit Corporation, a company that would become a contractor for Microsoft, Google and the US Marines. (See [HERE](#); also Amended Second Motion In Limine, pp 2, 3.)

*Thus, after acquiring my script, Pierce & Williams went from being out of business, to being (1) owners of numerous Big 6 subsidiaries; (2) subcontractors for Microsoft, Google and the US Marines; (3) producers of one of the biggest films ever (Avatar).

These facts suggest the financial structure behind the participants plans. Specifically, after accessing my script in January 2006, the conspirators created shells to receive payments (possibly from Steve Mnuchin and Goldman Sachs). And after they accessed my work in December 2007, and saw my ideas of an actionable time machine and policing systems based on "aggregated data," the participants committed to actualize these ideas, and may have planned to use Mnuchin and his connections at Goldman Sachs to distribute money to the participants, through All American Entertainment, Inc.

- **Chief Judge Sidney R. Thomas**, personally intervened, TWICE, to block my Briggs v Blomkamp appeal. He sat on the Feb 2018, three judge appellate panel (click [HERE](#)), and he sat on the April 6, 2018, three judge petition-for-rehearing panel (click [HERE](#)).
- More on Sidney R Thomas' shell companies toward the end of this article.

My Reporting On The Conspirators' Shell Companies Led to the End of All U.S. Shell Companies

"Shell" companies are companies in name only, that hide the true owner's identity, and are usually used for money laundering or other forms of business fraud. The BvC filings show the conspirators not only created countless shell companies, but protected these shells by hacking, and using The Corporate Service Company (CSC) to falsify WHOIS and ICANN internet records/reports for the conspirators' fraudulent websites and shells, by taking advantage of internet registration loopholes. (See Pages 43-46 of the BvC Complaint, for an explanation of how this scheme worked.) This is international organized crime.

Shell companies go back at least 150 years in America, to Thomas C. Durant's "Credit Mobilier". The "Panama Papers" (a huge document leak about shell companies) were leaked April 3, 2016. But after the Panama Papers were leaked, the Republican controlled Congress (under President Obama) did nothing about shells. And from January 2017 to December 2020, almost 4 years, Donald Trump (who owns 500 shells) and his Republican Senate, also did nothing about shells.

But January 1, 2021, sixteen days after I filed my Opening Brief, the US Congress passed the "Corporate Transparency Act," which bans anonymous shell companies. The act was tucked away in the annual National Defense Authorization Act. (See [HERE](#).) The Corporate Transparency Act was passed because of my Opening Brief.

- It should be noted that 9th Circuit Judge Vince Chhabria (who presided over both Briggs v Cameron AND Briggs v Spacey, and who dismissed Briggs v Spacey on a SATURDAY, 3 days before Christmas), did nothing to address the defendants' (MRC, Sony Pictures, and Ari Emanuel) extensive business fraud or their numerous shell companies, which I brought to his attention during Briggs v Spacey. (See [HERE](#).)

The Department Of Justice's Unlawful & Improper Intervention

Judge Orrick's Recusal

Circumstantial evidence indicates that former US President Donald Trump's Attorney General, William Barr, and the Department of Justice (DoJ) improperly interceded in Briggs v Cameron, to have the original judge, the honorable Judge William Orrick, recuse. Judge Orrick suddenly recused, on June 23, 2020, without explanation. (See [HERE](#).) It is also possible that Chief Judge Sidney R. Thomas is responsible for this change. Judge Orrick was replaced with Judge Vince Chhabria. Judge Chhabria presided over Briggs v Spacey, and dismissed the matter 3 days before Christmas. I believe Chhabria did this to keep news of the case silent, as media outlets are less inclined to check court docket activity on holidays and weekends (as courts rarely enter their orders on weekends, or holidays).

Court Filings Removed From Public Docket

Barr and the DoJ improperly interceded to have 25 of my BvC court filings removed from the court docket. Legal documents are public documents and should never be removed from the docket. Yet, by looking at the the copy of the docket (which is required in the Excerpt of the Record, filed December 16, 2020), one sees that 25 of my filings were removed from the docket, without explanation. The missing docket filings are numbers 4, 8, 18, 31, 35, 37, 39, 43, 45, 51, 52, 53, 67, 68, 80, 81, 83, 84, 86, 87, 99, 101, 103, 105, 109.) (See Excerpts of the Record, pp 2-10; click [HERE](#).)

February 2, 2021, I wrote a letter to the Ninth Circuit, asking why these documents were removed from the docket. Click [HERE](#) to see letter.

February 24, 2020, the Ninth Circuit sent me a PDF of the updated docket, showing that my 25 document were now back on the docket. The Ninth did not explain why my filings were removed in the first place.

- I believe the DoJ was acting, unlawfully, to protect President Donald Trump, who appears to be a participant in the conspirators' plan.

FEDERAL Aggregated Data Fraud, Under Trump

Former U.S. President Donald Trump authorized at least 8 different U.S. federal agencies (including the CDC and the Department of Defense) to produce and published falsified and fraudulently backdated web-articles on at least 8 federal websites. These falsified documents unlawfully endeavor to backdate the conception of "data aggregation" to before 2007. All of these fake web pages either had demonstrably fake Internet Archive crawls, or had never been crawled by the Internet Archive. Some had additional problems.

I made 2 videos for the court, of myself examining these fraudulent webpages and their Internet Archive "crawls," explaining how to spot the fraudulent Internet Archive URL elements. These videos can be seen at <https://youtu.be/8E3qt2facA0> and at <https://youtu.be/2XTHKDMbrWs>). (See Fifth Motion In Limine, pp 23-25.) The second video is also posted on this site. The first was too large to post on this site, but it is extremely informative.

My Warning Averts An Aggregated Data Disaster:

The DoJ Disconnects Google's Undersea

Internet Cable To Hong Kong

Because "aggregated data" and "police and military systems based on aggregated data" are both ideas that I conceived, I have unique insight about this subject. Once I realized that the conspirators had stolen my ideas to make one or more "actual" data aggregation systems for U.S. police and military, I alerted the court that Google and Amazon (and Microsoft) appear to be involved in creating aggregated data-based police and defense systems. I then tactfully warned that aggregated data-based defense systems can be hacked and "**give foreign hackers (of the systems or the data) the ability to predict US military responses and allow hackers (or the owners) to predict markets.**" (See BvC Complaint, p 124, [HERE](#).)

Five weeks later, April 2020, the US Department of Justice ordered Google and Facebook to disconnect Hong Kong from an undersea cable line that Google ran from the U.S. to Hong Kong, between 2016 and 2018. The DoJ ordered this disconnection because they realized that I was correct about this vulnerability. *Thus, as William Barr's Department of Justice was actively sabotaging my lawsuit, they eagerly accepted my guidance on how to keep hackers out of U.S. defense systems.

- I also warned of two more vulnerabilities in this sort of aggregated data defense system in my Amended Opposition To Google's MTD (page 3, filed May 28, 2020, see [HERE](#)). But I didn't elaborate. Neither the DoJ or the DoD enquired about these or other vulnerabilities. I believe the SolarWinds (Russian) hacking, December 2020, is a variation of one of the two vulnerabilities. This is not to say that had the DoJ or DoD contacted me, SolarWinds could have been avoided; but if you are dutifully protecting America, why not enquire?

TWO MONTHS AFTER THE LOBBY, THE ONLY

BLACK CEO OF A BIG SIX STUDIO WAS FIRED

As a thinker and writer, I research, analyze and report. I don't alter facts to be well-liked. So this next section is difficult to report. That said...

In 1999, when I mailed my short story, Hot Orange & Honey, to Rupert Murdoch's HarperCollins Books, ALL of the Big 6 film studios were owned Jewish men:

1. Disney - **Michael Eisner** (1984 – September 2005);
2. Paramount and CBS - **Sumner Redstone** (1994 – 2016);

3. Sony Pictures - **Michael Lynton** (CEO, 2004 – 2017);
4. Twentieth Century Fox - **Rupert Murdoch** (CEO 1985 – 2019);
5. Warner Bros - **Barry Meyer** (Oct 1999 – 2013)
6. NBCUniversal - **Edgar Bronfman** (1995 - 2001)

But in December 2001, something monumental happened in America: Gerald M Levin (a Jewish business man who had been the CEO of Time-Warner) resigned, after the bad AOL/Time-Warner merger, and Richard Parsons (a Black American businessman) was appointed as his successor.

Thus, in or around January 2002, for the first time in history, a Black American was the CEO of one of the Big 6 film studios (Time-Warner Bros). Well, technically, Richard Parsons was the CEO of Time-Warner, which is the parent company of Warner Bros movie company. So, although Parsons was not necessarily running Warner Bros directly, he was Barry Meyer's boss (Meyer was the CEO of the subsidiary Warner Bros). Richard Parson would not last long. But about 12 curious events would transpire before Parson's 5 year reign ended:

1. In 2004 NBC and Universal Pictures merged, becoming NBCUniversal (NBCU), and Robert Wright would be named CEO.
2. In 2004, Dan Glickman was appointed CEO of the MPA.
3. May 2005, I finished the first version of Butterfly Driver (Uberopolis), and I began emailing and giving it to a few family and friends.
4. A few months later, September 2005, Michael Eisner resigned at Disney, and Bob Iger became the new CEO.
5. Two months later, November 2005 MovieLabs was created.
6. December 2005, I registered my script with the Writers Guild of America, west (the WGAw is closely connected to the Big 6).
7. That same month, December 2005, Time-Warner (the only communication giant with a Black CEO) promoted Jeff Bewkes to President, directly under Richard Parsons. This allowed Bewkes to interact with Barry Meyer (CEO of Warner Bros) without involving Richard Parson.
8. Also, that same month, December 2005, NBCU promoted Jeff Zucker to CEO of NBC Universal Television Group, under CEO Robert Wright.
9. July 2006, around the same time that I revise my screenplay and renamed it "Butterfly Driver", MovieLabs named Steve Weinstein as MovieLabs' first CEO.
10. One year later, December 2006, I published the "aggregated data" version of Butterfly Driver, which started the aggregated data race.
11. Two months later, on February 6, 2007, Jeff Zucker was promoted to CEO of NBCUniversal, replacing Robert Wright.

At that point, February 2007, **ALL of the CEOs of the Big 6, AND the CEOs of the MPA and MovieLabs, and Steven Mnuchin and Stephen Margolis** (Future Films) were all Jewish:

1. Disney - **Bob Iger**;
2. Paramount and CBS - **Sumner Redstone**;
3. Sony Pictures - **Michael Lynton**;
4. Twentieth Century Fox - **Rupert Murdoch**;
5. Warner Bros - **Barry Meyer**;
6. NBCUniversal - **Jeff Zucker**;
7. The Motion Picture Association - **Daniel Glickman**;
8. MovieLabs - **Steve Weinstein**.

