Subject: Techdirt Daily Newsletter for Tuesday, 4 May, 2021
Date: Tuesday, May 4, 2021 at 4:41:23 AM Mountain Daylight Time
From: Techdirt Daily Newsletter <newsletters@techdirt.com>
To: Techdirt Daily Newsletter Subscriber <tanidowning@utah.gov>

read it online

Techdirt Email.

Stories from Monday, May 3rd, 2021

Are you interested in receiving a shorter, easy-to-scan, email of post excerpts? Check our our new

Techdirt Daily Newsbrief

Riot Shuts Down LoL Fan Server After Getting All Wiseguy With Its Developers

from the *nice-project-you-have-there...* dept

by **Timothy Geigner - May 3rd @ 7:58pm**

Way back in 2016, we discussed how Blizzard was very busy shutting down fan-made and hosted *World of Warcraft* servers, pretending like intellectual property forced it to do so. At the time, these fan servers were hosting *WoW*s vanilla experience, mimicking what the game looked like upon first release, rather than then current iteration of the ever-evolving MMORPG. While Blizzard has since come out with a vanilla experience product of its own, at the time, these fan servers were filling a market desire for a product that didn't exist. Rather than figuring out a way to work with these fans, Blizzard just shut them down.

And now it's all happening again with Riot, makers of *League of Legends*, an online game that similarly is ever-evolving. Fans of the game once more created a fan server that hosted the older, vanilla version of the game for those who wanted to play it that way. What makes this situation different, however, is that Riot only sent its C&D notice to the developers after the developers posted online an exchange they had with a Riot representative which took on a very 1920's wise guy tone.

> *Speaking with PC Gamer, Riot said that it has sent a cease-and-desist request to the developers of Chronoshift after one of them posted an exchange with a Riot employee to Reddit earlier this week. The post showed a back and forth over Discord, during which a member of Riot's security department named Zed wrote to a Chronoshift developer that Riot's legal team "isn't super thrilled about your project unfortunately and is looking for a way to come to a mutually acceptable end to it."*

> *A few lines later, Zed took the conversation in a decidedly bizarre direction, claiming that their team had archives of chat channels the Chronoshift team tried to delete. Zed followed that by saying, "you've obviously put a lot of work into Chrono shift, but I assure you that the chrono break is coming." When the Chronoshift developer asked Zed to dispense with the "scare tactics," Zed demanded that the developers hand over Chronoshift's website and source code to Riot, as well as "all identifiable information" they shared with a specific developer. Zed then made the stakes of the situation clear: "Give me what I'm looking for and we won't sue," they said. "Refuse and we will."*

Riot told PC Gamer that, while it didn't love the tone of its rep's interactions with the Chronoshift development team, still the request for code and information about the project was a "standard" request. That sort of thing happens so that the rightsholder can figure out exactly to what extent the project was infringing. But it's notable in this case again that Riot doesn't currently have a competing project of its own for this sort of vanilla *LoL* experience. Despite that, and despite the fact that the Chronoshift team never took a single dime in any way for this project, through donations or otherwise, Riot still shut the whole thing down and pretended intellectual property forced its hand.

> *In Riot's letter to the developers, which leaked despite the developers' apparent wishes, the company also noted that Zed's grab at the game's source code was "a standard demand made to all developers engaged in unauthorized activity in order to assist Riot's security team to understand the precise nature of the project, the manner by which it infringes Riot's intellectual property, and other rights, and the extent to which the code has been shared or disseminated online." In other words, it does not appear that the company is planning to use the work of fan developers to form the backbone of its own legacy servers, despite fan speculation to the contrary.*
>
> *In the letter, Riot further explained that it is compelled to defend its "valuable" intellectual property from conduct that "enables and encourages acts of copyright infringement," which in turn "harm Riot, its business, and ultimately, its employees." This is similar to what Blizzard said when it infamously shut down popular fan-run WoW server Nostalrius back in 2016. However, Blizzard has seemingly eased off fan-run servers like Elysium in the wake of WoW Classic's release.*

Similar and equally chock full of bullshit. There are plenty of ways Riot could have worked with these dedicated fans on their project to allow it both to come to fruition while also protecting its own rights. But Riot would have to *want to* have that kind of

outlook and interaction.

Instead, it sure seems like Riot instead wants to apologize for its own rep's "Nice project you have there, be a shame if anything happened to it" tact. Certainly the rest of the *League of Legends* fandom should be sitting up and taking notice.

2 Comments »

Fifth Circuit Strips Immunity From Cops Who Ended A Mental Health Crisis By Restraining A Man To Death

from the *unfortunately-it-took-a-death-to-obtain-this-result* dept

by Tim Cushing - May 3rd @ 3:41pm

The Fifth Circuit is the worst place to bring a civil rights lawsuit against law enforcement officers. But that may slowly be changing, thanks in part to the Supreme Court, which has played its own part in making qualified immunity an almost insurmountable obstacle in civil cases. Over the past few months, the Supreme Court has reversed and remanded two cases handled by the Fifth Circuit Court of Appeals, ruling that the lower court's extension of qualified immunity was the incorrect conclusion.

This case [PDF] may reflect the Supreme Court's qualified immunity attitude adjustment. Or it just may be that there's no excusing what happened here: a man suffering a mental health crisis being helped to death by San Antonio (TX) police officers.

Jesse Aguirre was reported to dispatchers by drivers on a heavily traveled eight-lane highway. Drivers noted Aguirre seemed to be "mentally disturbed" and possibly in danger of being injured or killed since he was walking on the thin media strip dividing the eight lanes of traffic. Officers arrived at the scene and things just kept getting worse for Aguirre. Fortunately, it was all documented by the dashcam on an officer's vehicle.

Here's the first "offer" of "help" Aguirre received from a police officer:

> *Officer Gonzales was the first to arrive. She left her vehicle blocking the left-most eastbound lane and approached Aguirre on foot with her firearm pointed at him, ordering him to "come here" and threatening, "I'm going to shoot you, m-----r-f----r."*

Lovely. Gonzales continued to walk after Aguirre, joined by Officer Morgan (also pointing a gun) and Mendez (pointing a Taser). Aguirre then stopped and placed his hands on the concrete median barrier. All three officers rushed Aguirre, grabbing him and placing him in handcuffs. According to the video, Aguirre did not "visibly resist" being handcuffed. The officers then tossed the handcuffed man over the cement

barrier, causing him to land on his head.

More officers arrived. And they apparently felt the unresisting man needed more "assistance" dealing with his apparent mental health crisis.

> *After one or two more officers arrived, they assisted in moving Aguirre from the car hood to the ground onto his stomach next to the median with his hands still cuffed behind him. The video does not show that Aguirre resisted during this maneuver, but instead that he stumbled with the Officers toward the median. After Aguirre was placed prone on his stomach, Officer Gonzales pushed his legs up and crossed them near his buttocks and kneeled forward on Aguirre's legs, holding them near Aguirre's bound hands in a hog-tie-like position. Officer Mendez knelt with one knee on the ground and the other on Aguirre's back, later changing position to hold Aguirre's shoulders and cheek down against the pavement with his hands. Officer Mendez testified that he was using part of his body weight to hold Aguirre down, thus applying pressure to Aguirre's back and neck. Officers Morgan and Arredondo then joined Gonzales and Mendez, placing their hands on Aguirre's arms and back to hold him prone in the maximal-restraint position.*

More officers arrived, including a supposed "medical tech officer" (Benito Juarez) but there's nothing on video suggesting he handed out any medical advice or paid any attention to the handcuffed man's condition. One officer noted Aguirre's lips were turning blue but chalked that up to "drug use," rather than the ongoing asphyxiation that was actually occurring.

Aguirre remained hogtied face-down on the pavement for more than five minutes. At some point during that time he stopped breathing, but it was only noticed by the large group of officers after he had spent five-and-a-half minutes in that position. Once they realized he had stopped breathing, the officers turned Aguirre over and the "medical tech officer" jogged off to get some medical equipment.

But no one really seemed to care.

> *At this point, the Officers appear to be in good spirits; according to the Plaintiffs, in the dashcam videos, Juarez can be seen smiling as he jogs to his vehicle, and several other Officers likewise appear to be smiling and laughing as they await Juarez's return around Aguirre's body. Juarez returned at a walk with his medical bag approximately one minute after he left.*

It wasn't until more than four more minutes had elapsed that any officer attempted to perform CPR. But it was too late. Aguirre was dead. The autopsy report confirmed what the dashcams had caught: the restraint method had asphyxiated Aguirre. The

conclusion: "due to restraint by police, this case is classified as a homicide."

Despite this direct link between their actions and Aguirre's death, the officers wanted qualified immunity. The court refuses to extend it. The amount of force used to restrain Aguirre was excessive. The situation did not call for maximal restraint of a cooperative subject, especially given the criminal act (which is still a stretch) at the center of it.

> *Defendants do not attempt to show that the severity of any crime committed by Aguirre weighed in favor of the level of force used by the Defendant Officers. In fact, defendants do not articulate any criminal investigatory function justifying their actions, and instead rely on the existence of a threat to the public safety—namely, the potential danger to motorists and himself that Aguirre's mental disturbance and walking along the median of the eight-lane highway caused. At most, the crime at issue was a traffic offense.*
>
> *[...]*
>
> *This factor thus weighs against it being reasonable or necessary to place Aguirre in the maximal-restraint position for over five minutes.*

And the cops can't swing the court their way by providing testimony that was often directly contradicted by their own dashcam recording.

> *In their declarations below, the Defendant Officers stated that Aguirre was resisting and they feared that he would break away and run into traffic, causing a dangerous collision and potentially dragging one of the Officers with him. But the Plaintiffs' summary judgment evidence and this court's own review of the video evidence at minimum raise genuine questions about whether it was objectively reasonable to believe Aguirre was actively resisting or even physically capable of posing an immediate safety threat that would justify the Defendant Officers in using extraordinarily dangerous force by placing and holding him in the prone maximal-restraint position that led to his death.*

The court also points out that the fact the officers suspected Aguirre had recently used drugs should have resulted in more caution being taken while restraining him, rather than less. Even the go-to excuse for in-custody deaths -- "excited delirium" -- is supported by plenty of documentation that shows hog tying suspects or holding them down with body weight increases the risk of death.

But at the end of it, the thing that undoes these officers' planned exit from this lawsuit is their own video. The court brings it up again in support of its qualified immunity denial.

> *Although the Officers presented their own version of events that included claims of Aguirre's resistance—including, for example that he "was resisting and trying to pull away from" the Officers while walking near the westbound side of the median, "was still resisting" when placed on the hood of the car, and "continued to resist by shifting his body around and trying to break free" while pinned against the hood of the patrol car—these averments in contravention of what the police dashcam videos show do no more than reinforce that genuine disputes as to material facts exist at this stage of the litigation.*

Clearly established enough, adds the Fifth, even without a case directly on point. The difference between "hog tying" and "maximal prone restraint" isn't enough to make it unclear to these "reasonable" officers whether the use of these nearly identical techniques in situations like this would be "excessive."

Whether or not the Supreme Court's recent hints nudged this in the right direction, at least the correct conclusion was reached: restraining someone to death -- especially an unresisting someone -- clearly violates their rights.

Read More | 8 Comments »

Only 14% Of Americans Think Communities Shouldn't Be Allowed To Build Their Own Broadband Networks

from the *listen-to-the-people* dept

by Karl Bode - May 3rd @ 1:39pm

A new poll from Morning Consult indicates that only around 14% of Americans think that communities should **not** be allowed to build and operate their own, local broadband networks:

source: imgur.com

That of course operates in pretty stark contrast to the 18 states that have passed obnoxious laws, usually written by incumbent broadband providers, that hamstring such efforts or ban them entirely. That total used to be 19 (Arkansas eliminated many of their restrictions earlier this year), and will soon be 17 (given Washington State just passed a law eliminating its restrictions as well).

The survey found that Democrats and urban residents are more likely that rural and Republican residents to support such options. But that too runs a bit in contrast with reality, given that the majority of community built broadband networks exist in more conservative leaning cities. Like a lot of tech subjects (net neutrality comes to mind),

entrenched business interests have successfully framed community broadband as a "partisan issue," which is a great way to stall consensus on a subject you oppose for purely selfish, successful reasons.

Industries, and the captured regulators and lawmakers who love them, adore demonizing such efforts as "socialism run amok" or automatic taxpayer boondoggles. But that's again not based on reason. Such efforts are an organic, grass roots reaction to market failure and monopolization. The efforts aren't pursued *because their fun*, they're pursued because Americans have, over thirty years, grown increasingly frustrated at the high cost, slow speeds, and terrible customer service that's the direct result of regional monopolization.

Christopher Mitchell, one of the country's top experts on the subject, tells me that COVID has really highlighted how stupid and unnecessarily punitive such restrictions are. But overall, it has proven harder and harder for regional monopolies to buy laws restricting community broadband:

> *"No new state has added a barrier in 10 years," said Christopher Mitchell, director of the Community Broadband Networks Initiative at the Institute for Local Self-Reliance. "The more recent dynamic has been states removing them."*

Interestingly, the survey did show that many Americans trust the private sector more than they do their local government when it comes to actually running the networks. Roughly 54% of respondents said they had either "a lot" or "some" trust in local governments to provide the best at-home internet service, while 75% said the same about private internet providers. Cable lobbyists were quick to then claim this is because US telecom providers are akin to "LeBron James":

> *"James Assey, executive vice president at cable lobby NCTA - The Internet & Television Association, said adults are aware of the potential failures of public infrastructure, such as electric grids or bridges. "In the same way if I was playing basketball, I'd want LeBron James on my team — I would want the people who do this day-in and day-out to help us bridge the divide that we know exists today," Assey said."*

I imagine if you really sat Americans down and asked them if they view Comcast and AT&T as the tech equivalent of LeBron James you'd probably see some... pointed responses to that comparison. Again, community broadband is a direct, organic response to failures by the private sector, which routinely hoovers up millions in taxpayer subsidies, tax breaks, and regulatory favors in exchange for networks only half completed. Such networks aren't a silver bullet, and of course depend on the competency of your local government and the quality of the business plan.

And while the Biden broadband plan leans heavily on community broadband, it's not

really an either or scenario. In the absence of functional regulatory oversight or competition, community broadband often acts as a way to pressure industry into trying harder, lowering prices, and upgrading their networks. If industry wants to avoid the "vile socialism" that is communities offering better, faster, cheaper fiber broadband, there's an easy option that doesn't involve buying shitty state laws that undermine the will of voters: do better.

