GolfTraxx.com 

October 27, 2021 Press Release- For IMMEDIATE Publication: Google CEO blames US government for attacks against US businesses and requests government funding to research "attacks" launched from it's own servers

https://www.wsj.com/articles/google-ceo-sundar-pichai-calls-for-government-action-on-cybersecurity-innovation-11634580600

In recent days, Sundar Pichai, chief executive of Google and parent company Alphabet Inc., said the U.S. government should take a more active role in policing cyberattacks and "encouraging innovation" with policies and investment.

Wait… so let me get this straight. After Google's own servers were again used to launch massive attacks against websites such as golftraxx.com in recent weeks, Pichai wants to receive grants from the US government to conduct "research" on how this happened???

Does anyone else smell **stinky rotten fish**?

During September, 2021 golftraxx.com reported to regulators on multiple occasions that our website was being attacked and taken down by massive Distributed Denial of Service attacks which are being launched over short spans of time. In excess of 200 million pages were requested by Google's own servers.

Google doesn't need to receive federal funding to see the IP addresses of the massive attacks against golftraxx.com in September, 2021. Google needs to tell the **truth**…Unfortunately truth seems to be something neither Pinchai nor his army of corporate in-house attorneys has much aptitude in. Moz.com corroborated the attacks. Does Pinchai want to suggest that moz.com is lying too???

Pinchai is a liar. Plain and simple. It is no longer subject to debate. The facts are the facts. Others have said that Pinchai and other executives lying about Google involvement are members of an elite upper crust caste system in India and must be respected just because they are members of that upper crust society. I beg to differ. It doesn't matter if someone is royalty or upper crust caste elite.

What matters is their choices. What matters is their integrity. What matters is their honesty when they've been caught cheating and stealing and f-ing over other smaller businesses repeatedly. Google needs to admit their illegal and unethical actions and make amends to each and every business they have harmed.

Google's actions are bullying to the nth degree.

Pinchai and his other upper-crust team members are demonstrating a **clear lack of integrity** in choices

to not respond about how Google servers were used for the massive attacks. To make matters worse, Pinchai is **covering up** for his business partners, particularly, in this case, COMCAST.

When we reported the attacks against my home network during the past year (which is hosted by COMCAST because there is not another choice where I live) , we attached the packet scan results. A bot was shown to be continuously executing a man-in-the-middle attack against my home network. In a man-in-the-middle attack, the bot **forces** the packets to be sent using an **unregistered** IP address (in all these attacks the packets were sent to COMCAST and Google). Bots employed by ISP's in denial of service attacks and in direct website attacks can also use the IP's of other corporations to (known as IP spoofing) because they're the ISP itself is the one that's supposed to be regulating such abuses.

ISP's can therefore **circumvent** the rules about IP addresses in their own illegal actions to **cover-up** what they did. COMCAST IP addresses are indeed implicated as having done exactly this in the attacks against my home network and through which they attacked the golftraxx.com website. Their IP's are in fact are included in the packet scan which COMCAST executives have stated is not possible.

The COMCAST bot on my home network sent hundreds of thousands of packets to COMCAST and to Google servers each and every packet was sent **without a valid IP.**

What makes us believe COMCAST did not do the exact same thing in launching "unregistered or spoofed IP address attacks against the golftraxx.com website?? We should not be so trusting of corporations who demonstrated themselves to not be trustable.