At that point, of all of the Big 6 CEOs, only Barry Meyer, at Warner Bros, had a superior in America. Parson was Barry Meyer's superior. (Note: Michael Lynton, of Sony Pictures, had a superior in Japan). That's when the twelfth and final event happened: **October 24-26, 2007, the Lobby convention occurred.**

Monday, November 5, 2007, just 9 days after The Lobby event, CNBC announced that Richard Parson, the only Black CEO in Big 6 history, was "stepping down." (See [HERE](#).) Jeff Bewkes was promoted to CEO of Time-Warner.

I'm confident that Parson was released because the other Big 6 CEOs worried that if Parson found out that MovieLabs was stealing the ideas of a Black American, he would not comply. But in fairness to Parson, he —like all good Americans— would not comply if he knew anyone, of any race, was being robbed and exploited.

So... You see why this is so troubling. It looks a subset of Jewish CEOs stole the ideas of a Black American; then gave those stolen ideas to a subset of White big-tech business owners, who used those stolen ideas to engineer aggregated data policing systems that would unfairly target Blacks and dark skinned minorities.

If you're a small-minded racist, intent to see Jewish people as bad or evil, you might read the last page of Morons Don't Ride Harleys (click [HERE](#)). It reminds us that the group that was perhaps most helpful to Blacks during the civil rights era was the American Jewish Community, who lost many lives defending the rights of Blacks.

Many Big Tech & Big Media Film Companies' CEOs Suddenly Resign, Due To Briggs v Cameron

As explained in the BvC Complaint, I began composing the Complaint in August, 2019. By late August or early September, 2019, I became aware that hackers were hacking into my laptop (the evidence of this is provided in the BvC Complaint). From the time that I began writing the Complaint

(August 2019), to the time I submitted it to the court (March 2020), then to the time that I published this website (February 2021), 18 months, the following ELEVEN major big tech and big media CEOs resigned:

1. Larry Page (CEO, Google) resigned Dec 3, 2019;
2. Sergey Brin (CEO, Google) resigned Dec 3, 2019;
3. Emma Watts (President, Twentieth Century Fox) resigned Jan 30, 2020;
4. Bob Iger (CEO Disney) resigned Feb 25, 2020.
5. Bill Gates (resigned from the board of Microsoft and Berkshire Hathaway), March 13, 2020;
6. Joe Lanniello (CEO of the CBS Entertainment Group) resigned March 23, 2020;
7. Ronald Meyer (President, Universal Pictures) resigned Aug 18, 2020;
8. Kevin Tsujihara (CEO Warner Bros) resigned September 2020;
9. Steve Burke (CEO NBCUniversal) resigned Dec 31, 2020;
10. Phil Griffin (President, MSNBC) resigned January 2021;
11. Jeff Bezos (CEO, Amazon.com) resigned Feb 2, 2021.

Also, as I wrote the Complaint, the following events occurred:

1. In October 2019, former President Trump's Attorney General, William Barr, met with Rupert Murdoch (owner of Fox News, and the former owner of Briggs v Cameron defendant Twentieth Century Fox). (See [HERE](#).) As the article indicates, here was a great deal of speculation about why Barr met with Murdoch
 2. After 13 years, Future Service Inc closed, September 27, 2019. (See [HERE](#).)
 3. After 11 years, Michael Pierce (co-owner of Zero Gravity Management, Inc) closed 212 Degrees Fahrenheit Corporation, January 3, 2020. (See [HERE](#).)
 4. Karyn Temple, the Register of Copyrights, left the Copyright Office in January 2020, and took a job at the Motion Picture Association.
- Also, Jeff Zucker, the CEO of CNN (who was the CEO of NBCU during much of NBCU's theft of my work, 2005-12), announced he would resign from CNN at the end of 2021.

Rather than holding these corporations and their CEOs criminally and civilly accountable, under Donald Trump, the Justice Department just let these CEOs resign.

- Immediately after I filed my BvC Complaint, March 4, 2020, Bill Gates went on a months long talk-show tour, presenting himself as a Covid-19 and an environmental wellness "expert" (although he has no such credentials). In all of these speaking engagement he had the host ask him about an absurd Covid-19 conspiracy theory that Gates has placed molecular microchip tracking devices in the Covid-19 vaccines. His intent was to use this absurd microchip story to encourage viewers not to believe conspiracy theories that involve Gates.
- Two months after I filed the BvC Complaint (and about a month after George Floyd was murdered by police), Hollywood began donating hundreds of millions of dollars to black causes, and hiring black writers and producers --at a time when Hollywood was losing billions, and laying off thousands, due to the Covid-19 theatre closures. Hollywood and big-tech did not explain why they ignored police murders of Blacks for generations before then (Amadou Diallo, Eric Garner, Philando Castile), including the murder of Black children (Trayvon Martin, Eric Garner, Philando Castile). Nor did Hollywood and big-tech explain why they did not support Colin Kaepernick's fight against police brutality and for Blacks' basic right to protest for their own survival. I believe this change was due to my Briggs v Blomkamp Complaint and subsequent action. (Meaning: **everything** that the conspirators and Hollywood and big-tech did **after** I filed the BvC Complaint, **every** gesture of support for Blacks and multiculturalism, was insincere, and done only to mitigate damages for when good-hearted, compassionate and fair-minded Americans found out what the participant/conspirators did. If the participant/conspirators are serious about taking responsibility for their actions, they can issue an apology, and return every penny of profit, with substantial damages.)

• HACKING

I began working on the Briggs v Cameron (BvC) Complaint in mid August 2019, but did not submit it to the court until almost 7 months later, March 4, 2020. Page 56 of the BvC Complaint describes some of the first signs that my laptop and phone were being hacked, which I first observed in late August or early September 2019; culminating with myself videotaping a hacking on January 14, 2020 (roughly three months before I filed the complaint). But by summer 2020, I would learn that the conspirators began hacking my computer and phones two decades earlier.

- You will find several videos on this website. One of these videos is from October 11, 2019. This video shows the strange way Internet Archive crawls of key pages began redirecting to other addresses, and is included to show that I began to suspect that I was being hacked, many months before my complaint was filed.

- **Hacking Caught On Video Tape**

On January 14, 2020, I discovered how the the conspirators' fake Google URL and fake Internet Archive crawl scheme worked, by comparing the URLs in my Google browser to my Explorer browser. Immediately after I discovered how the conspirators' scheme worked, Google stopped manipulating its Chrome browser, and displayed the correct URLs. However, although the actual URLs were now visible, the URLs in question all had fraudulent elements in them.

Quickly, I began making a video for the court, to explain how the fake Chrome URL and fake Internet Archive crawl scheme worked. Then, while making a video, I happened to film the hackers (Weinstein and MovieLabs) permanently remove a web document that I had just filmed and described to the court. This video can be viewed on this site, below, or at <https://www.youtube.com/watch?v=5pUX3T3iTY>. (Reading page 100 of the BvC Complaint will help to understand the video.) Evidence of the hacking occurs about 7 minutes and 15 seconds in. The BvC Complaint also describes and explains the Internet Archive app's improper URLs and improper redirecting, and more. See BvC Complaint, pp 100 and 115; and see:

1. https://www.youtube.com/watch?v=b-j5SQ4_NHg.
2. <https://www.youtube.com/watch?v=IKxuSUXEsQc&t=23s>.

- **The NSA Announced A Major Google Vulnerability, Jan 14, 2020, The Day I Videotaped The Hacking**

January 14, 2020 (the same day that I solved Google's and Internet Archive's fake URL and fake crawl scheme, and the same day that I videotaped the hackers hack into my computer), the National Security Agency (NSA) announced, in several news outlets, the discovery of a new "serious vulnerability" that could be used to create malicious software that appeared to be legitimate. The flaw "makes trust vulnerable." (See [HERE](#).) (See Briggs v Cameron Complaint, pp 96 and 100.) The conspirators ostensibly exploited this vulnerability.

- **Microsoft's Hacking & Business Fraud**

On June 6, 2007, a fictitious business named South East Film Association/Club sent a viral email to my computer, which erased 2 years of my outgoing Microsoft Hotmail email, from May 2005 to June 2007. (See BvC Complaint p 56, 57.) This was an ill-conceived effort to try to erase all evidence of my screenplay (with the new aggregated data and GenLab elements). Bill Gates and Paul Allen (who owned Hotmail) directed this virus, or faux-virus, attack. I suspect this because I am unfamiliar with a virus that erases outgoing email—although I am no cyber-virus expert. To this day I have never erased any email sent from any of my email accounts.

The Complaint (p 56, 57) explains how the conspirators used Register.com and Corporate Service Company (CSC) to expunge and erase all ICANN WHOIS internet registry information on South East Film Association/Club, and reset the ICANN registry to indicate that the company/site was created in October 22, 2019 (the very time that I was investigating the website), to indicate that South East Film Association/Club did not exist until 2019; despite the fact that it existed in 2007—and sent me an email that survives to this day. At the time of this email "hacking," Microsoft's business certificate showed that it used CSC as its agent for service of process.

- Almost immediately after the Biden administration took office, February 26, 2021, the ICANN (Internet Corporation for Assigned Names and Numbers) website announced that ICANN had revoked the credentials of "Net 4 India Limited". Net 4 India Limited is the webservice the conspirators used to fraudulently alter web documents, and falsify the WHOIS internet registry information for South East Film Association/Club (described above). You can see this announcement [HERE](#). The Biden administration took this action as a result of my court filings.
- **Google & Internet Archive's Internet Fraud & Abuse**

The Internet Archive produced countless demonstrably falsified website crawls of dozens of fake web articles created by the conspirators. The Internet Archive modified it's web app, so that when a user enters the web address of one of the conspirators' fake websites into the Internet Archive's search bar, the app redirects to the fraudulent and fake crawl pages, which displayed improper URLs.

To support this scheme, Google manipulated its Chrome browser to display fraudulent URLs (which appeared valid) of the falsified Internet Archive crawls. (See BvC Complaint, pp 26-50, and 96 to 121.)

- **Disappearing Federal Webpages Concerning Steve Weinstein**

On several occasions, after I attached web documents concerning Steve Weinstein to my legal filings (with accurate and valid URLs), the web pages later changed, significantly. Most recently, on December 16, 2020, I filed my Opening Brief with the Ninth Circuit; on Page 3 of this brief, I provided a screenshot of the US Sixteenth Air Force website (at: <https://www.16af.af.mil/News/Photos/igphoto/2001899947/>), which featured a photo and caption of Steve Weinstein teaching a group of adults at Stanford's "Hacking for Defense" class. After I filed the opening brief, this web page was removed, and the URL redirected to an archival address (at: <https://www.16af.af.mil/News/Legacy/?Page=66>). Weinstein's photo was buried on the new archival URL, and the photo no longer featured the original caption. The site was clearly created to hide what "Hacking for Defense" is. Moving this Sixteenth Air Force page could only have been ordered by Donald Trump or someone at the US DoD.