8 Comments »

Rep. Lauren Boebert Decides To Streisand Parody Site Making Fun Of Her, Threatens To Take Legal Action Against It

from the *supporting-the-1st-Amendment* dept

by Mike Masnick - May 3rd @ 12:06pm

Rep. Lauren Boebert is one of the new crew of elected Republicans who claims to be "pro-Constitution" and "pro-freedom" but when you get down into the details, it seems that the only part of the Constitution that matters to her is the 2nd Amendment. The website for her campaign proudly states that she's "Standing for Freedom" and is "Pro-Freedom, Pro-Guns, Pro-Constitution."

You do have to wonder if she skipped over the 1st Amendment in her rush to defend the 2nd, however. This morning, her press secretary Jake Settle (who came to her office after working on Mike Pence's communications team) sent quite a fascinating threat email to the operator of a Lauren Boebert parody site, TheLaurenBoebert.com.

The operator of that site, comedy writer Toby Morton, tweeted an image of the letter this morning:

> Hello Lawyers/Smart People - Lauren Boebert wants me to take down https://t.co/zjr5H9soIR. What say you @AriCohn @Popehat @ASFleischman @adamsteinbaugh @Jturk125 @wolmanj @questauthority @mmasnick @KathrynTewson @RichSeviora @thewolflawyer @estockbridge @USConst_Amend_I pic.twitter.com/FgBdXFdaCR
>
> — Toby Morton (@tobymorton) May 3, 2021

[Click to view this post on Techdirt with embedded content.]

I have since seen the original email that does, indeed, appear to come from Jake Settle. I have emailed Jake to confirm his side of the story, and asked him to answer a few questions as well. At the time of writing he has not responded. The email says the following:

> *To whom it may concern,*
>
> *This website (https://www.thelaurenboebert.com/) needs to be taken down since the photos on here are copyrighted property of the U.S. Federal Government. They are the property of the office of Congressman Lauren Boebert, and your use of them is unauthorized and illegal.*
>
> *Additionally, the entire website is a defamatory impersonation, and it goes against relevant terms of service and U.S. law. Please remove immediately or face further action.*
>
> *Sincerely,*
>
> *Jake Settle | Press Secretary*
> *Rep. Lauren Boebert (CO-03)*

If you're wondering what the parody site looks like, it does use the same main image as Lauren's official Congressional site (different from her campaign site). Here's what the mobile version of the parody site looks like:

And here's her official Congressional site (note the same image):

The parody site honestly doesn't have that much more on it. It shows a couple Boebert tweets, then has links to some other parody sites of wacky Republican members of Congress and Senators, and says that it's a parody site (which isn't just a talisman where saying it automatically makes it true). **Update:** There actually is a bit more on the website that I had missed on first pass: under the "blog" tab, there are some posts that include a number of images of Boebert. It is extremely unlikely that the copyright to any of those works are held by the US government. It is possible that some are held by Boebert herself (unclear if her Congressional Office would hold the copyright), but we'll get there.

Before we even dig into the legal analysis of Settle's threat letter, let's just make one thing clear: whether or not there's a legal leg to stand on, Settle's threat is **stupid**. All this has served to do is to Streisand a parody site that likely wasn't receiving much if any traffic prior to this. Indeed, Morton has confirmed to me that the site hadn't received much traffic, but now tons of people are looking at it. At *best*, Boebert comes off looking like a thin-skinned insecure whiner who can't take a mild parody. At worst, she comes off as a censorial bully who has no respect for "freedom" if it's associated with the 1st Amendment.

As for the legal issues... Settle's email is a mess of confusing concepts, so it's not even remotely clear what any actual legal claim might look like (which is not to say there are none -- just that Settle's email most certainly does not lay out a clear theory of one). First up, the copyright claims are a mess.

> *This website (https://www.thelaurenboebert.com/) needs to be taken down since the photos on here are copyrighted property of the U.S.*

> *Federal Government. They are the property of the office of Congressman Lauren Boebert, and your use of them is unauthorized and illegal.*

It's not entirely clear how they could be both the "copyrighted property" (which is not a thing) of "the U.S. Federal Government" and "the property of the office of Congressman Lauren Boebert" at the same time. There's only the one image on the front of the site as far as I can see, and it **might** be true that Boebert holds the copyright to it. A lot of people responded to Toby's tweet and *falsely* claimed that since it's on a government website it's public domain. That is not true. US copyright law does say that works created by the government are in the public domain and not subject to copyright. **But** (and this is important) that does not mean every work the government uses or posts to its website is automatically in the public domain. Other copyright holders can transfer a work to the government, and the government could then retain the copyright.

In this case, it seems highly unlikely that the work was created by the federal government. It is quite likely that it was created by Lauren Boebert's campaign or someone closely associated with Boebert and the campaign. There are then all sorts of possibilities about the copyright. It could be held by the photographer. It could be held by the Boebert campaign, or by Boebert herself if the copyright was assigned to her. In theory, it *could* have been assigned to the federal government, but that seems **highly** unlikely.

The claim that it is the "copyrighted property" of the US government seems like it is likely nonsense. The claim that its held by Boebert's office is not entirely crazy. However, even if that were true, Morton would have a very strong fair use argument, seeing as that he's set up a parody site. Parody is one of the quintessential examples of fair use. As the Supreme Court has said, the context of the use of the original work in a parody does matter, so it's not *automatically* fair use.

> *In parody, as in news reporting, see Harper & Row, supra, context is everything, and the question of fairness asks what else the parodist did besides go to the heart of the original.*

So, perhaps there's some argument somewhere that would persuade a court that this is not fair use, but that seems unlikely. The fact that this is parodying a politician, and criticizing or even mocking politicians is part of what the US considers an important element of our 1st Amendment free speech protections, it seems highly likely that any court would come down on the side of fair use should a copyright claim be brought.

As for the images on the "blog" portion of the site, there is perhaps an argument that some of those copyrights are held by Boebert (certainly not the federal government). Could those lead to a lawsuit? Very possibly, but if that was the case, the copyright holder should have sent a takedown notice first. Whether or not those images are fair use is a tougher call. They are used for criticism and commentary, which is part of the

fair use analysis, but there isn't *that much* commentary on them, and so it really would be up to the court where this landed. Still, at the very least, it doesn't make much sense for her press secretary to be sending out that threat letter, though.

As for the other claim of "defamatory impersonation" well...

> *Additionally, the entire website is a defamatory impersonation, and it goes against relevant terms of service and U.S. law. Please remove immediately or face further action.*

"Defamatory impersonation" is not a thing. Defamation is. But it's difficult to see anything on the website that would qualify as a defamatory statement of fact. The only real statements on the website about Boebert are calling her a "racist" and a "Qanon sympathizer" and both of those are either protected opinion, or substantially true. Either way, there's simply no way any defamation claim here would meet the actual malice standard necessary for defamation of a public figure (and as a member of Congress, Boebert is undoubtedly a public figure).

So, even if there is a legal claim buried in here, it's difficult to see it getting very far. But, either way, just sending such a threat is inherently stupid.

37 Comments »

What3Words Sends Ridiculous Legal Threat To Security Researcher Over Open Source Alternative

from the *never-use-what3words* dept

by Mike Masnick - May 3rd @ 10:47am

A couple years we wrote about What3Words, and noted that it was a clever system that created an easy way to allow people to better share exact locations in an easily communicated manner (every bit of the globe can be described with just 3 words -- so something like best.tech.blog is a tiny plot near Hanover, Ontario). While part of this just feels like fun, a key part of the company's marketing message is that the system is useful in emergency situations where someone needs to communicate a very exact location quickly and easily.

However, as we noted in our article, as neat and clever as the idea is, it's very, very proprietary, and that could lead to serious concerns for anyone using it. In our article, we wrote about a bunch of reasons why What3Words and its closed nature could lead to problems -- including the fact that the earth is not static and things move around all the time, such that these 3 word identifiers may not actually remain accurate. But there were other problems as well.

And, apparently one of those problems is that they're censorial legal bullies. Zach Whittaker has the unfortunate story of how What3Words unleashed its legal threat

monkeys on a security researcher named Aaron Toponce. Toponce had been working with some other security researchers who had been highlighting some potentially dangerous flaws in the What3Words system beyond those we had mentioned a few years back. The key problem was that some very similar 3 word combos were very close to one another, such that someone relying on them in an emergency could risk sending people to the wrong location.

The company insists that this is rare, but the research (mainly done by researcher Andrew Tierney) indicates otherwise. He seemed to find a fairly large number of similar 3 word combos near each other. You can really see this when Tierney maps out some closely related word combos:

> When this happens, you get cells with these offset areas *very* closely matched.
>
> We can see that the row above the banding has a "q" (the value on "n" on the lower left) that is approximately 14,560,000 lower than the cell below. pic.twitter.com/pYumzdxyTh
>
> — Cybergibbons (@cybergibbons) April 27, 2021

Toponce also admits he couldn't even sleep after receiving the threat letter. This is an underappreciated aspect of the insanely litigious nature of many censorial bullies these days. Even if you're in the right, getting sued can be completely destructive. Toponce was trying to help security researchers better research an application that is **promoted for being safe** and security researchers **should** be allowed to make use of reverse engineering to do exactly that. But, What3Words and their bullying lawyers made sure that's impossible.

To be fair to their bullying lawyers, the threat letter is not *as* aggressive as some others, and they even make it explicit that they are not seeking that Toponce stop criticizing the company:

> *In this connection, and to be clear, our client does not require the deletion of your criticism of and feedback in respect of its service.*

But... it still makes pretty stringent demands.

> *i) delete all copies of "What Free Words" and any other works derivative of W3W's software and wordlist presently in your possession or under your control;*
> *ii) confirm, to the best of your knowledge, the identities of all parties / individuals to whom you have provided copies or derivations of the*

software and/or wordlist;
iii) agree that you will not in the future make further copies or derivations of and/or distribute copies or derivations of the software and/or wordlist;
iv) delete any Tweets or other online references made to the copies / derivations of our client's software and wordlist and that are connected with or emanate from the "What Free Words", and agree not to make similar representations in the future.

Of course, there are some questions about **what** intellectual property is actually being infringed upon here as well. When the company's lawyers got the original WhatFreeWords site taken down, they claimed copyright and trademark rights, though extraordinarily broadly. They claim their own software is covered by copyright, but WhatFreeWords isn't using their software. They also claim that all the 3 word combos are covered by copyright and... eh... it might be in the UK where W3W is based, but in the US, it would be harder to claim that three random word combos are creative enough to get a copyright. Also, in the US there would be a strong fair use defense. Unfortunately, in the UK, there is a ridiculous concept known as "database rights" that let you claim a right over a mere collection of things, even if you have no claim to the underlying rights. But, even so, it seems that there should be a fair use defense here. The UK has a fair dealing exception for research and private study, which seems like it should apply as well.

As for the trademark claims, well, no one's going to get confused about it, since it's pretty clear that WhatFreeWords was designed explicitly not to be from What3Words, and in this particular case, it's not being offered widely, just to knowledgeable security researchers. Even more insane: the original threat letter over WhatFreeWords claimed that there could be **criminal penalties** for violating consumer protection laws, and that's just insane.

Still, as Mike Dunford notes in his thread about this situation, W3W's decision to focus on locking up and threatening everyone perhaps explains why so few people know about or use What3Words. Imagine if they had built this as an *open* tool that others could build on and incorporate into other offerings. Then they could have others experiment and innovate and get more people to adopt it. By making it proprietary, and locking it down with threats and asshole lawyers, there's simply no reason to bother.

The only proper response to this is **never, ever use What3Words for anything that matters**. Beyond not giving in to censorial, abusive bullies, their legal reaction to a security researcher doing reverse engineering work to help find **potentially dangerous problems** with What3Words screams loudly to the world that What3Words has no confidence that it's products are safe. They're scared to death of security researchers being able to really test their work.

Both of these reasons means that What3Words should be remembered as little more

than a failed.dumpster.fire rather than the cool.mapping.idea it could have been.

Read More | 21 Comments »

Daily Deal: The CompTIA Security Infrastructure Expert Bundle

from the *good-deals-on-cool-stuff* dept

by Daily Deal - May 3rd @ 10:42am

In the CompTIA Security Infrastructure Expert Bundle, you'll get comprehensive preparation to sit four crucial CompTIA exams: Security+, CySA+, CASP, and PenTest+. You'll learn how to implement cryptographic techniques, how to provide operational, information, application and infrastructure level security, how to analyze vulnerabilities, and more. The bundle is on sale for $30.

source: imgur.com

Note: The Techdirt Deals Store is powered and curated by StackCommerce. A portion of all sales from Techdirt Deals helps support Techdirt. The products featured do not reflect endorsements by our editorial team.

Comment »

Hollywood Lobbyists So Afraid Of Any Public Benefit From 'Intellectual Property' That They're Trying To Block COVID Vaccine Sharing

from the *you-did-what-now?* dept

by Mike Masnick - May 3rd @ 9:30am

Throughout the COVID pandemic, it's been truly shameful to watch how patent maximalists have tried to insist that we just need more patents to deal with COVID -- even though the incredible breakthroughs that brought such quick development of vaccines were not due to patents, but rather the free and open flow of information from a bunch of researchers and scientists who didn't care about whether or not information was locked up for profit, but did care about saving millions of lives.

And now that we've got vaccines, we're dealing with significant problems in rolling them out around the world -- and patents are often in the way, holding that rollout back. And we actually have a way of dealing with that: what's known as a TRIPS waiver. TRIPS is the Agreement on Trade-Related Aspects of Intellectual Property Rights, which set up a variety of standards among member nations and the WTO

regarding intellectual property. I have many problems with TRIPS (and the WTO), but TRIPS does include a process to grant waivers on intellectual property rights. This was in response to (very legitimate!) concerns by less well off nations that rich nations would use the patent system to block access to important life saving medicines.

So, to ease such concerns, the TRIPS agreement includes a process by which the WTO can grant a compulsory licensing regime that will allow others to make patented drugs, and thus increase availability. A key point of this so-called waiver is that it allows for better allocations of certain drugs during medical emergencies. Given that, issuing such a waiver right now seems like a no-brainer. But... it has not been.

India and South Africa put forth a a fairly straightforward waiver request for dealing with COVID-19. The key part of the request is that intellectual property requirements under TRIPS **solely in relation to the "prevention, containment or treatment of COVID-19"** should be waived during the course of the pandemic. It seems pretty straightforward. Even reliable patent maximalist sites like IP Watchdog are now publishing articles saying that the TRIPS waiver "is a necessary first step towards facilitating increased, rapid production of vaccines" and noting that it won't undermine the value of innovation in any way.

We've already noted that Big Pharma is lobbying against it -- which is to be expected. However, what is perhaps less expected is the fact that Hollywood is vehemently lobbying against it as well. Why? Well, they claim that because the waiver is not limited to just patents, it will be used to wipe away copyright as well.