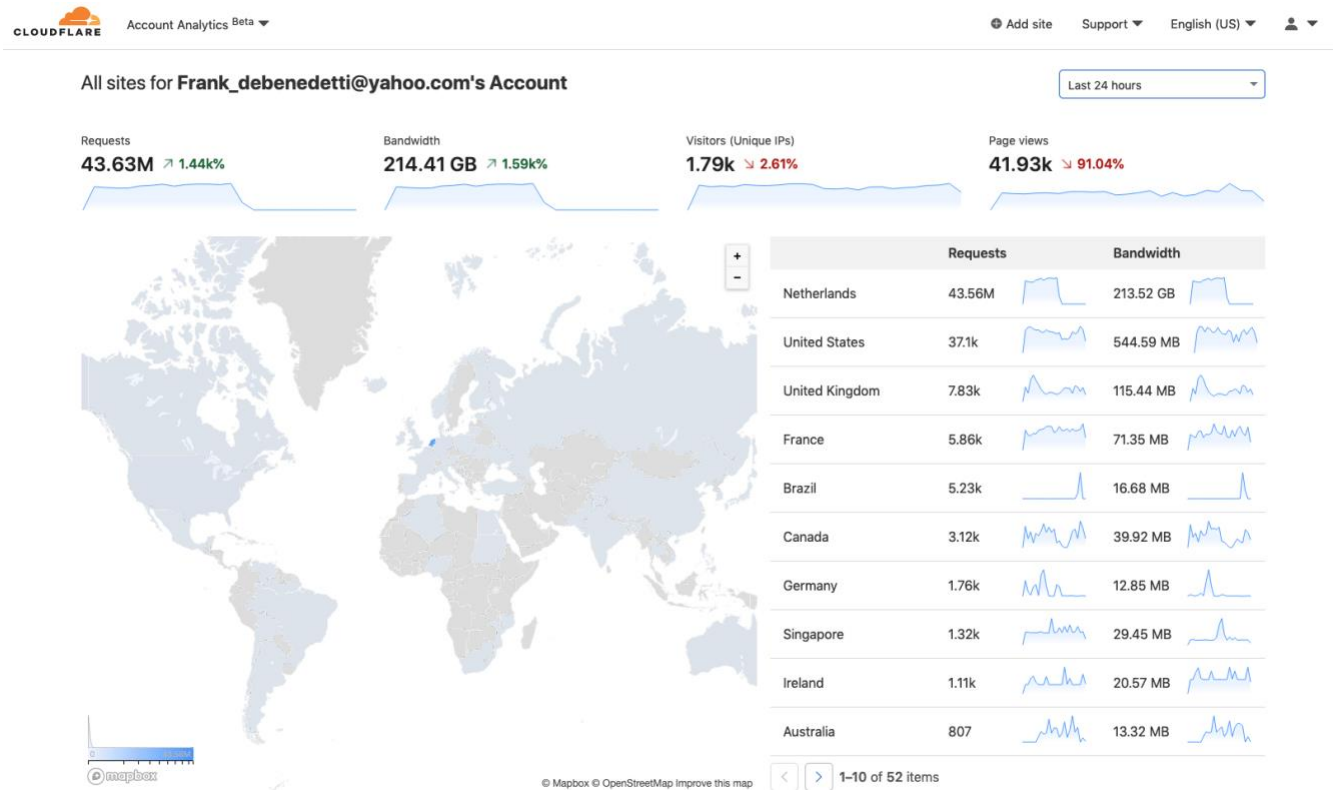
A highly problematic issue in the prosecution of treachery such as this is the fact that ISP's such as COMCAST and tech giants such as Google are regulated by different regulatory agencies, FCC regulates COMCAST and other ISP's while FTC (and others) regulate tech giants such as Google. Of course, there are state regulators as well, but no single state has the ability to stand up to Google which is exactly why 49 state attorney generals have joined the justice department lawsuits against Google.

It seems that ne'er the two regulatory agencies shall meet when corporations subject to different regulatory jurisdictions join forces to collaborate and operate an organized crime ring.

It should not go unnoticed that an invisible wall through which an unofficial but highly effective type of corporate immunity from prosecution for their crimes is created. These corporations are "protected" when regulators do not cross jurisdictional lines where corporations are found to have been collaborating and/or operating in an organized crime syndicate.