Because of the alteration of these webpages, I requested permission from the Ninth Circuit to submit a Corrected Opening Brief, to report this alteration to the court. The Ninth Circuit denied this request, but I have uploaded a PDF of the corrected brief on this site, for verification.

- Thankfully, after I published this website, February to March, 2021 (shortly after Joe Biden took office), the first Sixteenth Air Force webpage, linked above, was restored. The second webpage, on the archival site, is still there, and appears even more elaborate. I suspect this archival page was

created to give Steve Weinstein cover, as a US Defense Department agent. It is shameful that the US government would provide cover to people who are engaged in stealing honest Americans' intellectual property.

- Immediately after I reported to the court that Steve Weinstein teaches "Hacking for Defense" at Stanford University (see Aug 25, 2020, Amended Second Declaration, and Third Motion in Limine), new web pages concerning Weinstein began to pop up online. These new webpages suggested that "Hacking for Defense" is part of an innocuous youth environmental entrepreneurial mentoring program. It is not.

In Court Filings, Google Admits to Sabotaging My Personal Film Marketing Efforts --As Their First Amendment Right

In 2012, Google arranged to make my online efforts to market my own film projects and screenplays (on services such as KickStarter and Indiegogo) NOT appear in Google's Chrome search results. (See BvC Complaint p 57, 58.) Google's manipulation and control of search results can also be seen in The Amended Second Motion In Limine, pages 5 and 6. Google admitted to these charges in its motion to dismiss, filed May 22, 2020 (see [HERE](#)), stating:

- "...Google's choices in omitting certain websites from search results while allowing others to appear is protected by the First Amendment." (p 9)
- "Again, designing an algorithm that results in some pages being shown and not others is not actionable under First Amendment principles,..." (p 10)

MOVIELABS - PART 2:

MovieLabs Patents Its Method For Hacking Me & Distributing The Stolen Property To The Big 6

MovieLabs called itself an "R&D" (research and development) company for 14 year (see [HERE](#)), but after I alerted the court, in August and September of 2020, of the evidence that MovieLabs and Steve Weinstein are an organization of hackers, MovieLabs suddenly changed its California business statement of information, and now, as of January 11, 2021, MovieLabs claims to be a not-for-profit **Trade Association** (see: [HERE](#)). Although MovieLabs claimed to be an R&D company for 14 years, it only applied for **three** patents those 14 years, in 2007 and 2009 (and two of the patents appear simplistic and fraudulent, and one appears unlawful). Meanwhile, most technologies companies (like Sony) apply for dozens, even hundreds of patents EVERY year. MovieLabs is not an R&D company or a trade association. It is a hacking company.

Bizarrely, the Big 6 and MovieLabs were so confident that they would make huge money from hacking into my computer and phone(s), that they actually patented their method of hacking into my computer(s) and phone and giving the ideas stolen from my screenplays, shorts, books—and even my conversations, to the Big 6 film companies.

You can read brief abstracts to MovieLabs three patents [HERE](#).

MovieLabs first patent (2007), number 8655826, is a very generic verification system. I found no evidence that anyone is using MovieLabs technology. It appears as if this patent was submitted just to make the company appear credible.

The third patent (2009), number 7979464, is a patent for putting data in a simple software folder when downloaded. This is not patentable because it had been done, automatically and free of charge, for two decades before MovieLabs.

But the second patent (2009), number 8015283, is MovieLabs' patent for their method of hacking me and sharing the data with Big 6 film studios. The abstract reads:

- "Abstract: Particular embodiments include cooperative monitoring of peer-to-peer activity on a network including maintaining communication between a local monitoring process and a network monitoring process such that a process can use both network monitoring and local monitoring. The cooperative monitoring includes monitoring a local peer using local monitoring of a point in the network by monitoring packets passing through the point, monitoring the network using network monitoring by a monitoring system or agent coupled to the network, and analyzing the result of network monitoring and local monitoring to determine at least one file transfer association with the local peer."

You can read MovieLabs patent for hacking me on the Patent Office website, [HERE](#).

You can see the illustration that MovieLabs created for its system, at bottom of the first page. The illustration looks exactly as you may have imagined. In the illustration, I am represented by the entity named "Local peer," and MovieLabs (and Steve Weinstein and his cohorts) are the "Local monitor." The patent itself explains that the "local monitor" collects the information (AKA "packets") stolen from me ("local peer"), then distributes this stolen information through "a network address translation (NAT) router," which then delivers the stolen information to the "Remote peers".

MovieLabs Email Declares How Valuable My Ideas Are To The Film Industry, And Shows MovieLabs Derives No Legitimate Income

In 2014, Wikileaks released an email from Mitch Singer (Sony Pictures' CSO and a MovieLabs board member) to Leah Weil (Sony Pictures' legal counsel), in which Singer states how important stealing my ideas were to the film industry. Singer wrote:

- "Leah, I'm in a MovieLabs Board meeting and based on the increase in the number projects and the importance of many of their projects to the industry, they will be asking for a 5 percent increase in their budget for an additional research engineer."

Singer is discussing the fact that stealing my ideas was vitally important to the industry. No, he does not use my name. But there is no other explanation, as MovieLabs' patents show that they have not produced ANY technology that the industry uses, and shows that MovieLabs has patented a hacking system. The Big 6 make about \$300-Billion per year. If MovieLabs had a deserving technology they would be mega-millionaires, or billionaires. MovieLabs hacks. Further proof that MovieLabs is illegitimate is found in the remainder of this email, as Singer asks Weil for a budget increase. Singer writes:

- "...they will be asking for a 5 percent increase in their budget for an additional research engineer. There is support from the Movielabs Board for the increase, including me. No formal vote was taken. Movielabs budget for 2013 was 4.8M. Historically it has averaged 5.4M. they will be asking for slightly more than 5M. More than happy to discuss in more detail."

It is illegal for a parent corporation to pay a subsidiary's budget (see Opening Brief, pp 4, 34). A company buys a subsidiary because that subsidiary has a client base and is making money. But MovieLabs has no clients, and is begging the parent for money. [NOTE: In this email MovieLabs is seeking another hacker ("researcher") to monitor me, because, in October 2013, I sued Sony Pictures and Neill Blomkamp (Briggs v Blomkamp), and the Big 6 wanted to observe my work on this lawsuit.] This email can be seen [HERE](#).

**EVIDENCE THAT 9TH CIRCUIT CHIEF JUDGE
SIDNEY R THOMAS IS ENGAGED WITH THE CONSPIRATORS
AND HAS FALSIFIED HIS ARIZONA BUSINESS FILINGS
TO HIDE HIS CONNECTION TO THE CONSPIRATORS**

Because of the unusual rulings that I experienced at the hands of the Ninth Circuit (Briggs v Blomkamp, 2018), I decided to do some routine investigation on a few Ninth Circuit Judges. I chose to start with Chief Judge Sidney R. Thomas, who chooses which judges will hear each appeal, he the most powerful judge on the Ninth Circuit.

My investigation into Thomas was simple: I entered his name into the OpenCorporates.com app, to see if his name popped up on any business registrations. There, I found "Sidney R. Thomas" listed as a manager or agent on two Arizona (AZ) businesses: Thomas-Hume Holdings, LLC, and Trinity Property Development, LLC.

Amazingly, the first of these businesses, Thomas-Hume Holdings, LLC, was formed September 2006, just 6 months after ZGM accessed my work. (See [HERE](#).)

More amazingly, the second company was formed on January 11, 2007, just weeks after the new revised version (the aggregated data version) of my script appeared on TriggerStreet.com. (See [HERE](#).)

At the Arizona Corporation Commission's website I noticed that some of the listings for Sidney R. Thomas did not have the "R" in the name, and some added the suffix "III" ("the third") to the name. Thus, some of the listings appeared "Sidney R Thomas III." So, for example, on the second link (above) Trinity Property Development, LLC, both names appear on the webpage; at the top of the page the name is "Sidney R Thomas III", but at the bottom of the page the name is "Sidney Thomas". This was curious because when I searched on OpenCorporates.com, I didn't notice a "III" suffix on the names returned.

On the Thomas-Hume Holdings webpage, I clicked on the "Document History" link. The link took me to an "entity information" page with links to two documents: 1. "Articles of Organization" and 2. "Miscellaneous Document". But both links showed the same document, the "miscellaneous" document, an "Application for Registration of Corporate Name." About 90-120 minutes later, when I clicked on the "Articles" link, again, the Articles of Organization document suddenly appeared.

Even more amazingly, Trinity Property Development LLC was formed Jan 11, 2007, a month after I introduced the concept of "data aggregation," and introduced the idea of scanning human bodies and brains to make perfect digital reproductions (to insert into a massive universe simulation, the "GenLab" or "The Accelerator"). Why does this matter? Because the second page of Trinity Property's Articles names 3 partners: Sidney Thomas, Randy White, and Chris Jaska. Chris Jaska is an engineer for Spectra-Physics, a company that makes bio-imaging lasers. See Spectra-Physics' bio-imaging lasers [HERE](#). See Chris Jaska [HERE](#), and [HERE](#) (scroll down, you'll see Jaska has been with Spectra-Physics since 2001).

Bio-imaging lasers take extremely detailed 3D images of people's bodies (and brains). They're the lasers you'd want to use if you planned to make 3D cyber copies of a body and/or brain. Spectra-Physics' YouTube page actually shows its laser doing some brain and body scans:

<https://www.youtube.com/watch?v=MaGhrF7AotA> . Eighteen seconds into the video you'll see footage of a scan of a mouse striatum (center of a brain).

Clear Proof Of Fraud & Falsification (#1)

So, what follows are links to the PDFs of the Articles of Organization (business registrations) for Sidney R. Thomas' businesses, posted on the Arizona Corporation Commission's website. Then I'll show you verifiable evidence that they are fake.

Thomas-Hume Holdings LLC's Article of Organization link led to this document: [HERE](#).

Thomas-Hume Holdings LLC's "Miscellaneous" link led to this document: [HERE](#).

Trinity Property Development, LLC's "Article of Organization" link led to this document: [HERE](#).

Trinity Property Development, LLC's "Miscellaneous" link led to this document: [HERE](#).

(For safety and verification, I have created a combined PDF of these 4 filings: [HERE](#). If you you choose, you can verify the PDFs you find on the Arizona Corporation Commission's website, against the PDFs that I found.)