This is... misleading at best. It is true that the waiver would cover copyrights, but only in an extremely limited fashion. As the part I quoted above notes, it only applies to intellectual property protections that are blocking the prevention, containment, and treatment of COVID-19. And, that *can* include a very limited set of copyrights. For example, there still remain shortages of ventilators in many parts of the world, and early on in the pandemic, people were working on 3D printing replacement parts to help deal with this extreme shortage. However, with some companies issuing threats over these 3D printed parts, there are legitimate concerns that copyright could be used to shut down such operations. Another area where a copyright waiver is likely to help is in allowing researchers easier access to important scientific journals and research that may help them develop more and better solutions.

As if to make Hollywood calm down, South Africa and India included an **explicit statement** in the waiver request to say that the waiver cannot be used for entertainment products: "The waiver in paragraph 1 shall not apply to the protection of Performers, Producers of Phonograms (Sound Recordings) and Broadcasting Organizations under Article 14 of the TRIPS Agreement." That's literally the 2nd paragraph in a four paragraph waiver request. Already, it's kind of insulting that officials crafting this waiver request in an attempt to save lives had to waste time making sure that Hollywood wouldn't get angry at them.

And even then it didn't work.

> *The Motion Picture Association, which represents major movie and television studios, deployed five lobbyists to influence Congress and the White House over the waiver. The Association of American Publishers as well as Universal Music have similarly revealed that they are actively lobbying against it.*
>
> *Neil Turkewitz, a former Recording Industry Association of America official, blasted the proposal on Twitter, claiming it will harm musicians, performers, and other cultural workers who are already struggling.*
>
> *"As COVID has undermined the livelihoods of creatars around the [globe emoji], you want to further expand their precarity—in the name of justice?" Turkewitz wrote.*

The Turkewitz quote is particularly disgusting. There is nothing in the waiver that will harm the livelihood of creators. Indeed, **getting the world vaccinated** is how we bring things back to normal to help open up the world to help those musicians, performers, and other cultural workers survive. For him to even suggest that this waiver somehow harms them is not just disinformation, it's disinformation that will kill people. It's disgusting.

And the lobbying by Hollywood goes beyond just what was reported in the above linked Intercept article. ITIF, the Information Technology and Innovation Foundation, which may *sound* like a think tank that is focused on the tech industry, but which has long had close ties to Hollywood (and, indeed, an ITIF paper was the basis for the terrible SOPA/PIPA laws a decade ago), recently came out with a laughably ridiculous attack on the waiver, claiming that there's no possible way copyrights should be included in it:

> *This latest affront to IP rights is, to say the least, ill-placed, if not misinformed. There is simply no compelling reason to focus on the suspension of copyright in this case.*

Oh come on. People are fucking dying and this is the fight you want to have? It's not "suspension of copyright" that people are asking for. They're asking for a narrowly tailored, specific exemption to excessively restrictive copyright **solely** in cases where that exception is needed to help fight COVID. The idea that it is "ill-placed" or "misinformed" is pure propaganda.

And then, just as I was putting the finishing touches on this article, Senator Thom Tillis, who has made it clear that his main goal in the Senate is to push for Hollywood's extremist interests, wrote up one hell of an oped against the waiver. It is chock full of nonsense.

> *Yet, waiving intellectual property rights abroad would not hasten the end of COVID-19. It would harm our domestic IP industries, hand India and China valuable government-supported research free of charge and weaken the global IP system for decades to come. Just last week, in remarks before the Intellectual Property Owners Association (IPO) Spring Summit Daren Tang, Director General of the World Intellectual Property Organization (WIPO), stated that a strong intellectual property ecosystem was primarily responsible for allowing COVID-19 vaccines to "be brought to people in the fastest time in history." I wholeheartedly agree...*

First off, it wouldn't "harm" any domestic industry. That's nonsense. And if the research is for **saving lives** and (as Tillis states) was "government-supported" then it **should be freely available to anyone.** Government supported research means that the public paid for it and it should be widely available to anyone.

Second, just because a long time advocate of patent and copyright maximalism says something, doesn't automatically make it true. There is no **evidence whatsoever** that "strong intellectual property... was primarily responsible for allowing COVID-19 vaccines" to come about. Indeed, the stories about how the vaccines were developed show the opposite. They show how the free flow of information and ideas among researchers and scientists around the globe, and them agreeing to work together, rather than trying to lock up ideas, is what helped make it possible.

I can understand pharma companies fighting against it, even if that alone is disappointing given the situation. That Hollywood and its friends are flat out lying about it and creating a moral panic, claiming this will somehow hurt the creative industries, is dangerous disinformation.

Read More | 27 Comments »

Roku Users Lose Access To YouTube TV As Dumb Contract Fights Shift From Cable TV To Streaming

from the *meet-the-new-boss* dept

by Karl Bode - May 3rd @ 6:12am

For decades now, cable TV consumers have been subjected to idiotic cable TV "retransmission feuds" that black out content consumers pay for as broadcasters and cable operators bicker over rates. And while streaming TV was supposed to remedy many of the dumber aspects of the traditional cable TV model, that's not really happening. The names and gatekeepers are simply shifting.

Case in point: last year, bickering between AT&T and Roku over ad data sharing and contract details prevented AT&T's HBO Max from appearing on Roku devices. Later on

last year, Sinclair-owned CBS stations were pulled from Hulu completely because the two sides couldn't put on their big boy pants and agree to a new contract without taking it out on paying subscribers.

This week, it's Roku and Google (YouTube TV) in a standoff that resulted in the YouTube TV app being pulled from the Roku channel store. YouTube TV (not to be confused with vanilla YouTube) is Google's live TV streaming alternative to traditional cable. Users who already have it installed can still use it, but those who just bought the service and want to install it can't do so as of today. Fortunately this isn't a full ban either, since there's still a workaround that involves casting content from your phone, tablet, or PC to the Roku in a way that's a little more cumbersome but doesn't require the YouTubeTV app.

Why the hassle in the first place? Roku, in a statement earlier this week, claimed Google was abusing its "monopoly position" (which really doesn't make sense when talking about live streaming TV, where they're a relatively niche player) to do all sorts of dastardly things:

> *"Google is attempting to use its YouTube monopoly position to force Roku into accepting predatory, anti-competitive and discriminatory terms that will directly harm Roku and our users. It should come as no surprise that Google is now demanding unfair and anti-competitive terms that harm Roku's users."*

Google then issued a statement claiming Roku was just being a bully:

> *"We have been working with Roku in good faith to reach an agreement that benefits our viewers and their customers. Unfortunately, Roku often engages in these types of tactics in their negotiations. We're disappointed that they chose to make baseless claims while we continue our ongoing negotiations. All of our work with them has been focused on ensuring a high quality and consistent experience for our viewers. We have made no requests to access user data or interfere with search results. We hope we can resolve this for the sake of our mutual users."*

Roku says it's not demanding any additional money, even though these debates always revolve around money in one form or another. How much access each side has to valuable user usage data, where and how channels see placement within the GUI, search results, etc. But whichever side is to blame, it's all stuff that should be getting hammered out by adults long before it bubbles over into a giant annoyance that impacts consumers.

A YouTube TV blog post offers a little more detail, stating that Google simply wanted its existing contract renewed, but Roku, buoyed by significant user growth thanks to COVID lockdowns, has been getting increasingly demanding in negotiations. The post

also notes that Google really wants Roku to get on board with the AV1 codec, so things, you know, work:

> *"Our agreements with partners have technical requirements to ensure a high quality experience on YouTube. Roku requested exceptions that would break the YouTube experience and limit our ability to update YouTube in order to fix issues or add new features. For example, by not supporting open-source video codecs, you wouldn't be able to watch YouTube in 4K HDR or 8K even if you bought a Roku device that supports that resolution."*

While I doubt Google is faultless, I do tend to think Roku is starting to get cocky as it gets more powerful. And while I'll admit a certain enjoyment in traditional telecom monopoly gatekeepers like AT&T and Comcast whining about unfair gatekeeping behavior of streaming hardware companies, none of this is what adult professionals doing business should look like, and I worry a lot of these kinds of disputes will only be getting worse. Traditionally, regulators like the FCC have treated this kind of stuff as just "boys being boys." That, in turn, generally results in nobody, at any point, looking out for the interest of the end user.

22 Comments »

Visit Techdirt for today's stories.

Subject: Techdirt Daily Newsletter for Thursday, 13 May, 2021
Date: Thursday, May 13, 2021 at 4:26:44 AM Mountain Daylight Time
From: Techdirt Daily Newsletter <newsletters@techdirt.com>
To: Techdirt Daily Newsletter Subscriber <tanidowning@utah.gov>

read it online

Techdirt Email.

Stories from Wednesday, May 12th, 2021

Are you interested in receiving a shorter, easy-to-scan, email of post excerpts? Check our our new

Techdirt Daily Newsbrief

Estate Of 'Tintin' Comic Creator Loses On Fair Use Grounds To Artist Putting Tintin Alongside Women

from the *comic-con-job* dept

by Timothy Geigner - May 12th @ 8:10pm

By way of a throat clearing, there are a couple of things you need to know about Hergé, the nom de guerre for the artist behind the well-known *Tintin* comics of yore. First, Hergé's estate has found its way onto Techdirt's pages before and has a reputation for being wildly restrictive and litigious over any use or reference to *Tintin*. Alongside that, you need to know that Hergé absolutely did every last thing he could to keep women entirely out of his comic strips. His reasoning for this can be best summarized as a combination of having a too much "respect" for women to include them in his humor comic... and also that women, according to his estate, were "rarely comic elements." Women, in other words, are bad for humor.

So it makes perfect sense that a modern artist decided to create new material featuring Tintin in romantic or risqué settings with women and both parody and commentary on the original works. And, likewise, it makes perfect sense that the Hergé estate sued over it.

> *In Breton artist Xavier Marabout's Hergé-Hopper mashupsTintin is variously painted into Hopper's Road and Houses, scratching his head as he greets a woman in a car; looking disgruntled in a version of Hopper's Cape Cod Evening, 1939; and kissing a girl in a car, in a spin on Hopper's Queensborough Bridge, 1913. On his website, Marabout describes his work as "strip art", in which he "strips distant artistic universes to merge them together" in a style where "parody [is] omnipresent".*

> *But the Moulinsart company, which manages the Tintin business, disagrees, accusing Marabout of reproducing the world of Tintin without proper consent.*
>
> *"Taking advantage of the reputation of a character to immerse him in an erotic universe has nothing to do with humour," a lawyer for the company said in court in Rennes this week, where Moulinsart has sued for infringement, as reported by Ouest-France.*

Thankfully for the entire world, lawyers are not generally considered the arbiters of humor. And there is good reason for that. Most fair use equivalents throughout the world carve out specific exemptions for parody and commentary for this very reason. New artists seeking to provide social commentary, through humor or otherwise, need the room to produce that commentary. The upturned nose of some estate lawyer somewhere is not supposed to be a barrier.

With that in mind, Marabout's rebuttal to the suit is roughly what you would expect.

> *In response, Marabout's lawyer claimed the paintings were parody, reported Ouest-France, and cited a "conflict between copyright and freedom of expression and creation", asking: "Does an artist have the right to wonder about Tintin's sex life?" and "what about artistic freedom?" The Rennes court will rule in May.*
>
> *Marabout told the Guardian that his work echoed the historian Christian Jacob's belief that "there is no cultural transmission without reappropriation".*

Imagine a world in which an artist couldn't create artistic commentary on a socially important icon simply due to copyright law. More to the point, imagine one artist attempting to restrict artistic commentary from another on those same grounds. It's absurd and negates the way that art and commentary are made, not to mention that it hand-waves the importance of that commentary to society.

Fortunately, it appears that the French courts agree.

> *On Monday, Moulinsart's complaint was rejected by the court in Rennes. "The court recognised the parody exception and the humorous intention expressed by my client," Marabout's lawyer, Bertrand Ermeneux, said.*
>
> *The Rennes court also said that Moulinsart had "denigrated" Marabout by contacting galleries showing his work to say that it was infringing, Huffington Post France reported, adding €10,000 (£8,500) in damages for Marabout and €20,000 in legal fees to its ruling.*

Given how the legal system has let the Hergé estate run roughshod over others in the

past, this is as good an outcome as one could hope for. To not only see the suit tossed, but to see Moulinsart punished monetarily for his bullying ways is a breath of fresh air.

Still, we're left with the never ending question: why can't fellow artists and content producers understand that the same protections that protect their work also apply to other artists?

10 Comments »

Content Moderation Case Study: YouTube's New Policy On Nazi Content Results In Removal Of Historical And Education Videos (2019)

from the *godwin-in-effect* dept

by Copia Institute - May 12th @ 3:50pm

Summary: On June 5, 2019, YouTube announced it would be stepping up its efforts to remove hateful content, focusing on the apparent increase of white nationalist and pro-Nazi content being created by users. This change in algorithm would limit views of borderline content and push more viewers towards content less likely to contain hateful views. The company's blog post specifically stated it would be removing videos that "glorified Nazi ideology."

Unfortunately, when the updated algorithm went to work removing this content, it also took down content that educated and informed people about Nazis and their ideology, but quite obviously did not "glorify" them.

Ford Fischer -- a journalist who tracks extremist and hate groups -- noticed his entire channel had been demonetized within "minutes" of the rollout. YouTube responded to Fischer's attempt to have his channel reinstated by stating multiple videos -- including interviews with white nationalists -- violated the updated policy on hateful content.

A similar thing happened to history teacher Scott Allsop, who was banned by YouTube for his uploads of archival footage of propaganda speeches by Nazi leaders, including Adolph Hitler. Allsop uploaded these for their historical value as well as for use in his history classes. The notice placed on his terminated account stated it had been taken down for "multiple or severe violations" of YouTube's hate speech policies.

Another YouTube user noticed his upload of 1938 documentary about the rise of the Nazi party in Germany had been taken down for similar reasons, even though the documentary was decidedly anti-Nazi in its presentation and had obvious historical value.

Decisions to be made by YouTube:

- Should algorithm tweaks be tested in a sandboxed environment prior to rollout

to see how often they're flagging content that doesn't actually violate policies?
- Given that this sort of mis-targeting has happened in the past, does YouTube have a response plan in place to swiftly handle mistaken content removals?
- Should additional staffing be brought on board to handle the expected collateral damage of updated moderation policies?

Questions and policy implications to consider:

- Should there be a waiting period on enforcement that would allow users with flagged content to make their case prior to being hit by enforcement methods like demonetization or bans?
- Should YouTube offer some sort of compensation to users whose channels are adversely affected by mistakes like these?
- Should users whose content hasn't been flagged previously for policy violations be given a benefit of a doubt when flagged by automated moderation efforts?