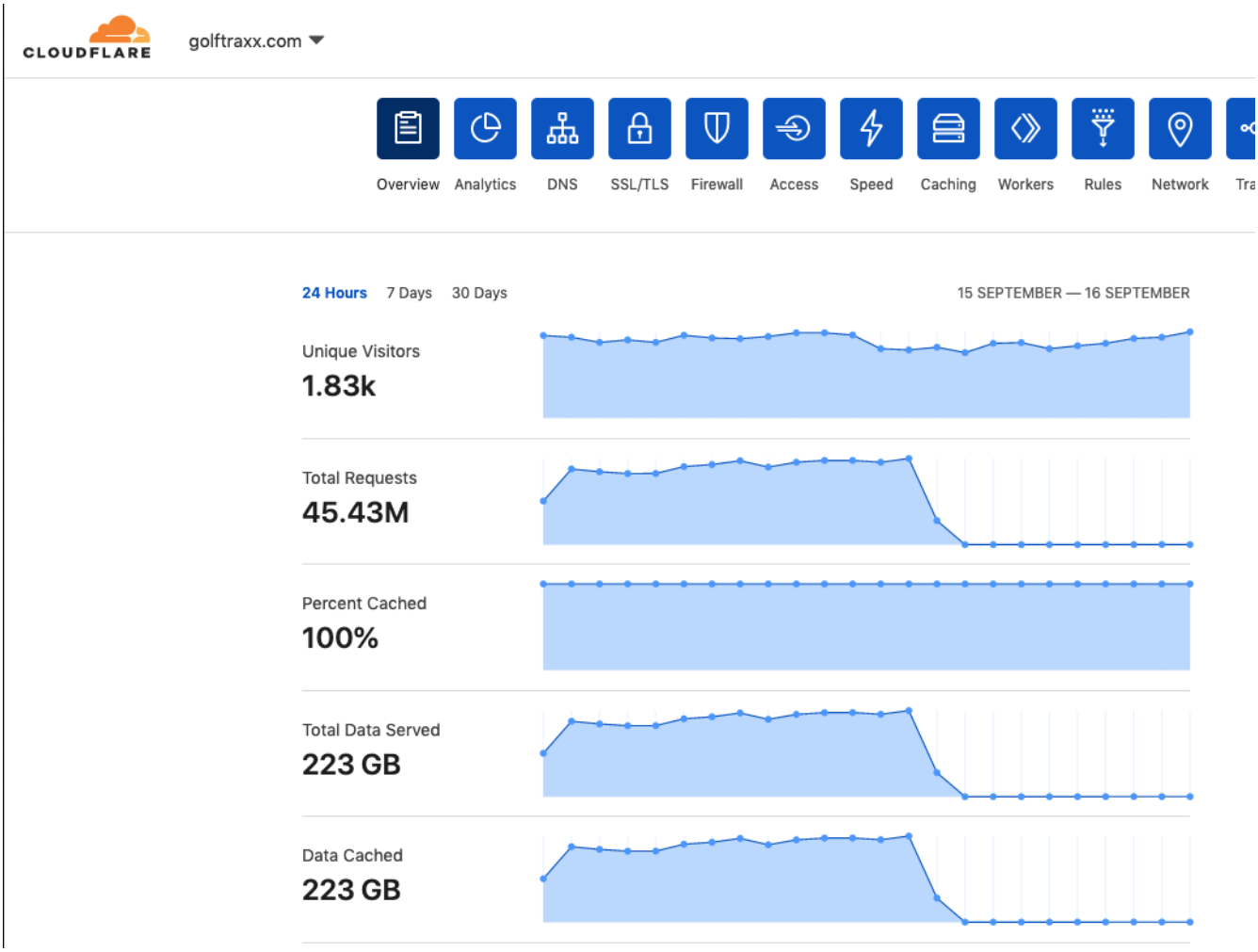
While neither Google nor COMCAST has agreed to release the records, we wonder why law enforcement is not **demanding** these records, **forcibly** if necessary.

We need to consider how few organizations in the entire world are capable of executing these massive attacks, and observe that it is FAR more likely than not that of those capable, the one that took the action was doing so to cause damage to its competition in the golf space.