So, what is the evidence of document falsification and fraud in these document?

There is lots of it. But I'll start with the catastrophic fraud and falsification.

Look at the upper left corners of the Articles of Organization for both

Thomas-Hume Holdings, LLC and Trinity Property Development, LLC. You will see short dash lines below the Arizona Corporation Commission's barcode; as if someone stuck a barcode sticker on the document, or cut out a barcode in a photo editor and added the barcode to the document with the same photo editor. That's because someone DID use a photo editor to add the barcode from the original documents to these fake PDFs.

How can I prove this? By comparing the fake AZ Articles to valid AZ Articles.

The Arizona Corporation Commission uses a neat and efficient stamping system that leaves a very clean and distinct barcode, with no lines or smudges. Consider the following 11 documents that were filed at the same time as the fake documents.

1. See CHC, LLC's Articles of Organization from September 1, 2006; See [HERE](#).
2. See GLOBAL BENEFITS CONSULTANTS, LLC's Articles of Organization, Jan 10, 2007; see [HERE](#).
3. See MOUNTAIN PARK RENTALS, LLC's Articles of Organization from Jan 10, 2007; see [HERE](#).
4. See STRENGTH-N-LENGTH PILATES, LLC's Articles of Organization from Jan 10, 2007: [HERE](#).
5. See FOLEY PATENT CONSULTING, LLC's Articles of Organization from Jan 10, 2007: [HERE](#).
6. See UV INDUSTRIES LLC's Articles of Organization from February 12, 2007: [HERE](#).
7. See BUTTERFIELD TRAIL, LLC's Articles of Organization from January 10, 2007: [HERE](#).
8. See FM INVESTMENTS LLC's Articles of Organization from January 30, 2007: [HERE](#).

These following final three Articles of Organization are particularly telling because they were filed by Randy White, who is named as a "vested manager" (partner), along with Sidney Thomas and Chris Jaska, in the Articles for Trinity Property Development, LLC. These filings are for three businesses that White owns, without Sidney Thomas or Chris Jaska.

9. See PRAISE COMMUNITY CHURCH's Affidavit of Publication from October 5, 2009: [HERE](#).
10. See PCIC INC's Articles of Organization from May 25, 2011: [HERE](#).
11. See NKB TECHNICAL SOLUTIONS, LLC from November 25, 2014: [HERE](#).

If you are checking my work, I have made a combined copy of the of all 11 PDFs of the Articles of Organization, just as I found them on the Arizona Corporation Commission's website. See 11 valid AZ filings [HERE](#).

More Clear Evidence Of Fraud & Falsification (#2)

If you compare both pages of the Articles of Organization for Trinity Property Development LLC ([HERE](#)), you will notice that the margins on the left side of the page (the portion where it says: "DO NOT PUBLISH THIS SECTION NOTE" at the top) are at a slight, but noticeable, angle on the first page. And you'll notice, on the second page, this angle is much sharper. You will also notice that there is a grey background in this left margin area on the second page; but on the first page, the background in the left margin area is white. This indicates that these pages were printed on different printers, or on different settings

Now, if you compare this fraudulent document to the 11 other legitimate filings that I've linked, above, you'll notice that:

1. All of pages in those 11 separate filings are consistent and uniform (meaning, each page has the same duplication quality):
2. All of the valid filings that use the AZ Corporation Commission's forms (with writing in the left margin) are consistent and uniform, none of them have a white background on one page and grey on another. (See valid docs #2,3,4,5,7.)
3. On the few valid documents that were duplicated at a slight angle, all of the pages of those documents were duplicated at the same angle (with the exception of documents that are composed of multiple documents; in which case, all of the separate documents were duplicated at the same consistent angle).

The fact that the Articles of Organization of Trinity Property Developers LLC are inconsistent in printing quality—between the two pages, AND the fact that the angles that the pages were printed at are noticeably different, shows that these pages were not printed by the Arizona Corporation Commission, and they are fake.

A Few Smaller Signs of Fraud (#3)

There are about 3 more problems with the Trinity Property Development LLC page.

ONE. In the Articles of Organization of Trinity Property Development, LLC, on page one, section 3. Line 1 and 4, the person who filed this document carefully wrote "Sidney R. Thomas, III", twice, on lines 1 and 4, of section 3. But on page 2, section 6, line 4, a person alleging to be Thomas, writes his name "Sidney Thomas," and writes "Sidney Thomas," again, after his signature (bottom of page 2). That's a curious inconsistency, because the two pages do NOT appear to have been printed from the same printer.

TWO. The signature don't match. There is a signature at the bottom of page one, and another at the bottom of page 2. They don't match.

THREE. Trinity Property Development LLC is composed of three partners (Sidney R Thomas, Chris Jaska and Randy White). The Articles of Organization for Trinity Property Development was signed and submitted by Sidney R. Thomas, on January 11, 2007. But Trinity Property Development's "Application For Reservation of a Corporate Name" was filed by Randy White on January 11, 2007. See [HERE](#); or [HERE & HERE](#).

It is unlikely that two different partners would fill out these two forms and file them separately. Logically, only one partner would file these forms. I suspect someone unlawfully changed the first page, to add "III" to the end of Thomas' name.

HOW I TWICE MET / ENCOUNTERED STEVE WEINSTEIN, IN 2017/2018

In 2016, to write my book, *Morons Don't Ride Harleys*, and to attend some legal affairs (copyright), I left my job at a high school in Redwood City.

In 2017, finished with my book, I began looking for a new job. I primarily used Indeed.com in my job search. Away from writing, I've always, primarily, worked with at-risk and emotionally troubled kids (anger management). Although Indeed sent me a reasonable variety of job listings, clearly the best fit, of the job listings that suited my background, was a makerspace "Tinkerer" position, in the Ravenwood school district, an under income, minority district in East Palo Alto, California (just a few miles from Stanford University). In the end, I accepted this position in September 2017, and worked as a "tinkerer" in the Ravenswood school district, from September 2017 to around July 2018.

Here's where it get interesting, if not weird.

The roughly 6 Ravenswood makerspace classes (at 6 different schools) were all sponsored by **Stanford University** and Facebook, and were largely funded/supported by Google (Alphabet Inc). You might recall that **Steve Weinstein** teaches "Hacking for Defense," at **Stanford University**. [To see that Stanford, Facebook & Google all finance Ravenswood's makerspaces, see [HERE](#), and [HERE](#), and [HERE](#), and other online sources (or see PDFs [HERE](#), and [HERE](#), and [HERE](#).)]

But it gets more curious.

While I was working as a tinkerer in the makerspaces in Ravenswood's "Cesar Chavez" and "Los Robles" schools, I and the other tinkers, and our makerspace leadership team, were required to attend various trainings and makerspace "conventions," which were all held a few miles from Ravenswood, at Stanford University. These trainings occurred about every 4-6 weeks. At least two of these trainings were multiple day trainings, 2-5 days. And one of these multiple day trainings (which I believe was a 3 day training), involved makerspace leaders and pioneers from around the world, and Steve Weinstein was very certainly at this training. The main training room at this particular training was fairly large (able to accommodate about 200 visitors), and the seats were positioned in semi-circular rows. Weinstein did not speak, as I recall, but he sat in the front row, where most of the leadership and speakers tended to sit. And for at least 2 days he positioned himself where he could see me (I tended to sit in the middle or back rows, toward the outer wings). I remember this quite clearly, because I am decidedly aware of my surroundings, and I found his semi-regular glances in my direction uncomfortable and unusual. After one of the breaks, I moved to another location in the classroom, hoping to sit a few rows behind him, where he'd have more difficulty glancing at me; but Weinstein also moved, to a position where he could glance at me, at will.

Perhaps more curious, during my first 2 months as a Ravenwood makerspace tinkerer, I was told that a group of international visitors wanted to come visit my makerspace, to see the kids, the tools and crafts, and to see me work with the kids. I welcomed the guests, a large group of 12-20 adults. Although my students were probably 90% minorities (Latinos, Pacific Islanders, Blacks), the visitors were disproportionately White (from around the nation, and the world, as I recall). But in this group of visitors was Steve Weinstein. I greeted all of the visitors, and shook hands with some/many, but I don't remember exchanging names. I can't recall if Weinstein gave me his name, or introduced himself or shook hands, but he was in this group of visitors. Of course, I had no idea, then, that he was involved in hacking and stealing my property.

- Ravenswood does a great job, under challenging circumstances, and their tinkers and makerspace team, top to bottom, are fantastic. Makerspaces are a great idea (and funding them is an even better idea); but allowing corporations like Facebook and Google to target low income communities, to develop tracking tools to learn the interests and habits of low income minorities (who these companies refuse to employ, and view as "suspects") is sickening and un-American.

NATIONAL NEWS MEDIA FRAUD & DISINFORMATION

Pages 25-55 and pages 96-121 of the Briggs v Cameron Complaint show that the conspirators relied on over a dozen national publications to produce numerous fraudulent and backdated articles. The proof of the fraudulence of most of these articles is confirmed by their fraudulent Internet Archive crawls, and other problems. Although some of the publication fraud and falsification may have been carried out by independent actors inside of these publications, many of these publications were owned by the conspirators (e.g., Amazon owns IMDb; MRC and Penske own Hollywood Reporter, News Corp owned IGN; Wikipedia was an original "Lobby" participant). Some publications, such as Bloomberg (who also owns BusinessWeek) appear to be ideological supporters, but may not have been active, regular participants. The national news and media outlets that produced the falsified documents (described in BvC Complaint were: Bloomberg.com, Los Angeles Times, Hollywood Reporter, Ain't It Cool News, The Guardian, Business Week, Variety.com, EW.com (Entertainment Weekly), EndGadget.com, MTV.com, IGN.com, JoBlo.com, MovieBytes.com, ComingSoon.net, IMDb, Wikipedia.

And on cue, March 16, 2021, immediately after I published this website/article, Cade Metz released a book about how great AI (artificial intelligence) is, stating that AI is a very necessary but misunderstood tool, and claimed the problems are not with AI or its programmers, the problems

are in the information that is widely available, online, which causes the AI to form biases against minorities. Metz's argument seems tailored by Russia (who seems to prefer a divided and weakened America).

And, on cue, immediately after Metz's book was released, the conspirators (who own CBS, ABC, NBC, CNN, MSNBC and FOX...) began to have Metz on their live TV news shows, to calm all concerns about the AI (data scrapers) the conspirators have injected throughout American commerce. On

March 15, 2021, the New York Times (a publication I once respected) featured a piece about Metz's book. (See [HERE](#).) I refuse to say the name of Metz's book, but you can see it [HERE](#). As you see on the cover, Metz exclusively singles out for praise the "genius" "mavericks" at **Google** and **Facebook** (the companies that have allowed the deepest Russian infiltration into America).