Resolution: In most cases, content mistakenly targeted by the algorithm change was reinstated within hours of being taken down. In the case of Ford Fischer, reinstatement took longer. And he was again demonetized by YouTube in early 2021, apparently over raw footage of the January 6th riot in Washington, DC. Within hours, YouTube had reinstated his account, but not before drawing more negative press over its moderation problems.

Originally published to the Trust & Safety Foundation website.

Comment »

New York Police Union Tells NYPD End Of Qualified Immunity Will Force Officers To... Act Lawfully

from the *kind-of-an-anti-climax* dept

by Tim Cushing - May 12th @ 1:57pm

One of the NYPD's unions -- the Sergeants Benevolent Association (SBA) -- is feeling ways about stuff again. Last month, the New York City Council passed a number of police reforms which included taking away qualified immunity as a defense in civil lawsuits filed in local courts. The bill has yet to receive the governor's signature, but the SBA is already making its unhappiness known.

The SBA issued a statement (via its lawyers) about the supposed downsides of giving the public a fighting chance in civil rights lawsuits. And in doing so, it has inadvertently generated a few arguments against qualified immunity, as Jay Schweikart points out at Unlawful Shield.

What was written as a cautionary advisory about the changing legal atmosphere is instead an unforced error that shows how often cops are protected by this immunity

even when it's clear they've violated rights. First, the SBA restates the doctrine's intent:

> *Qualified immunity means that government employees are immune from lawsuits if they acted reasonably and not in violation of a "clearly established statutory or constitutional right." It is designed to protect all government employees and officials from lawsuits and liability when they perform their duties in good faith and within what one reasonably believes to be the scope of existing law.*

But then it skips right past all the case law that shows the doctrine protects plenty of bad faith actions and unreasonable officers. As Schweikart notes, truly reasonable officers know where the Constitutional lines are drawn and have no need to worry about not being protected if sued.

> *Officers who are genuinely acting in good faith aren't violating anyone's rights in the first place, so by definition, they don't need qualified immunity to protect them. By suggesting otherwise to their members, these unions are engaged in reckless, dishonest fearmongering.*

And that's where the SBA letter veers into an unintended endorsement of ending qualified immunity. Cloaked in language that suggests law enforcement officers should do *less* law enforcement until the legal pendulum swings firmly back in their favor, the SBA explicitly tells officers how to avoid being sued. And it's a really simple fix that doesn't need to rely on deliberate work slowdowns or underenforcement.

> *As a direct result of the passage of this law, and the unavailability of the defense of qualified immunity under its provisions, we advise that you proceed with caution when taking any police action which could lead to physical engagement with any person, and avoid physical engagement to the greatest extent possible while also assuring your own safety and the safety of others. Also, you are strongly cautioned against engaging in any stop & frisk (unless doing so for your own or others' safety), search of a car, residence, or person* ***unless you are certain that you are clearly and unequivocally within the bounds of the law*** *. . .*

How hard is that to figure out? The Constitution has been around for a long time. While there are still some areas unexplored due to tech developments, it's been mostly clear for years how to police the public without violating citizens' rights. That officers still choose to operate outside the bounds so frequently makes it clear qualified immunity has shifted more power to the already-powerful, rather than shield the small minority of government employees who make mistakes while operating in legally-unclear areas.

Operating "clearly and unequivocally within the bounds of law" is not a difficult thing to do. Normal citizens do this all the time, despite being subject to far more unclear laws and ordinances than officers of the actual law. If an action seems brutal, vindictive, or not entirely justified, it's probably a violation of someone's rights. There's plenty of leeway given to officers to engage in their duties. Courts allow cops to lie to suspects during interrogations, take people's property with almost zero justification, draw them into reverse sting operations involving make believe contraband, and make up the law as they go along to engage in pretextual traffic stops.

And the courts have also taken a very expansive view of the term "reasonable," allowing all sorts of unreasonable violations to be waved away by innovations of qualified immunity. This is the only thing being removed by the proposed law. And it only affects cases brought in the city's courts. It's hardly the end of qualified immunity and it isn't the death knell to good policing the SBA pretends it is. If officers start exiting the force -- or refusing to do their jobs -- because QI is no longer available, it will merely indicate these officers are unable (or unwilling) to perform their duties lawfully.

8 Comments »

Canada Still Won't Commit To Supporting A Pandemic Patent Waiver

from the *inexcusable* dept

by Leigh Beadon - May 12th @ 11:57am

Few things illustrate the broken state of our global intellectual property system better than the fact that, well over a year into this devastating pandemic and in the face of a strong IP waiver push by some of the hardest hit countries, patents are still holding back the production of life-saving vaccines. And of all the countries opposing a waiver at the WTO (or withholding support for it, which is functionally the same thing), Canada might be the most *frustrating*.

Canada is the biggest hoarder of vaccine pre-orders, having secured enough to vaccinate the population five times over. Despite this, it has constantly run into supply problems and lagged behind comparable countries when it comes to administering the vaccines on a per capita basis. In response to criticism of its hoarding, the government continues to focus on its plans to donate all surplus doses to the COVAX vaccine sharing program — but these promises were somewhat more convincing before Canada became the only G7 country to *withdraw* doses from COVAX. Despite all this, and despite pressure from experts who explain how vaccine hoarding will prolong the pandemic for everyone, the country has continually refused to voice its support for a TRIPS patent waiver at the WTO.

Last week, the US finally said that it would support a waiver. This position has issues — there's no commitment to a *specific* proposal, just to negotiating a new one, so the devil is very much in the details — but the top-line promise of support for the general concept is meaningful and welcome. Some suspected that Canada might finally follow suit with, at least, a similarly open-to-interpretation promise — but apparently the government can't even go that far, and has stated that it's still "weighing support":

> *Following a meeting with his G7 counterparts, Foreign Affairs Minister Marc Garneau said discussion on whether to lift patents, as was done in the AIDS crisis, was "very active" but said Canada is still weighing the options.*
>
> *"Canada's position is that we need to obtain more vaccines, we need to all put more money into the COVAX program, and by the way Canada is the fourth largest contributor to the COVAX program, and we need to discuss with manufactures whether they're prepared to make licensing arrangements to allow greater production of the vaccine," he said in an interview on CTV News Channel's Power Play.*

This position is baffling and infuriating. Canada has already missed its chance to be a leader in the call for a truly cooperative global vaccine production strategy, and now it's missing its opportunity to at least be an early supporter among high-income countries. Meanwhile, the country's struggling rollout has convinced many citizens that its procurement has been too slow despite being the world's biggest hoarder of orders. As other countries like India face devastation, the ruling Canadian Liberal party's opposition (especially Conservative provincial premiers, who are among the most responsible for the failed rollout) are taking the opportunity to shift blame *and* bring dangerous isolationist dog whistles into the mainstream by claiming the country's only real problem is poor border controls. Canada is also struggling to fund development of a homegrown vaccine, and build out domestic manufacturing capacity that was sorely lacking when the pandemic hit. All of this is ample reason for Canada to support an IP waiver that would increase global supply, stem the spread of COVID around the world and especially in hard-hit places like India that traditionally have lots of people traveling to the country, and maybe even accelerate domestic vaccine production. Instead, Canada is hedging its bets and letting its struggling pandemic response become a partisan football in a political debate laced with misinformation and toxic nationalism while millions of Canadians — and billions around the world — still wait for their chance to get vaccinated.

16 Comments »

Florida City Officials Spend $50,000 To Find Out Who Gave Journalists A Public Record

from the *pettiest-cash-of-all* dept

by Tim Cushing - May 12th @ 10:40am

The city government of Tamarac, Florida has found a novel way to spend taxpayers' money: paying someone to find out who handed public records to someone entitled to receive public records. (h/t Peter Bonilla)

> *The cost to Tamarac taxpayers will be as much as $50,000 for the city to hire a private investigator to figure out who gave public records to a reporter, according to records released Friday.*
>
> *City leaders are scheduled to approve hiring the law firm of Kim Vaughan Lerner on Wednesday to conduct a "forensic" search to try to find who gave the South Florida Sun Sentinel a memo that is a public record in Florida.*

$50,000 from taxpayers to hire someone taxpayers likely don't believe needs to be hired to discover the source of records taxpayers are entitled to have access to. An investigation so self-serving the city can barely be bothered to defend it. But since the city holds the power and the taxpayers' purse strings, the investigation will continue.

Why are city leaders so hot and bothered they're willing to chase the paper trail of a presumptive public record that ended up in the hands of journalists? Well, it sure as shit isn't because they're concerned in any way about the public they're supposed to be serving.

No, this expensive paper chase is the result of city leaders being embarrassed by their own misuse of public funds. The budget amendments handed to the Sun Sentinel included plenty of perks for city employees -- several of which directly benefited the people approving the amendments. This $50,000 will just be more ill-spent taxpayer "revenue," joining other public expenditures that have done nothing but reward city legislators for being bad stewards.

> *The city memo in dispute had outlined several budget amendments that would benefit the city commissioners themselves, including new retirement, full health benefits, and stipends for technology and education.*
>
> *Those budget amendments, which have since been scrapped from being placed on a city agenda, came within months of other forms of spending that leaders passed for themselves to do their part-time job. That included a $25,000 personal initiative fund and a $15,000 local travel fund, on top of their salary, car and phone allowances, and out-of-town travel money.*

The $50,000 will be spent interviewing officials and staffers to determine who "leaked" presumptively-public information to the public. This includes reviewing communications sent and received by everyone currently under this super-weird form of suspicion, which apparently includes anyone with access to the budget documents. There's no word yet whether this internal investigation will manifest outwardly, but one suspects city officials willing to spend $50,000 investigating the source of public info won't shy away from targeting the journalists who published the information.

No commissioner expressed any dismay with the outsized set of perks being handed to them or the willingness to waste money investigating a non-existent breach/leak. But one commissioner mistook her public platform for a mirror, issuing this... um... statement:

> *Commissioner Debra Placko chastised whoever gave out the information, saying at last week's meeting, "Shame on you for being despicable."*

LOL. "Despicable" is spending $50,000 to find and punish the person who embarrassed you using nothing more than public records anyone could have obtained. Good luck with that. And good luck with your next election run, charlatans A-D (the decision to hire an investigator passed 4-1). This is not just stupid. It's expensive. And it does nothing more than show the public who their servants are actually serving.

12 Comments »

Daily Deal: The 2021 Complete PMP Career Training Bundle

from the *good-deals-on-cool-stuff* dept

by Daily Deal - May 12th @ 10:35am

The 2021 Complete PMP Career Training Bundle has 10 courses of training project management and different methodologies and tools. You'll learn about various methods like Lean Six Sigma, Agile, Scrum, Waterfall, and more. You'll also learn how to use Smartsheets, Trello, and Monday to help you organize and optimize your projects. One course covers what you need to know for the PMP certification exam. The bundle is on sale for $35.

source: imgur.com

Note: The Techdirt Deals Store is powered and curated by StackCommerce. A portion of all sales from Techdirt Deals helps support Techdirt. The products featured do not reflect endorsements by our editorial team.

Comment »

Bad Section 230 Bills Come From Both Sides Of The Aisle: Schakowsky/Castor Bill Would Be A Disaster For The Open Internet

from the *that's-not-how-any-of-this-works* dept

by Mike Masnick - May 12th @ 9:44am

It truly is stunning how every single bill that attempts to reform Section 230 appears to be written without any intention of ever understanding how the internet or content moderation works in actual practice. We've highlighted tons of Republican-led bills that tend to try to force websites to host more content, not realizing how (1) unconstitutional that is and (2) how it will make the internet into a giant garbage fire. On the Democratic side, the focus seems to be much more on forcing companies to takedown constitutionally protected speech, which similarly (1) raises serious constitutional issues and (2) will lead to massive over-censorship of perfectly legal speech just to avoid liability.

The latest bill of the latter kind comes from Reps. Jan Schakowsky and Rep. Kathy Castor. Schakowsky has been saying for a while now that she was going to introduce this kind of bill to browbeat internet companies into being a lot more proactive in taking down speech she dislikes. The bill, called the Online Consumer Protection Act has now been introduced and it seems clear that this bill was written without ever conferring with anyone with any experience in running a website. It's the kind of thing one writes when you've just come across the problem, but don't think it's worth talking to anyone to understand how things really work. It's also very much a kind of "something must be done, this is something, we should do this" kind of bill that shows up way too often these days.

The premise of the bill is that websites "don't have accountability to consumers" for the content posted by users, and that they need to be forced to have more accountability. Of course, this leaves out the kind of basic fact that if "consumers" are treated badly, they will go elsewhere, so of course every website has *some* accountability to consumers: it's that if they're bad at it, they will lose users, advertisers, sellers, buyers, whatever. But, that's apparently not good enough for the "we must do something" crowd.

At *best* the Online Consumer Protection Act will create a massive amount of silly busywork and paperwork for basically any website. At worst, it will create a liability deathtrap for many sites. In some ways it's modeled after the idiotic policy we have regarding privacy policies. Almost exactly a decade ago we explained why the entire idea of a privacy policy is dumb. Various laws require websites to post privacy policies, which no one reads, in part because it would be impossible to read them all. The only way a site gets in trouble is by not following its privacy policy. Thus, the incentives are to craft a very broad privacy policy that gives sites leeway -- meaning they have less

incentive to actually create more stringent privacy protections.

The OCPA basically takes the same approach, but... for "content moderation" policies. It requires basically every website to post one:

> *Each social media platform or online marketplace shall establish, maintain, and make publicly available at all times and in a machine-readable format, terms of service in a manner that is clear, easily understood, and written in plain and concise language.*

That terms of service will require a bunch of pointless things, including a "consumer protection policy" which has to include the following:

> *FOR SOCIAL MEDIA PLATFORMS.—For social media platforms, the consumer protection policy required by subsection (a) shall include—*
>
> > *(A) a description of the content and behavior permitted or prohibited on its service both by the platform and by users;*
> > *(B) whether content may be blocked, removed, or modified, or if service to users may be terminated and the grounds upon which such actions will be taken;*
> > *(C) whether a person can request that content be blocked, removed, or modified, or that a user's service be terminated, and how to make such a request;*
> > *(D) a description of how a user will be notified of and can respond to a request that his or her content be blocked, removed, or modified, or service be terminated, if such actions are taken;*
> > *(E) how a person can appeal a decision to block, remove, or modify content, allow content to remain, or terminate or not terminate service to a user, if such actions are taken; and*
> > *(F) any other topic the Commission deems appropriate.*

It's difficult to look at that list and not laugh and wonder if whoever came up with it has ever been anywhere near a content moderation or trust & safety team, because **that's not how any of this works.** Trust & Safety is an ongoing effort of constantly needing to adjust and change with the times, and there is no possible policy that can cover all cases. Can whoever wrote this bill listen to the excellent Radiolab episode about content moderation and think through how that process would have played out under this bill? If every time you change the policies to cover a new case you have to publicly update your already ridiculously complex policies -- while the new requirements be that those same policies are "clear, easily understood, and written in

plain and concise language" -- you've created an impossible demand.