One particular Distributed Denial of Service attack against golftraxx.com ran during a 24 hours for approximately 14 hours, versus the typical 3 hour attacks we have experienced over the past several weeks.

That massive attack from servers in the Netherlands coincided with the European Tour event in the Netherlands which kicked off today with its pro-am event. This latest attack was again documented by Cloudflare in the same fashion as prior attacks.



The above screenshots from Cloudflare demonstrates that the site did in fact receive close to 45 million requests in the span of several hours AND that the 45 million requests came from the Netherlands.

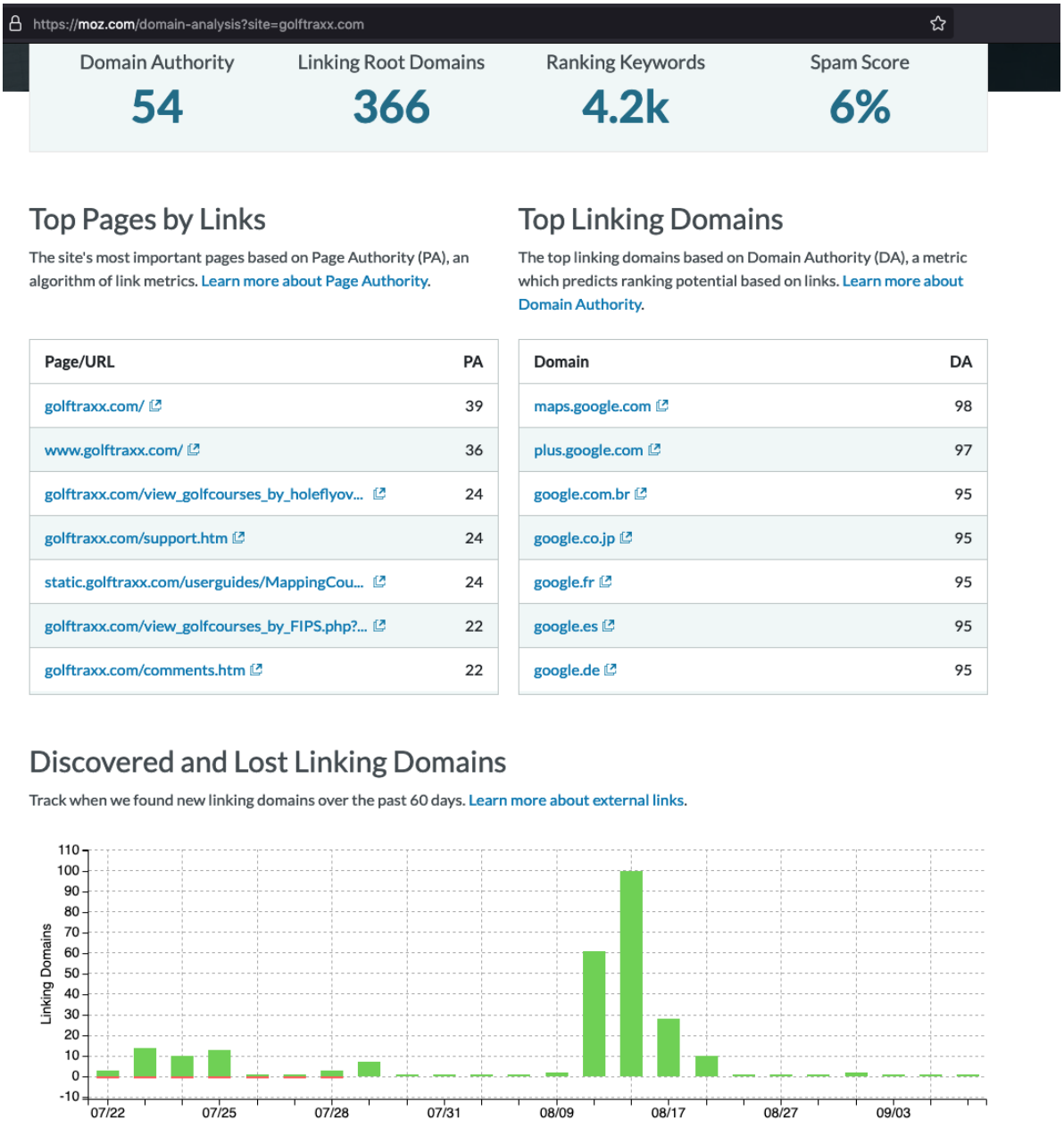
GolfTraxx site visitors were disabled from reaching the goltraxx.com website and blocked from receiving responses from the golftraxx.com server during these attacks.