Metz and the people who published articles about his book and invited him on TV are clueless. Here's why: If you are trying to create an AI to do an aggregated data-based predictive policing system, you need to feed that AI valid data. But the conspirators have created a propaganda arsenal that manufactures lies (Google falsifies web information and search results; Facebook manufactures fake hate and disinformation accounts). Do we want an predictive police system that tells us what fake people are going to do? Russia would love us to have this sort of disinformation-based system. You can't predict anything with an aggregated disinformation system.

STUXNET

- This "Stuxnet" portion of this article was researched and written from April 11, 2021 to April 19, 2021, while the rest of the article was written in February and March 2021. Thus, to avoid the arduous work of rewriting the entire article (to integrate these facts), and for continuity, I have moved this Stuxnet section to the end of the article.

In 2010, the world was introduced to the "Stuxnet" computer virus. But, as Kaspersky Lab reported in 2010, the Stuxnet virus secretly dated back to 2009—to the moment when the virus was first inserted into my computer.

Stuxnet was such an advanced and unprecedented virus that it is uniformly believed to have been made by the US government, perhaps with Israel (the US government does not deny this); but all experts agree that only an extremely advanced government (not a single corporation or person) could have created Stuxnet. (See <https://en.wikipedia.org/wiki/Stuxnet>.)

Here are a few comments about Stuxnet, from Wikipedia:

- "Kaspersky Lab concluded that the sophisticated attack could only have been conducted "with nation-state support." [E-Secure](#)'s chief researcher [Mikko Hyppönen](#), when asked if possible nation-state support was involved, agreed "That's what it would look like, yes." "
- "On 1 June 2012, an article in The New York Times said that Stuxnet is part of a US and Israeli intelligence operation named [Operation Olympic Games](#), devised by the NSA under President [George W. Bush](#) and executed under President [Barack Obama](#)."

To this day, Stuxnet is regarded as one of the most innovative and sophisticated viruses ever —perhaps only rivaled by the SolarWinds virus of 2020—which was inspired by Stuxnet. One of the most amazing things about Stuxnet is that it contained 4 zero day exploits. As Kim Zettters explained in Ars Technica "Out of more than 12 million pieces of malware that antivirus researchers discover each year, fewer than a dozen use a zero-day exploit." The fact that Stuxnet used four zero day exploits suggests that Microsoft (and Bill Gates and Paul Allen) helped the US government create Stuxnet—which only targeted Windows computers. The Stuxnet virus was unprecedented because of its functionality: it allowed the controllers/creators to observe an infected computer, take files, take control of the computer, or destroy all files and hard-drives.

You might wonder how the conspirators got the US involved in making Stuxnet, and why? That answer flows from the primary facts previously presented in this article. I'll explain...

After conspirators saw the December 2006 version of Butterfly Driver screenplay (which introduced the world to the concept of defense and policing systems based on aggregated data, etc.), which they accessed either on TriggerStreet.com or via Steve Weinstein's hacking apparatus, "MovieLabs," the conspirators contacted the US government about my new ideas. But rather than simply asking me if they could use my ideas, the US government chose to erase all digital evidence of my ideas from my computers and storage drives. (To be clear, I would not have agreed to allow the US to create this advanced spying and data collection system, because these ideas were created to showcase the evil potential of government without morality.) Thus, sometime in early 2007 (perhaps mid 2007) I was besieged by a very aggressive and destructive virus, which destroyed many files. However, this 2007 virus was not Stuxnet. But, like Stuxnet, it travelled via USB, so it may have been a Stuxnet prototype. This 2007 virus, ".Trashes", is discussed at the end of this Stuxnet segment.

Shortly after this 2007 virus, around August 2007, I decided that I would begin making my own films, so I wrote a film called "The Amazing Mr. Excellent," which I thought I'd be able to film for under \$20,000. By January of 2008, I had assembled a film crew. We began

filming around May 2008. But during post production, late 2008, I began experiencing technical problems which severely delayed production. These technical problems may have been related to computer viruses. If so, these viruses were less destructive than the 2007 virus, and FAR less destructive than the coming 2009 Stuxnet virus.

Production of The Amazing Mr. Excellent moved forward. Then abruptly, in December 2009, while I was working on the score and soundtrack for the Amazing Mr. Excellent, the Stuxnet virus launched on my computer. The virus was so severe that it destroyed about 4-5 hard-drives and 3-4 external hard-drives, destroyed 8 years of my music composition files, almost ruined the film The Amazing Mr. Excellent, and almost ended an important friendship.

Around January of 2010, after the 2009 Stuxnet virus destroyed several hard-drives, a friend and film crew member (named Matt) offered to let me to use his external hard drive. I accepted. The virus immediately destroyed Matt's hard-drive. In April 2010, I sent the first of several emails to The Amazing Mr Excellent cast and crew, explaining the devastating impact of this virus, spreading through my USB drive. (Stuxnet spreads exclusively via USB drive.) The first such email was sent on April 12, 2010, two months before the Stuxnet virus was first discovered. My first email about the virus can be seen [HERE](#). (This email went out to about 100 cast and crew members, whose email addresses have been redacted; thus, the first portion of the email is blacked out, but none of the actual email text, below, is omitted). As you can see from the Gmail time and date stamp on the email, this first email was sent out on April 12, 2010. And, as you can see from reading the email, the virus caused a serious argument between Matt and me. And, as you can read on page 2 of the email, I explained that the virus hit me in December 2009 —although evidence, presented later, suggests the virus was installed on my computer over 9 months earlier.

But before we further examine Stuxnet's origins, please briefly re-examine my April 12, 2010 cast and crew email. You will notice in paragraphs 2, 4, 6, 9, 12, 13, I never referred to the film as "The Amazing Mr. Excellent"; rather, I (and the cast crew) simply called the film "Mr. X". In fact, as you can see, [HERE](#), in this PDF screenshot of my Hotmail inbox from 2008, by November 2008, the cast, crew and I almost exclusively called the film "Mr. X". This is essential, because the original name for Stuxnet was MRx, a variation of "Mr. X."

STUXNET GETS ITS NAME

Stuxnet was originally named "MRx", or Mr. X. Microsoft, a central The conspirator in this matter, re-named the virus "Stuxnet," in September 2010.

As Wikipedia explains, Stuxnet was first discovered by the Belarusian antivirus company VirusBlokAda, on June 17, 2010. VirusBlokAda did not call the virus "Stuxnet"; the virus had no name. VirusBlokAda ONLY reported that the virus had two main files, named mrxnet.sys and mrxcls.sys. The original VirusBlokAda report can be seen at <http://anti-virus.by/en/tempo.shtml> . This article was crawled by the Internet Archive (see: <https://web.archive.org/web/20100722095105/http://anti-virus.by/en/tempo.shtml>) . The evidence indicates that Internet Archive's Wayback Machine is no longer a reliable service, and should not be trusted; however this crawl is legitimate.

The VirusBlokAda report reached few people, because VirusBlokAda is antivirus company, with a limited audience. The Stuxnet virus was next reported, semi-broadly, 28 days later, July 15, 2010, in Brian Krebs' blog "Kreb on Security." But, once again, the virus had no name. Brian Krebs' original article can be read at: <https://krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw/> . As you see, the ONLY file names that are mentioned in Krebs' report are mrxnet.sys and mrxcls.sys.

The word "Stuxnet" did not appear in print until September 14, 2010, when Microsoft's Jerry Bryant (Group Manager, Response Communications) used the name "Stuxnet" in a web posting about the virus, which can be seen at: <https://msrc-blog.microsoft.com/2010/09/13/september-2010-security-bulletin-release/> . That same day, Brian Krebs also used the name "Stuxnet" in his second blog about the virus. But Krebs' article referred to, and linked to, Jerry Bryant's posting. Thus, Microsoft's Jerry Bryant's post was the first use of the name "Stuxnet."

Wikipedia's Stuxnet entry cites a July 11, 2011, Ars Technica article "How Digital Detectives Deciphered Stuxnet, The Most Menacing Malware In History," by Kim Zetter, which further explains how Microsoft allegedly gave Stuxnet its name: "...dubbed Stuxnet by Microsoft from a combination of file names (.stub and MrxNet.sys) found in the code."

Microsoft named Stuxnet.

Why "Stuxnet"?

In all of my reading on the Stuxnet virus, the previously cited Kim Zetter's article, in Ars Technica, is the only article that mention a meaningless ".stub" file that was allegedly found in the code. I believe Microsoft and the conspirators gave the virus the absurd name "Stuxnet" to give the virus a name that I would NOT associate with my film. Because, after all, I had suffered an extreme viral attack, while

making Mr. X, in late 2009 —by a virus that behaved exactly like the Stuxnet virus. But the reason that Microsoft had to publicly change the virus' name is because the virus was rapidly spreading through USB drivers—because I was unwittingly giving the virus to other people connected to the Amazing Mr Excellent (who, in turn, were infecting other systems). Thus, a few months after I got the virus and unwittingly unleashed it on the world, the virus was being discussed in major antivirus circles. Microsoft and the conspirators reasoned that if I happened to hear of a virus named MRX or Mr. X, or of a virus' whose main files were named "MRx", and if I learned that this virus allowed the controllers to observe infected computer, steal files, take control of the infected computer, and destroy all files and the hard drives, I might realize that the creators of the MRx virus created that virus to hack into my system, steal my work, and destroy my files and hard-drives.

The Stuxnet Code Shows It Was Named "Mr. X"

F-Secure.com explains the central importance of MRxNet and MRxCls drivers, in the "Technical Details" section, at the bottom of a Stuxnet web-page, at: https://www.f-secure.com/v-descs/trojan-dropper_w32_stuxnet.shtm, I have paraphrased part of the F-Secure.com' article (underlined):

"On execution, the malware drops two files onto the system: mrxccls.sys and mrxcnet.sys, which are dropped in C:\Windows\System32\Drivers folder. The registry keys associated with the 2 dropped drivers are visible:

- HKLM\System\CurrentControlSet\Services\Services\MRxNet
- HKLM\System\CurrentControlSet\Services\Services\MRxCls"

As F-Secure explained, the visible registry key NAMES the two files: MRxNet and MRxCls. In BOTH key names the "MR" is capitalized to set the MR apart from the lower case "x"; then, the N (in the "Net" suffix) is capitalized to set the suffix apart from the "X", and the C (in the "Cls" suffix) is capitalized to set the suffix apart from the lowercase "x". Thus, by all rights, the virus was meant to be called the Mr X virus.