Hell, someone should turn this around and push it back on Congress first. Hey, Congress, can you restate the US civil and criminal code such that it is "clear, easily understood, and written in plain and concise language?" How about we try that first before demanding that private companies be forced to do the same for their ever changing policies as well?

Honestly, requiring all of this be in a policy is just **begging** angry Trumpists to sue websites saying they didn't live up to the promises made in their policies. We see those lawsuits today, but they're kicked out of court under Section 230... but Schakowsky's bill says that this part is now exempted from 230. It's bizarre to see a Democratic bill that will lead to more lawsuits from pissed off Trumpists who have been removed, but that's what this bill will do.

Also, what "problem" does this bill actually solve? From the way the bill is framed, it seems like Schakowsky wants to make it easier for people to complain about content and to get the site to review it. But every social media company already does that. How does this help, other than put the sites at risk of liability for slipping up somewhere?

The bill then has separate requirements for "online marketplaces" which again suggest literally zero knowledge or experience with that space:

> *FOR ONLINE MARKETPLACES.—For online marketplaces, the consumer protection policy required by subsection (a) shall include—*
>
> > *(A) a description of the products, product descriptions, and marketing material, allowed or disallowed on the marketplace;*
> > *(B) whether a product, product descriptions, and marketing material may be blocked, removed, or modified, or if service to a user may be terminated and the grounds upon which such actions will be taken;*
> > *(C) whether users will be notified of products that have been recalled or are dangerous, and how they will be notified;*
> > *(D) for users—*
> >
> > > *(i) whether a user can report suspected fraud, deception, dangerous products, or violations of the online marketplace's terms of service, and how to make such report;*
> > > *(ii) whether a user who submitted a report will be notified of whether action was taken as a*

> *result of the report, the action that was taken and the reason why action was taken or not taken, and how the user will be notified;*
> *(iii) how to appeal the result of a report; and*
> *(iv) under what circumstances a user is entitled to refund, repair, or other remedy and the remedy to which the user may be entitled, how the user will be notified of such entitlement, and how the user may claim such remedy; and*

(i) how sellers are notified of a report by a user or a violation of the terms of service or consumer protection policy;
(ii) how to contest a report by a user;
(iii) how a seller who is the subject of a report will be notified of what action will be or must be taken as a result of the report and the justification for such action;
(iv) how to appeal a decision of the online marketplace to take an action in response to a user report or for a violation of the terms of service or consumer protection policy; and
(v) the policy regarding refunds, repairs, replacements, or other remedies as a result of a user report or a violation of the terms of service or consumer protection policy.

Honestly, this reminds me a lot of Josh Hawley's bills, in that it seems that both Hawley and Schakowsky want to appoint themselves product manager for the internet. All of the things listed above are the kinds of things that **most companies do already** because you need to do it that way. But it's also the kind of thing that has evolved over time as new and different challenges arise, and locking the specifics into law does not take into account that very basic reality. It also doesn't take into account that different companies might not fit into this exact paradigm, but under this bill will be required to act like they do. I can't see how that's at all helpful.

And, it gets worse. It will create a kind of politburo for how all internet websites must be run:

> *Not later than 180 days after the date of the enactment of this Act, the Commission shall conduct a study to determine the most effective method of communicating common consumer protection practices in short-form consumer disclosure statements or graphic icons that disclose the consumer protection and content moderation practices of social media platforms and online marketplaces. The Commission shall submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate with the results of the study. The report shall also be made publicly available on the website of the Commission.*

Yeah, because nothing works so well as having a government commission jump in and determine the "best" way to do things in a rapidly evolving market.

Also, um, if the government needs to create a commission to tell it what those best practices are **why is it regulating how companies have to act before the commission has even done its job?**

There are a bunch more requirements in the bill, but all of them are nitty gritty things about how companies create policies and implement them -- something that companies are *constantly* changing, because the world (and the threats and attacks!) is constantly changing as well. This bill is written by people who seem to think that the internet -- and bad actors on the internet -- are a static phenomena. And that's just wrong.

Also, there's a ton of paperwork for nearly every company with a website, including idiotic and pointless requirements that are busywork, with the threat of legal liability attached! Fun!

> *FILING REQUIREMENTS.—Each social media platform or online marketplace that either has annual revenue in excess of $250,000 in the prior year or that has more than 10,000 monthly active users on average in the prior year, shall be required to submit to the Commission, on an annual basis, a filing that includes—*
>
> > *(A) a detailed and granular description of each of the requirements in section 2 and this section;*
> > *(B) the name and contact information of the consumer protection officer required under subsection (b)(4); and*
> > *(C) a description of any material changes in the consumer protection program or the terms of service since the most recent prior disclosure to the Commission*
>
> *(2) OFFICER CERTIFICATION.—For each entity that submits an annual filing under paragraph (1), the entity's principal executive officer and the consumer protection officer required under subsection (b)(4), shall be required to certify in each such annual filing that—*
>
> > *(A) the signing officer has reviewed the filing;*
> > *(B) based on such officer's knowledge, the filing does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements, in light of the circumstances under which such statements were made, not misleading;*
> > *(C) based on such officer's knowledge, the filing fairly presents in all material respects the consumer protection*

> *practices of the social media platform or online marketplace; and*
> *(D) the signing consumer protection officer—*
>
> > *(i) is responsible for establishing and maintaining safeguards and controls to protect consumers and administer the consumer protection program; and*
> > *(ii) has provided all material conclusions about the effectiveness of such safeguards and controls.*

So... uh, I need to hire a "consumer protection officer" for Techdirt now? And spend a few thousand dollars every year to have lawyers (and, most likely a new bunch of "compliance consultants" review this totally pointless statement I'll need to sign each year? For what purpose?

The bill also makes sure that our courts are flooded with bogus claims from "wronged" individuals thanks to its private right of action. It also, on top of everything else, exempts various state consumer protection laws from Section 230. That's buried in the bill but is a **huge fucking deal**. We've talked about this for years, as various state Attorneys General have been demanding it. But that's because those state AGs have a very long history of abusing state "consumer protection" laws to effectively shake down companies. A decade ago we wrote a definitive version of this in watching dozens of state attorneys general attack Topix, with no legal basis, because they didn't like how the company moderated its site. They were blocked from doing anything serious because of Section 230.

Under this bill, that will change.

And we've seen just how dangerous that can be. Remember how Mississippi Attorney General Jim Hood demanded all sorts of information from Google, claiming that the company was responsible for anything bad found online? It later came out (via the Sony Pictures hack) that the entire episode was actually funded by the MPAA, with Hood's legal demands written by the MPAA's lawyers, as part of Hollywood explicit plan to saddle Google with extra legal costs.

Schakowsky's bill would make that kind of corruption an every day occurrence.

And, again, the big companies can handle this. They already do almost everything listed anyway. All this really does is saddle tons of tiny companies (earning more than $250k a year?!?) with ridiculous and overly burdensome compliance costs, which open them up to not just the FTC going after them, but any state attorney general, or any individual who feels wronged by the rules.

The definitions in the bill are so broad that it would cover a ton of websites. Under my reading, it's possible that Techdirt itself qualifies as a "social media platform" because

we have comments. This is yet another garbage bill from someone who appears to have no knowledge or experience how any of this works in practice, but is quite sure that if everyone just did things the way she wanted, magically good stuff would happen. It's ridiculous.

Read More | 22 Comments »

Study Finds US Broadband Gaps Three Times Worse Than The FCC Claims

from the *can't-fix-a-problem-you-can't-acknowledge* dept

by Karl Bode - May 12th @ 4:51am

As one of his last acts as Trump's FCC boss, former agency Chairman Ajit Pai released a rosy report claiming that America was making great strides in bridging the "digital divide." According to the report (pdf), 14.5 million Americans now lack access to broadband, down from 21.3 million one year earlier. This progress, Pai proclaimed, was directly thanks to his decision to effectively lobotomize the FCC's consumer protection authority at telecom lobbyist behest:

> *"From my first day as Chairman, the FCC's top priority has been closing the digital divide. It's heartening to see these numbers, which demonstrate that we've been delivering results for the American people," said FCC Chairman Ajit Pai.*
>
> *"These successes resulted from forward-thinking policies that removed barriers to infrastructure investment and promoted competition and innovation. I look forward to seeing the Commission continue its efforts to ensure that all Americans have broadband access."*

But the numbers, and the claims, were based on little more than fantasy. A new study released this week manually inspected **actual** broadband availability at 58,883 different addresses across 11 ISPs in 48 states. They found that the real number of Americans without broadband access is likely somewhere closer to 42 million, or roughly three times higher than official government estimates:

> *"The firm manually checked broadband availability for 58,883 U.S. addresses at 11 different internet service providers (ISPs) across 48 states. They then compared this data with the Form 477 data ISPs provide the FCC, and found industry and the FCC routinely over reported broadband availability all across the country."*

There's ample debate among telecom data nerds about the degree of the problem, but there's a fairly widespread consensus on the fact there really is a problem. There's

several reasons it persists. One, ISPs have historically provided overly rosy data to the FCC, which the FCC lacks the staff, resources, or sometimes willpower (if AT&T and Comcast lobbyists get their way) to accurately and consistently verify. Another reason is the FCC continues to use a bizarre methodology that declares an entire census block "served" by broadband if just one home in that block can theoretically get service:

> *"There is a widely acknowledged flaw with Form 477 reporting," the study noted. "If an ISP offers service to at least one household in a census block, then the FCC counts the entire census block as covered by that provider." In many rural areas, a census block can encompass hundreds of square miles."*

Keep in mind that independent broadband experts say the FCC also dramatically underestimates the number of Americans living under a monopoly (83 million according to some estimates). The FCC historically also doesn't do a good job collecting or sharing data on broadband prices, which helps the telecom industry downplay the obvious impact regional monopolization and corruption has on real-world consumer costs.

This has been a problem for the better part of the last few decades, meaning the lion's share of government policy decisions are being based on a distorted and unnecessarily optimistic view of the problem. This also opens the door to folks like Ajit Pai using overly inflated progress to justify policies that often harm the market and consumers (like the mindless rubber stamping of megamergers, or the elimination of FCC consumer protections on net neutrality and privacy). "We don't need competent and consistent oversight of telecom monopolies, because things are *already going so well*!"

And while the government last year passed a new law (the DATA Act) that demands the FCC fix these problems, actual fixes (assuming they're even implemented correctly) will be years away. In the interim we're doling out billions in additional subsidies to fix a problem we're still incapable of actually measuring.

9 Comments »

Manage Your Subscription

Unsubscribe Automatically

newsletters@techdirt.com
Floor64, Inc.
370 Convention Way
Redwood City, CA 94063

Facebook

Twitter

Subject: Prevent Cyberbullying, Biking into a Data Breach, Should Employers Collect Your Vaccine Status?
Date: Tuesday, May 18, 2021 at 6:30:58 AM Mountain Daylight Time
From: Jodi Daniels <jodi@redcloveradvisors.com>
To: Tani Pack <tanidowning@utah.gov>

Podcast: A Day in the Life of a CPO

In this episode of She Said Privacy/He Said Security, Jodi and Justin Daniels sit down with Mike Jones. Mike is the Chief Privacy Officer at Randstad, an employment and recruitment agency for both temporary and permanent staffing. Mike is also the Director of Global Privacy for Monster, a global company that connects employers and candidates that are searching for their perfect fit.

Listen in as Mike talks about his daily tasks and concerns as a CPO, the distinct variations between privacy and security, and how to understand — and keep up with — your state's privacy laws.

LISTEN NOW

See you at RSA?

During the *'Hooked By Phisherman: Quarterbacking Breach Response with Law Enforcement'* session from 01:55 PM - 02:55 PM PT, Justin and I will be part of an esteemed panel of experts talking about how to prepare and respond in a ransomware event.

Hope to see you there!

LEARN MORE

Peloton's API Exposes Riders' Private Data

Peloton's leaky API has allowed any hacker to obtain any user's account data — even if that user had set their profile to private.

A flaw in Peloton's online service was making data for all of its users available to anyone anywhere in the world,

even when a profile was set to private. All that was required was a little knowledge of the faulty programming interfaces that Peloton uses to transmit data between devices and the company's servers.

Data exposed included:

- User IDs
- Instructor IDs
- Group Membership
- Workout stats
- Gender and age
- Weight
- If they are in the studio or not

The company has in the meanwhile provided a partial fix, where they bike next will be crucial.

Wondering about your next ride?

READ MORE

Return to Office 'a perfect storm' of Privacy Issues for Businesses

As vaccinations continue to progress at a steady pace, many employers and employees are eager to get back into the office. But...

The number-one question for many companies has been whether an employer can implement a mandatory vaccine policy. Regulatory guidance surrounding this issue has been lacking and with no precedent to lean on, there have been many questions.

The best advice? Approach it with a privacy eye. Think about all these questions: What are we collecting? What are we going to do with it? Who is going to have access to it? What are we going to use it for?

Weigh your risks along with the option to continue with remote working if possible.

Read More on This Hot Topic

How Can Cyberbullying Affect Kids?

Cyberbullying can include text messages, posts on social media, the spreading of pictures, or other forms of

bullying over technology. Cyberbullying has become a recent phenomenon, as it is increasingly easy for a bully to hide behind their screen of choice and promote hurtful ideas about another person.

How can you help your kids understand how cyberbullying could affect them and also how to prevent it? Use these 5 discussion questions to jumpstart the conversation in your family!

GET THE DISCUSSION QUESTIONS

Who Is Responsible For Data Privacy?

Historically, companies have left it to the IT departments to protect company data and users' sensitive personal information from hacks. After all, data is stored on servers, accessed through networks, and analyzed on computers—and that's technical IT stuff.

Privacy is a team sport, though! Your cybersecurity team should touch every aspect of your business—from your leadership team to marketing to customer service.

A great privacy team will have input from people in multiple roles. This might include:

- Executive Leadership
- Information Technology
- Marketing
- Legal
- Human Resources
- Customer Service

Whether you've already tried to start a data privacy program and failed, your existing program needs updates, or you are a smaller business with a small team, Red Clover Advisors can help you build strong, agile processes that get you where you need to be.