The hours during which we received the Denial-of-Service attacks during the past day coincided with the hours of the leading up to and spanning the Pro-Am event in the Netherlands at Bernardus Golf Club where amateur golfers joined the European Tour pros on this week's European Tour event for a day of team competition.

We have consistently reported to regulators that previous attacks against our website have implicated Google, COMCAST, and other corporations. We KNEW for example that the first massive attack of 42 million page requests did in fact come from Google right here in the USA as we had only days earlier submitted our two million pages of content with Google-specified JSON attributes attached to each individual page that correctly identify the course name, course zip code, course phone, course address, city, and state.

Win recent weeks, we have been requesting from Cloudflare the IP's submitting the massive page requests, and while we received the corporation names in prior attacks previously from Cloudflare, we have not yet received a response from Cloudflare to our latest inquiries as to the corporate sources of these latest attacks.

A highly respected website authority ranking site called moz.com made things 100% clear in a single screenshot that we'd like to share with you now.



What we'd like you to notice in the graph of Discovered and Lost Linking Domains is the large increases shown Top Linking Domains during August and their correlation between Google domains in other countries who recently linked to golftraxx.com, while bearing in mind the list of countries from which we experienced massive distributed denial of service attacks during the past month: Brazil, France, Spain, and Germany, as well as USA. Not all of the attacks correlate, so you can conclude that yes, we were also attacked by Russia last month and that may not have been a Google-sponsored attack.

But you can also conclude that all those Google off-shore servers that connected to golftraxx.com in the past month from google are in the exact **same** countries that the massive distributed denial of

service attacks occurred against the golftraxx.com website.

What's even more **despicable** about the most recent attack (believed to be orchestrated by Google using its servers in the Netherlands) is of course the **timing** of their execution of the attack. Would any reasonable person believe that Google's execution of massive distributed denial of service attacks upon the golftraxx.com website repeatedly in the hours leading up to the major professional golf event in the Netherlands was anything but **intentional**? We don't believe it was some unfortunately-timed coincidence either. We don't recommend that you believe that it was anything but intentional.

We believe that Google takes aggressive and illegal action against any site that stands in its way of world search dominance. As a reminder, Distributed Denial of Service attacks are **illegal**.

https://www.justice.gov/usao-ndtx/pr/man-receives-maximum-sentence-ddos-attack-legal-news-aggregator

Often, it is difficult to identify the perpetrator in Denial of Service attacks. Remarkably, Google seems to be going out of its way to make it **obvious** that its own servers did commit the illegal acts. Some might conclude that Google is trying to get caught so that its legal team may be able to manipulate the legal process as well and exclude the golftraxx.com website from inclusion in any Google Search results.

Any legal remedy for businesses affected by corporate treachery such as this requires a carefully applied balance of criminal and financial penalties against the aggressors and civil protections for the victims, such that Google, COMCAST, and others involved in the illegal and/or criminal acts are penalized and prosecuted for their illegal acts AND the affected parties receive restitution for their losses, but also, at the same time, the offending corporations MUST thereafter be forbidden from taking other adverse actions against the injured party such as exclusion from indexing, or blocking the injured party from receiving services vital to the survival of their website or business. To complete the feedback loop, any injured victims must be enabled to immediately report any further abuses for IMMEDIATE prosecution (as well as restoration of any essential services that have been blocked by the aggressor).