FUNCTIONALITY. The F-Secure.com website also explains Stuxnet's functionality (paraphrased, underlined): "The injection is performed by the mrxccls.sys file, which is responsible for attaching and copying the DLL into the target process. The rest of the injection routine is carried out by 2 additional components embedded in the mrxccls.sys file, which are also loaded into the same process space. The file mrxcnet.sys checks for files on the system with the following extensions: .TMP, ~WTR, .LNK. If a match is found, the files are hidden by modifying the FileInfo structure.... If the targeted files are not found, Stuxnet will save copies of itself as TMP files onto an available removable drive, using the following filenames: ~WTR4132.tmp - Main installer from the USB drive..."

Stuxnet's Earliest History;

When Stuxnet First Infected My Computer

In Wikipedia's Stuxnet article, Kaspersky Lab (a world leader in antivirus) speculated that a variant of the Stuxnet worm first appeared in June 2009. Specifically Kaspersky stated:

- "Kaspersky Lab experts at first estimated that Stuxnet started spreading around March or April 2010, but the first variant of the worm appeared in June 2009."

Steve Weinstein and MovieLabs could have inserted Stuxnet on my computer, at any time in 2009. However, I suspect the virus may have been installed when I opened an unexpected email, sent by Google, on March 1, 2009 (a few months earlier than Kaspersky speculates the worm first appeared). This email was not responsive to anything that I sent Google. It just appeared in my email box. I first opened my Google email (Gmail) account 6 weeks earlier, in January 2009. A PDF screenshot of the March 1, 2009 email from Google, in my Gmail box, can be seen [HERE](#).

Why Would The US & The Conspirators Make Such An Boneheaded Mistake As To Name Both Of The Primary Files "MRx"?

It's hard to guess why the US government and the conspirators would name make such an obvious mistake as to name the primary virus files MRX. But I think there were two reasons.

First, the development of the Mr X virus (later named the Stuxnet virus) started under President George Bush (in early 2007). The fact that the virus was launched onto my computer in March 1, 2009, only 6 weeks after Barack Obama took office, suggests that Barack Obama was not aware of the MR X virus (Stuxnet) or the plan to unleash it to erase all of my files. However, other parties who were still in the US government, leftover from the Bush administration, likely wanted to release the virus before the Obama administration killed the plan. So the conspirators may have been working too quickly to change the MRx files names.

Second, I don't think the US government and the conspirators thought that Stuxnet would go beyond my computer. I think the conspirators thought that the virus would destroy my computer(s), then I would realize that the infection was on my USB drive and I would

stop using the USB drive, and destroy it. At that point, the conspirators would have destroyed all evidence of my files, and the Mr X virus could be retired. Unfortunately, for everyone, since my USB drive was fairly new, I was slow to realize that the infection was on the USB drive. Complicating matters, I had several other important files on the USB drive (including Mr. X music files). So, after the virus destroyed my computer(s), I unwittingly infected other friends and associates computers, as I worked to complete the Mr. X soundtrack and fight the insanely aggressive virus.

Why Stuxnet Works On USB

As explained earlier, in early 2007, shortly after I introduced the the collected concepts of defense and policing systems based on data aggregation, I was suddenly hit with a severe virus that wiped out many files, erased many 3.5-inch floppies, and may have destroyed a hard drive. As a result, moving forward, I made an effort to disconnect my computer(s) from the internet, and I tried to keep one computer offline. Thus, I believe it became harder for the conspirators to hack into my system, or to know if I might have another computer that they weren't aware of. Once the conspirators decided to destroy all possible evidence of the December 2006 version of my Butterfly Driver screenplay, they resolved that the best way to execute that plan was to infect whatever computer I connected to the internet with a virus that would attach itself to any storage drive that attached to a USB port (because I sometimes transported files between the two computers). By creating a virus that moved this way, and by observing my activities (using the new Stuxnet spying utilities), the conspirators could see what files I was transferring, if any, then trigger the destruction of any hard-drives and files they wished.

The Suffix Names

My theory on the suffix names (three ending letters) of the MRx virus driver files is pretty simple: I believe that when the US government first conceived the MRx virus (Stuxnet), it was one single virus file, named MRxNet (or mrxnet.sys). This virus was created to spy on me and eventually destroy all of my files and hard-drive. This virus was named MRxNet, because it was designed to infect a computer that I often connected to the internet.

However, as the US designed the virus they observed that my internet behavior had changed (because of the 2007 virus), and I appeared to be using more than one computer, and one of these computers was rarely, or never, online; it was on a closed system. And this closed system computer seemed to be the computer that I used for creative writing; so any evidence of the December 2006 version of Butterfly Driver (which the conspirators hoped to erase) was likely on the closed system computer. The US and the conspirators also likely noticed that sometimes I transferred files between the two computers. Thus, the US and the conspirators hatched the idea of a virus that could be transferred by USB drive, to infect the closed system computer. Thus, the suffix "CIs" in the name MRxCIs, likely stand for Closed.

BACKDATING STUXNET

In 2017, eight years after the MRx (Stuxnet) virus appeared on my computer, the US tried to fraudulently backdate the origin of Stuxnet by releasing a fake Wikileaks "Note", which reads: "[Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation](https://web.archive.org/web/20101230121529/http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/)". The "note" claims that Stuxnet may have began destroying Iranian nuclear labs as early as June 2009. But the quickest way to show this document if fraudulent is by clicking on Wikipedia reference link, which leads to this Internet Archive crawl page: [https://web.archive.org/web/20101230121529/http://mirror.wikileaks.info/wiki/Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation/](https://web.archive.org/web/20101230121529/http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/)

But, if one enters this article's web address in the Internet Archive's Wayback Machine, the fraudulence is revealed. As you can see above (if you understand Wayback URLs) the article's root address is:

[http://mirror.wikileaks.info/wiki/Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation/](http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/)

But that page does not exist, or can't be reached. But when you enter that same address into the Wayback Machine, rather than going to a valid crawl page, the Wayback Machine improperly adds four digits ("2017") to the URL, and redirects in an invalid URL crawl. A valid Internet Archive Wayback crawl of the address should lead to this address:

[https://web.archive.org/web/*/http://mirror.wikileaks.info/wiki/Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation/](https://web.archive.org/web/*/http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/)

However, the Internet Archive Wayback machine redirects to:

[https://web.archive.org/web/2017*/http://mirror.wikileaks.info/wiki/Serious nuclear accident may lay behind Iranian nuke chief's mystery resignation/](https://web.archive.org/web/2017*/http://mirror.wikileaks.info/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_nuke_chief's_mystery_resignation/)

By clicking on the first address (without the "2017" in the address) you can watch the Wayback Machine improperly add the "2017" to URL, then redirect to a fake crawl. A valid Wayback search is composed only of the Internet Archive's uniform and standard prefix

https://web.archive.org/web/*/, followed by the address that the user enters into the search bar. Thus, if you enter www.paypal.com into

the Wayback search app, the app will direct to https://web.archive.org/web/*/www.paypal.com.

So, why would the US government and the conspirators try to backdate the Stuxnet virus? Because, as shown earlier, the the Stuxnet virus was originally called the Mr X, or the MrXnet virus, and if I became aware of Stuxnet, and learned that the primary drivers were named "MRx", I might suspect Stuxnet was related my film "Mr. X". So the conspirators determined that if they released a story that the virus was created before I and the crew and cast began calling the film "Mr X," then I would not suspect Stuxnet was created to destroy my files and sabotage my film. Unfortunately, for the conspirators, of the 2 or 3 documents that the conspirators used to falsely backdate the Stuxnet virus, none can be verified.

THE IRAN NUCLEAR FACILITY STORY & ATTACK

One of the most unusual things about the Stuxnet virus is that shortly after Stuxnet was discovered, rumours and reports began to leak that Stuxnet was created to attack the Natanz nuclear plant in Iran. These reports were leaked MONTHS BEFORE Stuxnet actually attacked the Natanz nuclear power plant in Iran. Please read the previous underlined section again.

Why would the US create a virus to attack a nuclear facility in Iran, but release news reports about the planned attack, in American publications, BEFORE THE VIRUS ACTUALLY ATTACKED ITS TARGET? Is America so feckless that it would created the most advanced virus ever conceived, then bone-headedly tell the world what it had done months before the virus attacked the intended target? Of course not. The US did this to hide why the government originally created the Stuxnet virus. Stuxnet's payload—two files— were created to destroy my files. The government did this NOT because I am important or interesting, they did this simply because they were preparing to invest hundred of billions into an unprecedented aggregated data collection-base defense and policing system (which I conceived), and they wanted to eliminate all cyber evidence that these ideas ALL came from me. Even if the virus cost a few million to create, the aggregated data defense systems that it would help secure would generate hundreds of billions, eventually trillions, of dollars.

As far as the Natanz nuclear facility... Somehow the US got an infected USB driver into Natanz, briefly took control of the facility, and interrupted enrichment for a few weeks. This provided a reasonable explanation as to why the US had created an amazing new virus (which only did a few million dollars in damage to Natanz).

INFORMATION & DISINFORMATION

As you may have observed in the previous portions of this article, the conspirators have no respect for facts, and they seem to believe it is reasonable to produce false documents, and fraudulently backdate documents. Keeping with this, I found an unusual Russian report called "Stuxnet Under The Microscope," at

https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf. This report attempted to date the origin of Stuxnet mrxnet and mrxls drivers. However, when I entered the documents into the Internet Archive's Wayback Machine, the Internet Archive redirected to a demonstrably fake crawl. Thus, when you enter the URL of the Russian report into the Wayback app, the Wayback adds four digits to the URL ("2020"), then redirects to a fake crawl page. Thus, the waback should direct to:

https://web.archive.org/web/*/https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf, however the wayback improperly adds "2020" and directs to:

https://web.archive.org/web/2020*/https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf. Click the first URL (without the "2020" in the URL) to see the URL add "2020" and redirect to a fake crawl.

ALARM

It is alarming that, in MovieLabs 16 year history, it just so happens that the same year that Stuxnet attacked my computer, 2009, MovieLabs applied for its only valid patent—a hacking system that allows MovieLabs to monitor and spy on a targeted "peer". See this patent [HERE](#). The patent describes functionality that is precisely what Stuxnet's operators would need to monitor a hacked computer system. This patent was granted 2.5 years later, September 6, 2011. (NOTE: In MovieLabs 16 year history, it only has applied for 3 patents, two of which appear fraudulent, as explained earlier in this article).

This suggests that the US government created a monster hacking system (now called Stuxnet) which features fantastic spyware and destructive tools, then gave MovieLabs the patent for this system. This is, at a minimum, implicit permission for MovieLabs to continue to unlawfully monitor me, with the MR X (Stuxnet) hacking/virus system, for the remainder of my life. This is also, at a minimum, implicit permission for MovieLabs (which is owned by the Big 6 film companies and the Motion Picture Association) to unlawfully distribute my ideas to amongst Big 6 film studios, their news companies, and their big-tech conspirator associates, to claim as their own.