READ MORE

Do privacy regulations have your head spinning? Our team is here to help!

SCHEDULE A CALL

Stay Up to Date on State Privacy Laws

Check out our updated list to stay in the know and stay compliant! View it here.

Check out our Complimentary Resources

Top Cyber Security Tips for Small Businesses, Complete 2021 Privacy Compliance Checklist and More! Download here.

Privacy Terminology Got You All Tongue Tied?

Welcome to the only privacy cheat sheet you'll ever need, download it here!

Daily Updates

Follow Red Clover Advisors for daily privacy and online security updates.

Follow Red Clover Advisors on LinkedIn ➡

Website

Unsubscribe | Update your profile | jodi@redcloveradvisors.com | www.redcloveradvisors.com
4780 Ashford Dunwoody Road, Suite 540 #207, Atlanta, GA 30338

Subject: Techdirt Daily Newsletter for Friday, 21 May, 2021
Date: Friday, May 21, 2021 at 4:26:52 AM Mountain Daylight Time
From: Techdirt Daily Newsletter <newsletters@techdirt.com>
To: Techdirt Daily Newsletter Subscriber <tanidowning@utah.gov>

read it online

Techdirt Email.

Stories from Thursday, May 20th, 2021

Are you interested in receiving a shorter, easy-to-scan, email of post excerpts? Check our our new

Techdirt Daily Newsbrief

Unofficial Amiibo Guidebook That Was Essentially Advertising Nintendo Products Gets Nintendo'd

from the *nintendon't* dept

by Timothy Geigner - May 20th @ 8:10pm

Nintendo really can't help itself. With the company's storied reputation for valuing strict control of all things intellectual property over literally everything else, we have detailed plenty of occasions where this restrictive attitude seems to work directly against the company actually selling things. From DMCAing fan-made ports of Nintendo's games to antiquated game systems, to getting fan-made expressions of Nintendo fandom taken down from 3rd party creation games like *Dreams*, to just DMCA carpet-bombing a wide range of fan-made games that serve as homages to Nintendo properties, the company has made it very clear that it will choose strict control over being good to its fans at every opportunity. Even, as is so often the case, when that means getting content taken down that essentially serves as an advertisement for Nintendo products.

Perhaps this has never been more evident than when Nintendo recently got a Kickstarter project shut down, as that project was for a guidebook to Nintendo Amiibo products.

> *Made by Ninty Media, the unofficial amiibo handbook was designed as a guidebook that catalogued every single amiibo available at the time of the book's release. Not only does this compendium show off every amiibo, it also gives fun facts about each character listed, and even has estimated prices to help those trying to purchase these desired figures today. The Kickstarter for the book launched last month and has long surpassed its initial goal of £3,000 with £36,172 at the time of its being*

taken down.

However, that Kickstarter has now come to a halt thanks to this new dispute from Nintendo. Viewing the copyright notification on the Kickstarter page reveals that it is under dispute due to the use of the amiibo logo on the cover of the book, along with some of Nintendo's other design marks. Paul Murphy, the man behind the amiibo handbook, along with other projects from Ninty Media, has posted on Twitter that he would respond shortly to this claim, demonstrating that the book isn't cancelled yet. But he did offer refunds to anyone who contributed to the Kickstarter in the event that he loses the dispute.

Now, a couple of things I should stipulate right up front. First, Nintendo is well within its rights to take this action. Use of Nintendo's branding and imagery certainly runs afoul of copyright and trademark laws. Second, it was fairly silly of the makers of this book to use that branding and imagery, including font-types, without ever having reached out to Nintendo for any kind of approval. That would be the case if this were a book about the products of "Company X", but when it's Nintendo? C'mon, guys.

So, with those stipulations out of the way, we can now get into just how stupid this all is on Nintendo's part as well. First, again, Nintendo doesn't *have* to spit directly in the faces of its fans.

Given Nintendo's history, it's unsurprising that what have been dubbed by many as the "Nintendo Ninjas" are at it again. Similar to Nintendo's past cases, it's a dispute where Nintendo is legally in the right, but dubious in its morality. The more of these projects Nintendo cancels, the clearer the message that Nintendo is against these types of fan projects. It's not a good message to send to the community, and it harms the relationship Nintendo has with its consumers.

And then let's add to all of that that this book would essentially serve as a giant advertisement for Nintendo's Amiibo products. There are a zillion ways the company could have worked amicably with this Kickstarter project so as to both protect its IP, say with a cheap or free license to use the assets in question, while also ensuring that a book for Amiibo enthusiasts still got released. By all accounts, such possibilities were never even explored by Nintendo.

That's not surprising any longer, but it remains quite disappointing. If we acknowledge that this book generally didn't serve any real threat to the monetary income of Nintendo, and likely would have been a boon instead, there was literally nothing to lose and everything to gain if Nintendo had chosen to be human and cool in this instance.

Instead, it takes a hit on the relationship front with its fans and loses out on the free

advertising for Amiibo products. Great job.

10 Comments »

G7 And Technical Standards: Blink And You Might Have Missed The New Battleground

from the *governments-encroaching* dept

by Konstantinos Komaitis and Dominique Lazanski - May 20th @ 3:42pm

Amid all the news about the third wave of the COVID-19 Pandemic and the politics behind the vaccination roll out, you might have missed the Ministerial Declaration from the G7 Digital and Technology Ministers' meeting. As per tradition, the G7 Digital Ministerial provides the opportunity for the seven richest countries of the world to declare their commitments and vision on the type of digital future they would like to see. The document is non-binding but it has the tendency to provide some useful insights on the way the G7 countries view digital issues and their future positions in multilateral fora; it is also informative of other, more formal, multilateral processes. On 28 April 2021, a statement was made addressing key technology issues and opportunities including security in ICT supply chains, Internet safety, free data flows, electronic transferable records, digital competition and technical standards.

Yes, you read that right - technical standards. In the last several years technical standards have moved from the realm of engineers into wider politics. News stories have been replete with China's efforts to become a competitive force on 5G, AI and facial recognition standards and its wish to be developed internationally based on their national rules, culture and technology. But the public eye turned more closely to China when it was discovered that the facial recognition standards being developed by China in the UN system were from countries on the US sanctions list and used by China for monitoring Uighurs.

None of this is new. For the past few years and for anyone who has been paying attention, China has been strategically positioning itself in various standards bodies realizing that shifting from a unipolar to a multipolar world order cannot happen unless it is capable of demonstrating a more strategic and competitive approach to the domination of the west. What was the tipping point, however, that made the seven richest countries in the world offer explicit language on standards inserted into their declaration? Everything seems to be pointing to the "newIP" standard proposal, recommending a change in the current Internet technology, that was put forward by Huawei and supported by China in the International Telecommunications Union (ITU). Although this new standard did not manage to pass the ITU's study group phase, it did raise the eyebrows of the West. And, rightly so.

Historically, Internet standards have paved their own path and have majorly managed to stay outside of politics. In one of the earliest Requests for Comments (RFC), the

definition of a standard was specific and narrow: a standard is "a specification that is stable and well-understood, is technical competent, has multiple, independent and interoperable implementations with operations experience, enjoys significant public support, and is recognizably useful in some or all parts of the Internet".

Traditionally, governments have had a hands-off approach in the development and deployment of standards related to the Internet; their development was part of the consensus-based, community-driven process developed and nurtured by the Internet Engineering Task Force (IETF) and their deployment was left to the market. A standard's life has always depended on its utility and contribution to the evolution of the Internet.

This seems to be the case less and less. Over the past years, governments have shown increasing interest in the development of standards, and have sought ways to inject themselves into Internet standardization processes. There are two distinct ways that this trend has emerged. First, there's China, which actively seeks to displace the current Internet infrastructure. That was clear in the attempt with the "newIP" proposal. China has been strategic in not directly suggesting a complete rejection of the Internet model; instead, its claims have been that the Internet cannot meet future technologies and needs and, therefore, a new infrastructure, developed and nurtured by governments, is necessary. The second trend continues to support the open, market-driven standards development processes, but seeks ways for governments to be more actively involved. This, so far, has mainly been interpreted as identifying ways to provide incentives for the creation and deployment of certain standards, often those deemed strategically important.

Even though these approaches reflect different political and governance dimensions - China supports a top-down approach over the West's bottom-up model - they do share one commonality: in both cases, politics are becoming part of the standardization process. This is entirely unlike the past 30 years of Internet development.

This could have significant implications in the development and future of the Internet. There are benefits from the current structure: efficiency, agility and collaboration. The existing process ensures quick responses to problems. But, its main advantage is really the collective understanding that standards are driven by what is "good for the Internet"; that is, what is required for the Internet's stability, resilience and integrity.

This doesn't mean that this process is perfect. Of course, it comes with its own limitations and challenges. But, even then, it is a tested process that has worked well for the Internet throughout most of its existence. It has worked - despite its flaws - because it has managed to keep political and cultural dimensions separate. Participants, irrespective of background, language, and political persuasion have been collaborating successfully by having **the Internet** and what's good for **it**, as their main objective.

On the contrary, intergovernmental standards are driven by political differences and political motives. They are designed this way. This is not to say that governments

should not be paying attention to the way standards are developed. But, it is crucial to do so in ways that do not seek to upend a model that is tested and responsive to the needs of the Internet.

Dr. Konstantinos Komaitis is the Senior Director, Policy Strategy and Development at the Internet Society.

Dominique Lazanski is the Director of Last Press Label, and a Consultant in International Internet and Cybersecurity Standards and Policy.

2 Comments »

Redditors Launch A 'Rescue Mission' For Embattled Sci-Hub, With The Ultimate Aim Of Building A Decentralized Version

from the *but-what-about-protecting-Elbakyan?* dept

by Glyn Moody - May 20th @ 1:53pm

Techdirt has just written about belated news that the FBI gained access two years ago to the Apple account of Alexandra Elbakyan, the founder of Sci-Hub. This is part of a continuing attempt to stop the widespread sharing of academic papers, mostly paid for by the public, and currently trapped behind expensive paywalls. You might think somebody helping scholars spread their work to a wider audience would be rewarded with prizes and grants, not pursued by the FBI and DOJ. But of course not, because, well, copyright. It's easy to feel angry but helpless when confronted with this kind of bullying by publishing giants like Elsevier, but a group of publicly spirited Redditors aim to do something about it:

> *It's time we sent Elsevier and the USDOJ a clearer message about the fate of Sci-Hub and open science: we are the library, we do not get silenced, we do not shut down our computers, and we are many.*

They have initiated what they term a "Rescue Mission for Sci-Hub", in order to prepare for a possible shutdown of the site:

> *A handful of Library Genesis seeders are currently seeding the Sci-Hub torrents. There are 850 scihub torrents, each containing 100,000 scientific articles, to a total of 85 million scientific articles: 77TB. This is the complete Sci-Hub database. We need to protect this.*

The Redditors are calling for "85 datahoarders to store and seed 1TB of articles each, 10 torrents in total". The idea is to download 10 random torrents, then seed them for as long as possible. Once enough people start downloading random torrents using

these seeds, the Sci-Hub holdings will be safe. That would then lead to the "final wave":

> *Development for an open source Sci-Hub. freereadorg/awesome-libgen is a collection of open source achievements based on the Sci-Hub and Library Genesis databases. Open source de-centralization of Sci-Hub is the ultimate goal here, and this begins with the data, but it is going to take years of developer sweat to carry these libraries into the future.*

The centralized nature of Sci-Hub is certainly its greatest weakness, since it provides publishers with just a few targets to aim for, both legally and technically. A truly decentralized version would solve that problem, but requires a lot of work, as the Reddit post notes. Still, at least this "rescue plan" means people can do something practical to help Sci-Hub; sadly, protecting Elbakyan is harder.

Follow me @glynmoody on Twitter, Diaspora, or Mastodon.

2 Comments »

Violent, Bigoted Cop Accused Of Beating Another Cop Is Upset His Text Messages Expose Him As A Violent Bigot

from the *petard-toting-mfers-getting-themselves-hoisted* dept

by Tim Cushing - May 20th @ 12:06pm

Lawyers for a cop accused of beating an undercover cop during a 2017 protest are pretty angry prosecutors have let the public know just what kind of bigoted dirtbag the indicted officer is.

St. Louis police officer Dustin Boone -- along with four other officers -- attacked undercover officer Luther Hall. Boone is white. Detective Hall is black. This is relevant information, even if Boone's lawyers are claiming his texts -- which contain plenty of bigotry -- aren't. Boone's legal rep is seeking to have prosecutors sanctioned for bringing Boone's texts to his prosecution.

> *Boone's attorney, Patrick Kilgore, argues in a court filing that the now-public information is "inflammatory, irrelevant, and highly prejudicial" and disclosing them violates a judge's order to file much of the information under seal. He notes that the St. Louis Post-Dispatch wrote about the texts and other information from the prosecutors' filing and claims it could taint the jury pool and keep Boone from receiving a fair trial.*

They're definitely "inflammatory." How could they not be? These are former officer

Boone's own words. And they seem relevant as they make it pretty clear how easily a bigot like Boone could "mistake" a black undercover officer for a protester in need of a beating. Here's Boone in a group text [PDF] to other St. Louis police officers a few months prior to the beating he's now facing charges for:

> *It's already a state of emergency! There are r niggers running wild all across the city and even if/when we catch them..... they don't get in any trouble because there are plate lips running the CAO!*

Here's what the CAO reference means:

> *CAO is apparently a reference to the St. Louis Circuit Attorney's Office, which is under the supervision of the city's first Black circuit attorney, Kim Gardner.*

That's not the only one containing the n-word. This term was used in a group text to "Kayla, Kelsea, Mom, Ashley Marie, Dad" that reads:

> *What city r we in?*
>
> *These fuckin niggers r the same as St. Louis niggers.*

So, the lawyer for this lovely person wants these texts tossed and prosecutors sanctioned for introducing "highly prejudicial" information. And, to be fair, it will certainly make jurors feel things about Boone that they likely wouldn't have felt without them. But is it too unfair? It certainly seems relevant -- not just because of how Boone apparently views black people, but because it also shows how gleefully he participated in the beating of a fellow officer.

> *Prosecutors say that Boone hooked his phone on his uniform and livestreamed Hall's beating for Ditto. The hour-long video wasn't saved, but prosecutors say Ditto's messages back and forth with Boone prove that she watched what happened — and that Boone was involved. Afterward, Ditto wrote "That was SOOOOOO COOL!!!!"*

Perhaps the most memorable part of this exchange (other than Boone's sudden contrition after the news came out he had beaten an undercover detective) is his girlfriend's response to the beating. Everyone tells you "just comply" with cops' orders if you don't want to get hurt. Here's a civilian take, and it's a good one considering it's from someone who was in a personal relationship with a cop:

> *But damn you guys need to practice more. Even I was confused. One guy was sayin HANDS DOWN, HANDS DOWN.*

Next dude saying HANDS UP.