Websites need to be included in Google Search results to get found. So it places websites who have been repeatedly attacked by huge tech corporations such as Google LLC and COMCAST on vastly unequal footing…perhaps more aptly characterized as perched precariously on cliff's edge.

Title 18 Section 241 makes it illegal for two or more persons (or corporations) to conspire to injure, oppress, threaten, or intimidate any person of any state, territory, or district in the free exercise or enjoyment of any right or privilege secured to him/her by the Constitution or the laws of the United States (or because oh his/her having exercised the same).

Where massive tech corporations use their free and unmonitored access into our homes for illegal purposes, **Title 18 Section 241** also makes it unlawful for two or more persons to go on the premises of another with the intent to prevent of hinder his/her free exercise or enjoyment of any rights so secured.

Americans who have discovered these "uninvited" massive tech corporations in their homes taking illegal actions against them **deserve** the same types of protections afforded by the **Title 18 Section 241** code provisions. But **Title 18, Section 241** does not go far enough.

California has enacted **SB-22 Communications: broadband internet access** service in which it

declares it illegal for any fixed Internet Service Provider to: Sec. 3101 *(7) (A) Unreasonably interfering with, or unreasonably disadvantaging, either an end user's ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of the end user's choice, or an edge provider's ability to make lawful content, applications, services, or devices available to end users.*

California has also enacted the **California Privacy Act** which provides in part that: 2 (C) (ii) that the service provider [COMCAST] does not further collect, sell, or **use** the personal information of the consumer *except as necessary to perform the business purpose*.

There is no legitimate business purpose that can EVER cause damage to the website of a COMCAST customer.

There is no legitimate business purpose that can utilize a bot installed onto the home network of a COMCAST customer for the purpose of declaring itself as the gateway of the home network then executing a man-in-the-middle attack against the home network in which packet buffer overflow causes every packet from the home network to be forwarded to COMCAST and Google servers.

There is no legitimate business purpose when COMCAST servers execute DNS Leaks across multiple COMCAST servers that stand between atheCOMCAST customer's home network and the internet

There is no legitimate business purpose in COMCAST's refusal to provide the records requested under the **California Privacy Act** regarding all information collected by COMCAST about their customer and how it was used.

There is no legitimate business purpose in COMCAST's use of the collected information (obtained through the backet buffer overflow attacks) to repeatedly cause damage to a COMCAST customer's website.

We're reasonably certain that no grant of authority **EVER** existed whereby the ISP, COMCAST, was granted the right to orchestrate multiple DNS Leaks through its own clusters of COMCAST servers between a customer's home network connection and the internet, and simultaneously allowed to execute **man-in-the-middle attacks** on that customer's home network by installing a bot such that every packet from the customer's home network was forwarded using a buffer overflow attack on the home network then routed from the customer's home network to Google and COMCAST servers, from which point the multiple COMCAST DNS servers substantially delayed those packets for several minutes then resubmitted to the golftraxx.com webserver as though those were valid requests from my home network (thereby **impersonating our team members, illegally re-using our site credentials, obtaining unauthorized access to our server, illegally making changes to our data, and causing damage to data on the customer's website**) .

The attack strategy enabled COMCAST/Google to overwrite updates we made to golf courses on our server with their DNS Leak-generated, delayed packets, which had the effect of overwriting our valid updates with bad data. It created an appearance that the editors work on our website was being monitored 24/7/365 because golf courses that had just been updated by our editors were getting changed to bad data.

California Penal Code Section 502 declares it illegal to do these things:

(c) Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

The **California penal code section 502 penalties** are substantial and they should be**:**

(d) (1) Any person who violates any of the provisions of paragraph (1), (2), (4), (5), (10), (11), or (12) of subdivision (c) is guilty of a felony, punishable by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years and a fine not exceeding ten thousand dollars ($10,000), or a misdemeanor, punishable by imprisonment in a county jail not exceeding one year, by a fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

(2) Any person who violates paragraph (3) of subdivision (c) is punishable as follows:

(A) For the first violation that does not result in injury, and where the value of the computer services used does not exceed nine hundred fifty dollars ($950), by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000) or in an injury, or if the value of the computer services used exceeds nine hundred fifty dollars ($950), or for any second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(3) Any person who violates paragraph (6), (7), or (13) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, an infraction punishable by a fine not exceeding one thousand dollars ($1,000).