But this is more than just a theory. As F-Secure.com explained earlier, Stuxnet hides the MRx virus drivers in the C:\Windows\System32\Drivers folder. Thus, as I completed this "Stuxnet" section, I found 5 mrx drivers in my

C:\Windows\System32\Drivers folder. (See screenshot [HERE](#)). The suffixes of these MRx drivers have changed, indicating that the

C:\WINDOWS\SYSTEM32\DRIVERS\FOLDER. (see screenshot [HERE](#)). THE DATES OF THESE MRX DRIVERS HAVE CHANGED, INDICATING THAT THE MovieLabs and the US government have updated and improved this virus. I purchased my current computer in March or April 2019. But, as you can see from the screenshot, all of the mrx drivers were installed in my computer AFTER the purchase date, and as recently as April 15, 2021, while I was writing this Stuxnet section.

All of this unlawful conduct, which appears executed with the awareness and approval of former Presidents George W Bush and Donald Trump, is a betrayal of American values, is utterly evil, and is a disgrace.

The 2007 Pre-Stuxnet “.Trashes” Virus Attack

In 2007 I experienced two severe hack/viruses. On page 56 of the BvC Complaint, I discussed one of these 2007 hacking/viruses, which erased all of my Hotmail email from May 2005 to September 2007 (this was an effort to erase all records of the December 2006 Butterfly Driver script). In the BvC Complaint, I speculated that this email virus was unleashed by an infected email, sent by a company named SE Film Club, or SE Film Association, which erased all history of itself as I wrote the BvC Complaint (see BvC Complaint, p 56, and exhibits F5, G5, H5). However, the SE Film Club email may have released countless viruses types. And Microsoft, a central conspirator, likely erased the emails themselves, without need of some email-erasing subcontractor.

But the 2007 “.Trashes” computer virus (which, as I recall, manifest in January 2007, but may have manifest as late as Summer 2007), erased 7-12 of my 3.5-inch floppy drives and destroyed one hard drive. The 2007 virus that was injected into my computer (likely via Steve Weinstein and MovieLabs) was the first “.Trashes” virus.

“.Trashes” can also be a type of Mac/Apple file extension, which can sometimes be loaded onto Windows USB and floppy drives, if they are inserted into a Mac/Apple computer. The “.Trashes” virus that I was infected with was designed to appear as if a Mac/Apple “.Trashes” folder had been loaded on a Window 3.5-inch floppy or USB drive. Like Stuxnet, “.Trashes” attacks hard-drives, USB drives, and 3.5-inch floppy drives, and replicates itself onto those drives.

The “.Trashes” virus was unknown until 2008 or 2009. But one or two years before then, the conspirators first released the “.Trashes” virus onto my computer, around January 2007. This is proven by doing a basic Google Chrome search for “.Trashes virus” (in quotes); see [HERE](#), a PDF of this modified Google Chrome search. Examining the PDF, you will see various blogs about the virus going back to 2008.

If you modify this Google search, using Google Chrome’s special search “Tools,” then using the drop-down menu to select the “Custom range” time parameters of January 2006 to December 2007; see [HERE](#), a screenshot of this modified Google search. As you see in the previous screenshot, this virus was not discussed anywhere before 2008 or 2009.

However, if you expand this custom range search parameters to January 2006 to December 2009; see [HERE](#), a PDF of this custom range Chrome search. The single search result, displayed in the previous PDF, shows that, suddenly, in 2009, the world first began discussing a “.Trashes” virus that attaches to USB (and floppy) drives.

However, one or two years before the world knew about the “.Trashes” virus, I had the “.Trashes” virus destroy one hard-drive and many 3.5-inch floppy drives—and I still possess several of these infected floppies. The contents of one of these floppies, showing the “.Trashes” virus folder, can be seen [HERE](#). Regrettably, to produce the previous screenshot of the “.Trashes” virus folder on one of my old floppies, I had to connect an infected floppy, via an external 3.5-inch floppy drive, to my computer. In doing so, I re-infected my current, modern computer with the 2007 “.Trashes” virus. Although this infection did not destroy my hard-drive, the old “.Trashes” virus now replicates itself and attaches to USB drives inserted into my computer. You can see a screenshot of this new “.Trashes” virus now on one of my USB drives [HERE](#). (As you can see in screenshot, the “.Trashes” virus created three folders on this USB drive, which all have the strange future date-of-creation year of 2106.)

Further proof that this “.Trashes” virus was infecting my computer in early 2007, can be seen [HERE](#), a screenshot of the virus on a floppy from 2007. This screen shot is the only floppy drive that the “.Trashes” virus folder manifest but did not erase all other files. I suspect that the hackers who installed the “.Trashes” virus on my computer wanted this disk to survive. I suspect this because the “.Trashes” virus is designed to steal and/or destroy all files, then leave the “.Trashes” folder, to make the hacking appear as if the owner of the hacked computer/drive caused the erasure or disappearance of his/her work by mistakenly connecting his/her Windows drive to a Mac/Apple computer. I suspect the hackers wanted this one disk to survive, as it is, because on this disk the “.Trashes” virus appears with a “.DS_Store” file, which is another Mac/Apple format file. From what I’ve read, a “.Trashes” folder with a “.DS_Store” file sometimes appears on Windows USB and floppy drives when they are inserted into Mac/Apple computer ports. This did not happen with my floppies. I exclusively used Windows computers, from 2002 to the present. Period.

I originally published this Stuxnet (and .flashes) section on April 17, 2021, and this section, and the entire article ended with the previous sentence, reading: "Period." Now, as I write this added passage, it is 12:11 a.m. I am updating this article because I've just learned that the same day that I completed this final Stuxnet section (which conclusively proved that former President George W Bush was directly involved in the theft of my property), former President Bush just happened to release a heart-warming story, in USA Today, about his little-known friendship with Michelle Obama. See [HERE](#). The story actually ends with Bush discussing an art book he has authored, featuring 43 painting of immigrants, which will be released soon. Hmm.... A lot of Americans don't remember Bush doing much for Blacks or immigrants when he was in office. Many Americans remember George W. Bush doing little or nothing for New Orleans Blacks as they baked in the Louisiana sun, in the aftermath of Katrina; American Blacks remember being singled-out for heightened security checks when we travelled, for years, in the aftermath of 911; many Americans remember Bush's military strapping electrodes to the testicles of war prisoners in Abu Ghraib; many Americans remember Bush locking up ONLY brown-skinned detainees in Guantanamo Bay; many Americans remember Bush authorizing water-board torture of ONLY brown-skinned war prisoners, throughout the Middle East. But, because Americans are ever hopeful, and our hearts are full of love, we hope that George W. Bush has finally come to value the lives of immigrants, and non-Whites too. But if he has truly changed and evolved, he should also admit to his approval of the unlawful and ongoing theft of my intellectual property. Otherwise, he should be remembered for deeds, and for his involvement in trying to create a White nationalist surveillance state --a plan that was entirely comprised of ideas that were stolen from a Black American patriot.

-----END

POSTSCRIPT

POST-SCRIPT

Russia's Role In The Plan

I have no idea what Russia's exact role was. But because corporations (and people who don't care about US national security and don't believe in accountability) have convinced Congress not to do oversight on US corporations, Russia may have paid for backdoor access to the conspirators' aggregated data plan before the US government signed on. Or Russia may have asked to help produce some system software. In either scenario, Russia could have coded a portal into the system.

This would also explain Trump's submissiveness to Putin, and explain why in 2017 Trump proposed that the US and Russia form a cyber security unit; see [HERE](#).) And this would also explain why Putin proposed a joint Russian and U.S. cyber security group in 2018; see [HERE](#).

The most troubling thing about the conspirators' data aggregation plan, with respect to Russia, is the conspirators had NO CLUE that, militarily, with a predictive aggregated data defense system, a nation does not want other nations to be able to access its domestic data, because an infiltrating nation can use it to predict our military responses. Militarily, we want our aggregated data collectors pointed at our adversaries, not at home. The US conspirators were clueless about this. Meanwhile, Russia absolutely knew the strategic value of having access to America's domestic data.

Russia & Hollywood's Manipulation of White Americans' fears of Blacks, to Destabilize America

It appears that Russia and a powerful subset of Hollywood, for different reasons, were able to expand their power and influence in the USA, to the point that they believed that they could create a secret new world order, by currying the trust of powerful American conservatives, by unjustly, improperly and evilly portraying Blacks and immigrants as a threat to American stability.

Thus, Russia used the Hollywood subsets' method for currying conservative support (by scapegoating dark-skinned minorities), to ingratiate itself into the good graces of the same conservatives that should have been watching Russia (and the rest of the world). And before anyone knew anything, Russia had played these conservatives' fears against the conservatives, and had infiltrated into the software of U.S. security systems (SolarWinds), and had infiltrated into the fabric of America (through hate-groups on Facebook, that were secretly run by Russians), until they unleashed an insurrectionist siege on the US Capitol, on January 6, 2021.

Russia was light years ahead of the American conspirators. The American conspirators (Microsoft, Amazon, Google, Facebook, Twitter, the Big 6, and their conservative backers) did nothing good for America, and allowed their embarrassing fears to be manipulated --to lay the groundwork for a possible American civil collapse.

Aggregated Data: What Can Be Done?

Today, Microsoft and Amazon both provide aggregated data-based cyber defense services to the US Department of Defense. In 2020, Microsoft and Amazon entered a bidding war for the U.S. JEDI (Joint Enterprise Defense Infrastructure) military contract. Microsoft won. Aggregated data-based policing and defense systems are real.

You can fight back against mass data collection, by not using Amazon Ring Doorbell, and not using devices (like Alexa and Siri) that listen to your domestic activity, not using web services that share your data or collect unnecessary data, tuning off your computer when not in use, covering the cameras on your phones and computers when you are not using the camera function. But you can fight back most effectively by:

1. voting for officials who will work to end aggregated data-based police and military systems ;
2. supporting officials who are committed to enacting and enforcing serious criminal penalties for corporate executives responsible for data abuses;
3. supporting officials who are committed to breaking up the technology giants (Google, Microsoft, Amazon, Facebook) and breaking up the media giants (Comcast and NBCUniversal, ViacomCBS, WarnerMedia);
4. supporting candidates who refuse to take money from big-tech and big-media,
5. supporting officials who are committed to holding all corporations that collect your data without your permission accountable [if you are a Democrat, like me, this means NOT supporting Nancy Pelosi or Kamala Harris, who have taken money from the Big 6 and California's big-tech for decades].