Then HANDS DOWN, HANDS DOWN, GET YOUR FUCKIN HANDS UP.

And that's not the end of the disturbing communications. There are multiple texts celebrating excessive force use -- including Boone's efforts to ensure these beatings weren't captured by nearby CCTV cameras or bystanders. There's a text suggesting Boone stole money from a crime scene. There's a whole string of texts detailing he and his fellow officers' abuse of prescription drugs like Adderall and Concerta.

Here's his recommendation to fellow officer Kyle Santa who was asking on behalf of another police officer.

> *Depends on if he wants to feel like he feels like seeing in HD and making night turn into day (adderall) or if he just wants to feel a really really focused white guy (concerta). Adderall is essentially cocaine base in a compressed pill form..... It's pretty special. It makes u chew on ur tongue and like ur lips like a crack head and u can't stop talking for the first 8 hours. It is also nearly impossible to get drunk AND cures hangovers in a matter of 11 minutes.*

Sure, I can see why Boone's lawyer wants these messages kept out of court. They make his client look like a violent, racist drug addict. That's certainly not going to help -- not when his lawyer is trying to clear him of charges related to the violent beating of a black man... one that Boone seemingly would never have regretted if the beating victim hadn't turned out to be a fellow officer.

Even if Boone's lawyer manages to get these texts tossed and the prosecutors sanctioned, they'll hopefully be enough to prevent Dustin Boone from ever wearing a badge again. And it should serve as a wakeup call for all the officers he worked with -- the ones who ignored his violence, racism, and drug abuse until he made the only unforgiveable mistake: beating up another cop.

Read More | 15 Comments »

Parler Was Allowed Back In The Apple App Store Because It Will Block 'Hate Speech,' But Only When Viewed Through Apple Devices

from the *fracturing* dept

by Mike Masnick - May 20th @ 10:43am

Last month we noted that Apple told Congress that it was allowing Parler's iOS app to return to its app store, after the company (apparently) implemented a content

moderation system. This was despite Parler's then interim CEO (who has since been replaced by another CEO) insisting that Parler would not remove "content that attacks someone based on race, sex, sexual orientation or religion." According to a deep dive by the Washington Post, the compromise solution is that such content will be default blocked **only** on iOS devices, but will be available via the web or the sideloaded Google app, though they will be "labeled" as hate by Parler's new content moderation partner, Hive.

> *Posts that are labeled "hate" by Parler's new artificial intelligence moderation system won't be visible on iPhones or iPads. There's a different standard for people who look at Parler on other smartphones or on the Web: They will be able to see posts marked as "hate," which includes racial slurs, by clicking through to see them.*

Hive is well known in the content moderation space, as it is used by Chatroulette, Reddit and some others. Hive mixes "AI" with a large team of what it refers to as "registered contributors" (think Mechanical Turk-style crowdsourced gig work). Of course, it was only just last year that the company announced that its "hate model" AI was ready for prime time, and I do wonder how effective it is.

Either way, this *is* interesting for a variety of reasons. One thing we've talked about in the past with regards to content moderation is that one of the many problems is that different people have different tolerances for different kinds of speech, and having different moderation setups for different users (and really pushing more of the decision making to the end users themselves) seems like an idea that should get a lot more attention. Here, though, we have a third party -- Apple -- stepping in and doing that deciding for the users. It is Apple's platform, so of course, they do get to make that decision, but it's a trend worth watching.

I do wonder if we'll start to see more pressure from such third parties to moderate in different ways to the point that our mobile app experiences and our browser experiences may be entirely different. I see how we end up in such a world, but it seems like a better solution might be just pushing more of that control to the end users themselves to make those decisions.

The specific setup here for Parler is still interesting:

> *Parler sets the guidelines on what Hive looks for. For example, all content that the algorithms flag as "incitement," or illegal content threatening physical violence, is removed for all users, Peikoff and Guo said. That includes threats of violence against immigrants wanting to cross the border or politicians.*
>
> *But Parler had to compromise on hate speech, Peikoff said. Those using iPhones won't see anything deemed to be in that category. The default*

> *setting on Android devices and the website shows labels warning "trolling content detected," with the option to "show content anyway." Users have the option to change the setting and, like iOS users, never be exposed to posts flagged as hate.*
>
> *Peikoff said the "hate" flag from the AI review will cue two different experiences for users, depending on the platform they use. Parler's tech team is continuing to run tests on the dual paths to make sure each runs consistently as intended.*

Of course, AI moderation is famously mistake-prone. And both Parler and Hive execs recognize this:

> *Peikoff said Hive recently flagged for nudity her favorite art piece, the "To Mennesker" naked figures sculpture by Danish artist Stephan Sinding, when she posted it. The image was immediately covered with a splash screen indicating it was unsafe.*
>
> *"Even the best AI moderation has some error rate," Guo said. He said the company's models show that one to two posts out of every 10,000 viewed by the AI should have been caught on Parler but aren't.*

I do question those percentages, but either way it's another interesting example of how content moderation continues to evolve -- even if Parler's users are angry that they won't be able to spew bigotry quite as easily as previously.

34 Comments »

Daily Deal: The Complete Become A UI/UX Designer Bundle

from the *good-deals-on-cool-stuff* dept

by Daily Deal - May 20th @ 10:38am

The Complete Become a UI/UX Designer Bundle has 9 courses UI/UX design, sales funnels, and business development. You'll learn about the phases of web development, the UX design process, different UI design types, and more. You'll also learn about freelancing, starting your own business, and how to create highly profitable sales funnels. It's on sale for $35.

source: imgur.com

Note: The Techdirt Deals Store is powered and curated by StackCommerce. A portion of all sales from Techdirt Deals helps support Techdirt. The products featured do not

reflect endorsements by our editorial team.

Comment »

Senator Wyden Tells The DOJ It Needs To Stop Going After Journalists During Leak Investigations

from the *if-they-aren't-a-target,-don't-target-them* dept

by Tim Cushing - May 20th @ 9:36am

Earlier this month, it was revealed the DOJ -- while headed by Bill Barr and an extraordinarily leaky White House -- decided it would be cool and constitutional to demand journalists' phone and email records while supposedly investigating leaks pertaining to Trump's first impeachment.

The DOJ apparently did manage to get the phone records. For whatever reason, it never bothered to collect the email metadata, despite having obtained a court order to do so. Nearly four years after this occurred, the Washington Post journalists were finally notified about the government's interest in their communications.

The Justice Department's statement was less than satisfactory. It claimed that this sort of First Amendment-troubling activity was "rare" and that it followed all of its internal guidelines when targeting journalists' communications. It also claimed it was ok because the journalists weren't the target of the investigation. All the DOJ wanted were their *sources*.

That's not ok no matter what internal guidelines are followed. If the DOJ has a leak to investigate, it needs to confine itself to the end doing the leaking, not the recipients of the leaks. Just because it might be easier for investigators to work their way backwards from journalists' communications to identify the source of leaks doesn't make it acceptable. The ends don't justify the means -- not when the means wander across the constitutional lines.

Now the DOJ has (yet again) angered Senator Ron Wyden. Wyden has sent a letter [PDF] to Attorney General Merrick Garland, demanding he revamp the internal rules to make this sort of thing far less likely to reoccur. Wyden is also asking for full reports on any surveillance of journalists the DOJ engaged in over the last couple of years.

As Wyden points out, using subpoenas and court orders to sniff out journalists' sources may be less disruptive than subjecting them to the justice system, but the end result is the same breach of trust and Constitutional protections.

> *In years past, the government would often attempt to force journalists to reveal their sources, by dragging them into court, where many chose to spend time in jail for contempt of court, rather than violate their oath to keep their sources' identities hidden. Now that most Americans*

> *carry always-on, always-recording smartphones, the government prefers to go to telecommunications companies, hoping that records of calls and texts might reveal the source. While certainly more convenient for the government, using subpoenas and surveillance orders to pry into a journalist' communications history is no less invasive and destructive than forcing a journalist to reveal their source.*

From there, Wyden goes on to note he's working to introduce stronger protections for journalists. And with that in mind, he asks the new Attorney General to start repairing some of the damage done by the previous administration.

> *[T]he Biden Administration has the opportunity to voluntarily leave behind the thuggish and Orwellian abuses of power of the last administration, and stand up as a world leader for press freedoms. [...]* ***Simply put, the government should not collect journalists' communications records unless it's investigating them for a crime or as part of an investigation into foreign espionage, in which case it should get a warrant.***

That's far more restrictive than the DOJ's current standards, which seem pretty low for something with the word "justice" in it that operates in a nation that has held itself out to be the standard-bearer for personal freedoms. Hopefully, AG Garland will decide it's time for the DOJ to respect the rights all government employees swear to uphold.

Read More | 6 Comments »

As The US Press Withers, Glorified Marketing Aims To Take Its Place

from the *not-helping* dept

by Karl Bode - May 20th @ 6:28am

More than 16,000 journalists and editors were laid off last year, a tally that excludes broader media jobs and freelancers. While COVID certainly played a role (read: advertisers not wanting the brands to appear in ads next to stories telling people the truth about a pandemic), the layoffs were part of a broader trend in which the unprofitable business of delivering the factual reality (usually) continues to wither on the vine.

Mindless media consolidation has created vast news deserts where local news of any quality literally no longer exist. Incompetent but wealthy new media CEOs, free from anything vaguely resembling accountability, fire their entire newsrooms on a dime at the slightest hint of unionization, a threat that wouldn't be so pronounced if we'd

managed to pay reporters a living wage. The US press feels broken, a consensus on how to fix it remains elusive, and bad ideas seem to outnumber good ones by a wide margin.

Into that vacuum has stumbled all manner of terrible beasts, ranging from phony "pink slime" local news, a steady parade of foreign and domestic propaganda artists, and consolidated broadcasters for which truth is a distant afterthought. Just this week, OAN, a "news" channel found on most mainstream cable lineups and pumped into millions of American homes, not only trumpeted the bogus election "audit" in Arizona, it was happily fundraising off of it with zero repercussions whatsoever:

> *"What's more, one of those reporters, Christina Bobb, is the network's most visible correspondent covering the very "audit" that she is helping scare up money for on OAN's airwaves, while she and the network enjoy unique access to the process where private contractors and volunteers are searching for fraud and have examined ballots for nonexistent watermarks and "bamboo fibers." OAN has a deal as the exclusive livestream partner for the audit."*

At the same time, wealthy individuals and organizations also have an eye on using their vast fortunes to reshape the news industry in their interests. Silicon Valley venture capital giants like a16z have begun building their own news empires to counter what they believe are overly critical media narratives (aka the truth about things like environmental harms, unfair labor practices, and anti-competitive shenanigans). And this week, cryptocurrency giant Coinbase announced it too would be building a new media arm. With a notable caveat:

> *"Unlike a typical newsroom, that person would report into Coinbase's marketing team."*

Granted it's not entirely impossible Coinbase could build a quality news operation, though past efforts like this traditionally haven't gone that well. Without an adequate firewall between marketing and news, you wind up with bungled experiments like Verizon's short-lived Sugarstring news venture, which quickly collapsed after the journalists they hired were banned from writing about issues Verizon clearly had a stake in (most notably, surveillance and net neutrality).

Not too surprisingly, Coinbase's jump into news was met with the sort of skepticism you'd expect:

> "Unlike a typical newsroom, that person would report into Coinbase's marketing team."
>
> Ok. So not a media arm, a corporate propaganda arm.
> https://t.co/hPoxB5YOqi

— Aram Zucker-Scharff (@Chronotope) May 19, 2021

[Click to view this post on Techdirt with embedded content.]

I spent much of February talking to as many media scholars as I could for a piece on how we fix the country's news and disinformation crisis, and found there's still nothing even close to a consensus on how to proceed. There's not even a real sense among many academics that there's a serious problem taking root. Policy and legislative solutions, many admittedly terrible (fairness doctrine 2.0!), will never survive free speech concerns or a rightward-lurching court system. There's some scattered suggestions (forcing a la carte cable to reduce revenue to dodgy channels like OAN, require more transparency in ads), but nothing that comes close to comprehensive.

That leaves finding ways to creatively-fund and amplify trustworthy news outlets, something that's not really happening at any scale either. Often, it feels like we've found creative ways to fund everything but journalism. White supremacist chat rooms? Check. Hot tub influencers? Sure! Meme-based joke cryptocurrencies? Why not! Gamers watching gamers watching gamers? Of course! Ridiculously speculative blockchain-based art? Yep! Journalism, a purported cornerstone of democracy? Meh. Education? Whatevs.

Instead, the journalism industry seems content to pat itself on the back for reinventing the newsletter for the umpteenth time, as genuine journalism and expertise slowly gets swallowed in a sea of COVID-denying influencers, bullshit-artists, billionaire ego projects, trolling Substack opinion writers, timid "view from nowhere" journalism, and just rank political and corporate disinformation. There's surely a path out from the current US information apocalypse, but it's anything but obvious what it looks like at the moment.

32 Comments »

Defense Department Is Buying Domestic Internet Metadata From Data Brokers

from the *bringing-the-war-back-home-via-bulk-purchases* dept

by Tim Cushing - May 20th @ 3:28am

Joseph Cox broke the news for Motherboard late last year: the US military was *also* making use of location data purchased from data brokers, joining a host of other federal agencies that seemed to feel buying from brokers was an acceptable alternative to respecting the Fourth Amendment.

Of particular interest to the Defense Department was location data generated by apps popular with the world's Muslims, including the Muslim Pro prayer app and Muslim Mingle, a Muslim-centric Tinder. The DoD didn't have much to say in its... um... defense

at that time, obviously preferring everyone to assume the focus on Muslim-focused apps was indicative of its good and righteous work fighting terrorist organizations around the world.

Unfortunately, the data came from brokers who also collect plenty of location info from US located app users and there was no information provided by the government that showed the military made an effort to steer clear of acquiring this data.

More confirmation has arrived, via some half-answers, redactions, and "can we talk about this in private?" responses to Senator Ron Wyden's demand for more information from the Defense Department. Once again, it's Joseph Cox and Motherboard bringing us the latest:

> *The Pentagon is carrying out warrantless surveillance of Americans, according to a new letter written by Senator Ron Wyden and obtained by Motherboard.*
>
> *Senator Wyden's office asked the Department of Defense (DoD), which includes various military and intelligence agencies such as the National Security Agency (NSA) and the Defense Intelligence Agency (DIA), for detailed information about its data purchasing practices after Motherboard revealed special forces were buying location data. The responses also touched on military or intelligence use of internet browsing and other types of data, and prompted Wyden to demand more answers specifically about warrantless spying on American citizens.*

Unfortunately, further details have yet to be released. For the moment, Senator Wyden is indulging the Pentagon's demands for further secrecy. But his letter lets the public know some of what he knows -- even if the Defense Department has refused to make this information public.