(B) For any violation that results in a victim expenditure in an amount not greater than five thousand dollars ($5,000), or for a second or subsequent violation, by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(C) For any violation that results in a victim expenditure in an amount greater than five thousand dollars ($5,000), by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment pursuant to subdivision (h) of Section 1170 for 16 months, or two or three years, or by both that fine and imprisonment, or by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(4) Any person who violates paragraph (8) or (14) of subdivision (c) is punishable as follows:

(A) For a first violation that does not result in injury, a misdemeanor punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

(B) For any violation that results in injury, or for a second or subsequent violation, by a fine not exceeding ten thousand dollars ($10,000), or by imprisonment in a county jail not exceeding one year, or by imprisonment pursuant to subdivision (h) of Section 1170, or by both that fine and imprisonment.

California SB-22 Communications: broadband internet access also specifically prohibits such conduct by ISPs, but nothing has been done related to COMCAST repeated attacks against me and my website.

The **California Privacy Act** which provides in 2 (C) (ii) that: the service provider [COMCAST] does not further collect, sell, or **use** the personal information of the consumer *except as necessary to perform the business purpose*.

The **California Privacy Act** provides that repeat offenders of provisions within its Act shall be find up to $10,000/occurrence.

The website, GolfTraxx.com features 40,000 courses in its database from 105 countries. Roughly 30,000 of these courses contain course-specific information such as the course scorecard, a course map, hole-by hole maps, video flyovers of the course and its holes, lists of nearby courses, and ability to use the site as a rangefinder and scorekeeping tool on each of its courses. To provide all the information about all these courses, the golftraxx team created close to 2,000,000 pages intended for site visitors! In the days leading up to the Netherlands pro-am this past week, the golftraxx team added the hosting course Bernardus Golf Course to its database. https://bernardusgolf.com/storage/files/course-information/bernardus-course-guide-v2.pdf

Some unique features at Bernardus made the mapping a bit more complex, such as distances measured to the front of each green instead of the center which can be corroborated by our Gradebook for Bernardus containing a **negative** variance for each hole equivalent to half the depth (front to back) of each green. Of course, the course needed to be converted from meters to yards as well for proper hole measurement.

The attacks by Google corporation and COMCAST and other powerful tech corporations against the golftraxx.com website raise serious questions as to the proper levels of regulatory authority, not to mention about the inhumanity of executives within these powerful tech corporations who would place their egos and greed above social conscience to order such attacks against a person known to have been disabled by cancer.

In the view of this author, neither regulators nor law enforcement, nor the agencies set up for the protection of human rights should tolerate these types of corporate abuses, and Google itself (as well as the other corporations implicated in these attacks- Microsoft, COMCAST, and Amazon)) should police their own operations sufficiently to preclude these types of malicious abuses and attacks.

Further, where it is demonstrated unequivocally that corporations did in fact participate in and/or execute the attacks against a man disabled by cancer, they have a civic duty to open their checkbook and make amends.

Neither regulators nor law enforcement should watch idly while these abuses continue to occur to innocent victims. 49 states attorney generals have sued Google. It's not because Google is operating as an ethical corporate citizen. Google is out for blood.

COMCAST received the data showing their IP's participated, in attacks against me personally and my website, yet simply issued blanket corporate denial statements.

The golf community and professional tours worldwide should demand accountability from these corporations who take such malicious and illegal, abusive actions against American citizens.

I ask every executive in America to join me in **demanding accountability** from Google and COMCAST for their treacherous activities.

Contact:

Frank DeBenedetti

877-354-4653

916-806-4036 cell

frank@golftraxx.com

frank_debenedetti@yahoo.com