Why Does All Of This Matter?

The conspirators' actions matters because America became a world leader, and the US Dollar became the international standard, because the world believed that the US strongly believes in truth and justice. Accountability matters. If the conspirators do not pay for their actions, America's international standing will suffer. It also matters because the conspirators appear intent to create an isolationist nation, that hides, fearful of the multi-racial world outside. That fearful vision is a doomed and un-American. The needs of societies change, like resources. If America is to survive, it must engage in the world, to acquire the resources we need. We cannot survive by cowering behind our borders, collecting data on our fellow Americans.

If you are an patriot, this matters because you believe in justice, fair play and the American dream—that a person is entitled to the benefit and reward of their ideas and hard work. By stealing my screenplays, shorts, books, and ideas, the conspirators violated every central American tenet. As a patriot, this also matters because the Fourth Amendment protects against such invasions and theft of our "persons, houses, papers and effects" (such as our screenplay, our ideas, and our personal data).

If you are an enlightened progressive who believes in justice and the equality of all people, this matters because the conspirators have acted in a manner that suggests that they are above the law and accountability. It also matters because the conspirators are designing a nation that is not fair or just.

If you are a racist and/or a White supremacist, this matters because you believe that your race is superior, so these corrupt big-tech corporations that are planning your future society should not need to steal the intellectual property (e.g., aggregated data, universe replication and acceleration, brain imaging, etc.) of a Black liberal.

A HUGE Shell Loophole Not Addressed In The Corporate Transparency Act

Corrupt shell owners steal intellectual property by buying and creating countless empty shell companies (opening a shell only cost about \$75). Then, these corrupt shell owners just let these shells (which exist only as company names in a state database) sit, and wait. Then, years later, if the corrupt owner discovers a new concept or technology that he/she wishes to steal, the corrupt shell owner can dust off one of their fake unused company names, created years earlier, and announce that that old shell company name, has quietly been working on the technology that the shell owner wants to steal. Thus, by making a formal new technology announcement, then associating the new technology with the pre-existing shell company name, corrupt businessmen unlawfully steal technology by backdating concepts to pre-existing shells. Then, the poor actual inventor of the new technology must prove that the corrupt owner is lying. Hint: the inventor will not be able to prove this.

This is a flaw so flagrant that it is as if American courts and lawmakers wanted corporations to continue steal intellectual property.

Corrupt lawmakers and judges have created an intellectual property (I.P.) theft machine that is poised to severely harm America. We can't shake our fingers at Russia and China for I.P. theft, when OUR system promotes I.P. theft from foreigners and our fellow Americans alike.

To end this abuse, businesses should be required to write brief annual statements, declaring and describing what product or service the company is endeavoring to provide (a generic description, like "film company," should not be sufficient). This way, if a company that was making ping pong paddles in 2021, suddenly invents anti gravitational boots, in 2022, the court might guess foul play is afoot.

Snowden & Assange

If you read *Morons Don't Ride Harleys* (pp 70 & 83), you'll find a couple passages where I was very critical of Edward Snowden and Julian Assange. (See [HERE](#).) At that time, I certainly didn't understand the extent of the data collection that the US was engaged in, and I certainly didn't understand

that there were powerful forces within the US government who were dumb enough to believe there was some value to America becoming a racist state, and who believed they had the right to create a new White nationalist surveillance state, without consulting the rest of the country.

Now that I have a better understanding of what Snowden and Assange were seeing, I believe they were acting on their consciences, and they truly believed they were doing the right thing. I now think that there were extenuating circumstances. I think Assange and Snowden deserve reasonable punishment, but not life sentences, and not death sentences. And, at the same time, it should be recognized, that Snowden and Assange were right, and forces within the US government were taking unprecedented and unlawful action, without proper authorization and disclosure, and in violation of the Fourth Amendment.

- **FOURTH AMENDMENT:** The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Russia Likes My Book

In 2017, just days after I released *Morons Don't Ride Harleys*, the book wound up on a Russian website that gives away free, unauthorized PDF copies of Western (primarily American) books. The other books that I saw on this site were well-known works, by major publishers. I spent quite some time trying to get the book taken down from the site, unsuccessfully. I believe Google (Sergey Brin, Larry Page), Bill Gates, Jeff Bezos and the other conspirators wanted my book available for themselves and their associates to muse about. But they made it available for free, on the Russian bootleg book site, to make sure that I earned no money from my book (why buy what you can download for free?). I have attached an email I sent to this Russian book company (in April 2017), below. The peculiar email address, "concatdevelop@gmail.com" (a Google email address), was the only contact email provided on the site.

DISCLAIMER:

Everything written, said or presented on this website or in the article "Hollywood, Big Tech, and the Aggregated Data Caper" is/are just allegations, not necessarily facts. Although I, the owner of this site, whole-heartedly believe these allegations to be true, and although the attached PDF court filings present seemingly overwhelming evidence, everything presented or connected, no matter how persuasive, is/are just allegations.

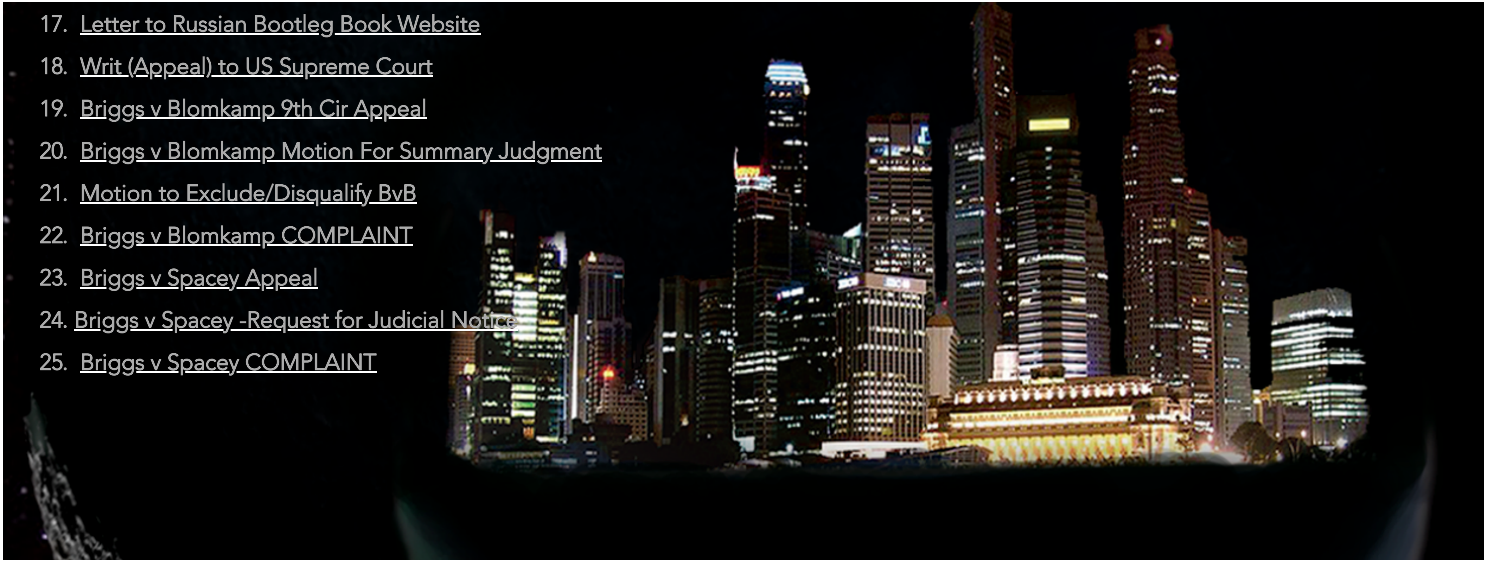
PDF PAGE

PDFs

1. Hollywood, Big Tech, And The Aggregated Data Caper
2. OPENING BRIEF
3. Briggs v Cameron COMPLAINT with exhibits
4. Briggs v Cameron COMPLAINT WITHOUT exhibits
5. Fifth Motion In Limine
6. Amended Second Declaration
7. Amended Motion In Limine
8. Amended Second Motion In Limine
9. Third Motion In Limine
10. Second Request For Judicial Notice
11. Third Request For Judicial Notice
12. Excerpts of The Record
13. Substitute/Corrected Opening Brief

- 14. Judge Orrick's Recusal Letter
- 15. Letter to the Ninth Circuit
- 16. Moron's Don't Ride Harleys (Feb 2017 book)

- 17. [Letter to Russian Bootleg Book Website](#)
- 18. [Writ \(Appeal\) to US Supreme Court](#)
- 19. [Briggs v Blomkamp 9th Cir Appeal](#)
- 20. [Briggs v Blomkamp Motion For Summary Judgment](#)
- 21. [Motion to Exclude/Disqualify BvB](#)
- 22. [Briggs v Blomkamp COMPLAINT](#)
- 23. [Briggs v Spacey Appeal](#)
- 24. [Briggs v Spacey -Request for Judicial Notice](#)
- 25. [Briggs v Spacey COMPLAINT](#)



GOOGLE &

ALPHABET'S INTERNET FRAUD, RELATED TO THIS WEBSITE

NOTE: I created this website between February 17, 2021 and March 15, 2021. On March 14, 2021, I discovered that Google LLC (a conspirator named in the main article "Hollywood, Big Tech, and the Aggregated Data Caper," and a defendant in *Briggs v Cameron*) had cached the "Screenplay" page on this website to say that the site was created in 2019, and Google did not cache the main article (the Home page) at all (the Home page should be the first page indexed by Google). Google did this (1) to cause people to believe that this site and the information on this site, were several years old, and (2) to prevent people from finding the main article. (You can see a screenshot of how Google improperly cached the page [HERE](#). You can read my direct message to Google, asking them to correct the problem [HERE](#), and [HERE](#) (sent March 14, 2021).

Because of Google's efforts to keep people from finding this homepage, I had to relocate the "Screenplay" and "Litigation" pages to the lower portion of this Home page.

March 17, 2021, three days after relocating the "Screenplay" and "Litigation" webpages to the lower portion of this homepage, Google, once again, cached my website so that it was difficult to find, and so that it falsely indicated that it was made in 2019. That is false. Again, this website was created, in entirety, in 2021. I will update new facts and evidence, related to Google's recent web fraud, soon.

THE SCREENPLAY (BUTTERFLY DRIVER)

MORONS DON'T RIDE HARLEYS

(click to download)

Morons
Don't Ride

CONTACT

snc.steve@gmail.com

Name

Email

Phone

Address

Subject

Type your message here...

Submit

All Posts



Posts Are Coming Soon

Stay tuned...

©2021 by Hollywood, Big Tech and the Aggregated Data Caper. Proudly created with Wix.com