> *"I write to urge you to release to the public information about the Department of Defense's (DoD) warrantless surveillance of Americans," the letter, addressed to Secretary of Defense Lloyd J. Austin III, reads.*

The DoD may not have publicly admitted to this surveillance of Americans but Wyden is willing to make that disclosure on its behalf.

According to Wyden staffers, this refers to the DoD's bulk purchases of internet metadata that contain information about US persons' communications. Some of these are wholly domestic conversations. Some involve communications between Americans and people located in other countries. In either case, the DoD appears to be bypassing protections erected to prevent this sort of bulk surveillance. And while components of the Defense Department are in the intelligence business, their adversaries and targets are supposed to be foreigners. Incidental collection is one thing. Buying data in bulk

and sifting through it with zero oversight is quite another.

6 Comments »

Visit Techdirt for today's stories.

Subscription Reminder

You're Subscribed to: Techdirt Daily Newsletter using the address:
tanidowning@utah.gov

Manage Your Subscription

Unsubscribe Automatically

Contact

newsletters@techdirt.com
Floor64, Inc.
370 Convention Way
Redwood City, CA 94063

Connect

Facebook

Twitter

Subject: Today's Headlines: Belarus Forces Down Plane to Seize Dissident; Europe Sees 'State Hijacking'
Date: Monday, May 24, 2021 at 2:01:01 AM Mountain Daylight Time
From: The New York Times <nytdirect@nytimes.com>
To: tanidowning@utah.gov <tanidowning@utah.gov>

The New York Times

Monday, May 24, 2021

Top News

Belarus Forces Down Plane to Seize Dissident; Europe Sees 'State Hijacking'

By Anton Troianovski and Ivan Nechepurenko

The dissident, Roman Protasevich, co-founded a Telegram channel that is a popular opposition outlet in Belarus. The plane was flying from Athens to Lithuania when it was forced down.

Before Rage Flared, a Push to Make Israel's Mixed Towns More Jewish

By Isabel Kershner

An eruption of Arab-Jewish violence inside Israeli cities has focused attention on a movement of religious nationalists seeking to strengthen the Jewish presence in areas with large Arab populations.

A Year After George Floyd: Pressure to Add Police Amid Rising Crime

By Tim Arango

Los Angeles, like other cities across the nation, is facing a rise in gun violence. And the police budget is growing.

For more top news, go to **NYTimes.com »**

Editors' Picks

HEALTH

These Sisters With Sickle Cell Had Devastating, and Preventable, Strokes

By Gina Kolata and Ilana Panich-Linsman

Kyra and Kami never got a simple test that could have protected them. Their story exemplifies the failure to care for people with the disease, most of whom are Black.

OPINION | THOMAS L. FRIEDMAN

How Joe Biden Can Win a Nobel Peace Prize

By Thomas L. Friedman

The latest Israel-Palestinian conflict could result in a peace deal — if the Americans are willing to broker it.

Today's Videos

Video VIDEO: At Least 14 People Killed After Cable Car Plummets in Italy

By Reuters and Storyful

A cable car plunged from a height of nearly 40 feet as it was traveling from the Lake Maggiore area to Mottarone mountain in northern Italy on Sunday.

Video VIDEO: Lava Recedes After Volcanic Eruption in Congo

By The New York Times

People returned to areas in the eastern Democratic Republic of Congo on Sunday that were threatened by an eruption from Mount Nyiragongo. Thousands had been forced to evacuate nearby neighborhoods overnight.

Video VIDEO: Biden Expresses Deep Concern Over North Korea's Nuclear Program

By The Associated Press

Standing next to the leader of South Korea at the White House on Friday, President Biden said he was "deeply concerned" about the nuclear threat from North Korea and said he wouldn't repeat the mistakes of past administrations.

World

Iran, a Longtime Backer of Hamas, Cheers Attacks on Israel

By Farnaz Fassihi

Tehran jumped at the chance to portray militants' barrages on Israel as revenge for Israeli attacks on Iran. But Israel says Tehran played no role in the latest conflict.

As India Stumbles, One State Charts Its Own Covid Course

By Shalini Venugopal Bhagat

Kerala uses tracking of patients and supplies, a network of health care workers and coronavirus "war rooms" to succeed where the national government has fallen short.

21 Runners Dead After Extreme Weather Hits Chinese Ultramarathon

By Alexandra Stevenson and Cao Li

The 62-mile mountain race in Gansu Province left athletes in shorts and T-shirts facing freezing rain, hail and high winds.

For more world news, go to **NYTimes.com/World »**

U.S.

A Family Sought Revenge Against a Tormentor. They Shot the Wrong Man, Police Say.

By Maria Cramer

Members of a family in Texas who were being harassed have been charged with murder in what a sheriff called "a tragic case of mistaken" identity.

No, People Are Not Returning Pandemic Dogs in Droves

By Michael Levenson

Despite alarmist headlines, the happy truth is most people are keeping their newly adopted pets, animal welfare groups say.

They Haven't Gone for a Shot. So Shots Are Coming to Them.

By Christine Hauser and Ruth Fremson

Mobile Covid-19 vaccine clinics in vans and buses are rolling up to neighborhoods in Delaware, Minnesota and Washington State to reach people who have been unable to travel to vaccination centers.

For more U.S. news, go to **NYTimes.com/US »**

Politics

Why Arkansas Is a Test Case for a Post-Trump Republican Party

By Jonathan Martin

Sarah Huckabee Sanders seems likely to bring the Trump brand to Arkansas politics in a big way. But the state is a testing ground for different possible futures for the party.

It's Crunch Time and Biden's Climate Gambit Faces Steep Hurdles

By Lisa Friedman

He wants to require power companies to replace fossil fuels with clean energy. It's a broadly popular idea but its path in Congress is perilous.

U.S. Grants Temporary Protections to Thousands of Haitians

By Eileen Sullivan

The designation, which will be in place for 18 months, could protect as many as 150,000 Haitians living temporarily in the United States.

For more political news, go to **NYTimes.com/Politics »**

Business

'We Always Rise.' A Black-Owned Bookstore Navigates the Pandemic

By Kevin Armstrong

Source of Knowledge has been a Newark mainstay for decades. It survived the past year thanks to the generosity of its customers and an owner who provides more than just books.

WHEELS

A 1960 Corvette That Vanished for 40 Years After Le Mans Is Auctioned Off

By Jerry Garrett

Since its chance rediscovery in 2011, the heavily altered racecar has been the subject of seemingly endless legal twists and turns and acrimonious confrontations.

WORK FRIEND

Look, Just Keep Filling the Chocolate Dish

By Roxane Gay

A reminder to mind your own business and know your worth.

For more business news, go to **NYTimes.com/Business »**

Technology

Daimler's Truck Unit Maps Plans to Replace Diesel With Hydrogen

By Jack Ewing

Electric cars get all the attention, but truckmakers are also under pressure to shift from fossil fuels to electricity.

Shoshana Zuboff Explains Why You Should Care About Privacy

By Lauren Jackson

In a wide-ranging interview, the author of "The Age of Surveillance Capitalism" talks about why people should pay attention to how big tech companies are using their information.

Founder of TikTok's Parent Company Will Step Down as C.E.O.

By Raymond Zhong

Zhang Yiming steered ByteDance to become China's first truly globally successful internet company.

For more technology news, go to **NYTimes.com/Technology »**

Sports

Phil Mickelson, at 50, Wins P.G.A. Championship

By Bill Pennington

Mickelson became the oldest winner of a major golf tournament after a tense final round on the treacherous Ocean Course at Kiawah Island.

N.B.A. PLAYOFF PREVIEW

The Phoenix Suns Are Chris Paul's Latest Project

By Scott Cacciola

Paul is pulled in many directions — acting, training, arguing with referees — but now he has his eyes set on winning a championship with the Suns.

ON PRO BASKETBALL

The Nets' Starters Are Back Together. And So Are the Fans.

By Jonathan Abrams

Over 14,000 fans attended Game 1 of the Nets-Celtics series as Kevin Durant, Kyrie Irving, James Harden, Blake Griffin and Joe Harris started together for the first time this season.

For more sports news, go to **NYTimes.com/Sports »**

Arts

Eurovision, Celebrating the Sounds of a Postpandemic Continent

By Thomas Erdbrink

A dancing finger, chained demons and a victory for Italian rockers. But Eurovision, the largest music contest in the world, is more than just weird.

Her Book Doesn't Go Easy on Publishing. Publishers Ate It Up.

By Elizabeth A. Harris

Zakiya Dalila Harris, a former editorial assistant, is making a splash with "The Other Black Girl," her debut novel about an African-American woman navigating a nearly all-white workplace.

CRITIC'S PICK

Allow Olivia Rodrigo to Introduce Herselves

By Jon Caramanica

On her excellent debut album, "Sour," the 18-year-old singer and actress expresses just how challenging it is to arrive at who you are.

For more arts news, go to **NYTimes.com/Arts** »

New York

Yes, Pot Is Legal. But It's Also in Short Supply.

By Tracey Tully

Cannabis corporations are rushing to meet what is expected to be a "tidal wave" of demand in New York and New Jersey.

2 Dead and 12 Wounded in House Party Shooting in New Jersey, Police Say

By Marie Fazio and Tracey Tully

The New Jersey State Police responded to reports of a shooting in Fairfield Township late on Saturday night.

Candidates Escalate Attacks as Mayoral Race Enters Final Month

By Katie Glueck

With less than a month before the June 22 primary, Democratic candidates are trying to steal momentum from the perceived front-runners, Eric Adams and Andrew Yang.

For more New York news, go to **NYTimes.com/NewYork** »

Media & Advertising

It's the Media's 'Mean-Too' Moment. Stop Yelling and Go to Human Resources.

By Ben Smith

In public radio, there is either an epidemic of bullying or an epidemic of whining, depending on whom you ask.

Scrounging for Hits, Hollywood Goes Back to the Video Game Well

By Brooks Barnes

After decades of game-to-film flops, a new effort, led by Sony, aims to adapt big PlayStation and Xbox franchises for movies and TV.

The Youth Prepare for #Summer2021, a Glorious Summer They're Unlikely to Get

By Sophie Haigney

After a traumatic year, it's hard to simply flip a switch toward fun. But have teenage summers ever lived up to expectations?

For more media & advertising news, go to **NYTimes.com/Media »**

Science

There's a New Definition of 'Normal' for Weather

By Henry Fountain and Jason Kao

New baseline data for temperature, rain, snow and other weather events reveal how the climate has changed in the United States.

What Can and Can't Be Learned From a Doctor in China Who Pioneered Masks

By Wudan Yan

Dr. Wu Lien-Teh helped change the course of a plague epidemic in the early 20th century and promoted the use of masks as a public health tool.

It Might Be Time to Break Up Your Pandemic Pod

By Jancee Dunn

Yes, you really need to start seeing other people.

For more science news, go to **NYTimes.com/Science »**

Obituaries

Yuan Longping, Plant Scientist Who Helped Curb Famine, Dies at 90

By Keith Bradsher and Chris Buckley

His development of high-yield rice hybrids in the 1970s led to steeply rising harvests in Asia and Africa and made him a national hero in China, credited with saving countless lives.

Paul J. Hanly Jr., Top Litigator in Opioid Cases, Dies at 70

By Katharine Q. Seelye

Mr. Hanly had been central to the current nationwide litigation against pharmaceutical companies, pharmacies and others in the opioid supply chain.

Mark Levitan, Who Measured the True Face of Poverty, Dies at 73

By Sam Roberts

He came up with a more realistic threshold, changing the way New York City determines who is impoverished and persuading the Obama White House to follow suit.

Roger Hawkins, Drummer Heard on Numerous Hits, Is Dead at 75

By Bill Friskics-Warren

An innately soulful musician, he recorded with Aretha Franklin, Wilson Pickett and many others and was an architect of what became known as the Muscle Shoals sound.

For more Obituaries, go to **NYTimes.com/Obituaries »**

Opinion

MICHELLE COTTLE

Hail Kevin McCarthy, People Pleaser and Trump Appeaser

By Michelle Cottle

Kevin McCarthy will do anything to be speaker of the House.

CHARLES M. BLOW

White Troopers Policing Black Bodies

By Charles M. Blow

The officers involved in Ronald Greene's death aren't just a few bad apples. It is the whole tree that is shading the truth.

For more Opinion, go to **NYTimes.com/Opinion »**

Subject: Techdirt Daily Newsletter for Thursday, 27 May, 2021
Date: Thursday, May 27, 2021 at 4:31:41 AM Mountain Daylight Time
From: Techdirt Daily Newsletter <newsletters@techdirt.com>
To: Techdirt Daily Newsletter Subscriber <tanidowning@utah.gov>

Techdirt Email.

Stories from Wednesday, May 26th, 2021

Warner Bros. Bullies Airbnb Hobbit-Themed Offering Into Changing Its Name Over 'Hobbit' Trademark

from the *napoleon-complex* dept

by Timothy Geigner - May 26th @ 7:56pm

We've covered intellectual property issues that revolve around Tolkien's *Lord of the Rings* properties before. By now, everyone should know that any use of or homage to those properties, or even coincidental usage, will typically result in angry letters from lawyers. What's even more fun about all of that is you get to play the game called, "Whose lawyers are going to write the angry letter this time?" Between the Tolkien estate and its IP management partners and Warner Bros., the studio behind the *LotR* films, they have managed to block an unrelated wine business from using the word "hobbit," bullied a pub named "The Hobbit" to get it to change its name before recanting said bullying, and got a Kickstarter project shut down for trying to create a real-world "Hobbit house."

This is where it's worth reminding everyone that Tolkien did *not* come up with the word "hobbit". That word already existed, though it meant something different than how Tolkien used it to name his race of diminutive folk. The Kickstarter example above is apropos to this post specifically, as it seems that Warner Bros. is at it again, having forced an Airbnb listing clearly designed to be another homage to Tolkien's hobbit homes in the Shire to change its name.

> *The Okanagan homage to middle earth that doubles as a popular Airbnb spot officially has a new name. It's now the Second Breakfast Hideaway.*
>
> *"And the h***** mountain hole is now a Second Breakfast Hideaway (I'm still full from the first one)," the AirBNB owners wrote in a May 22 post.*

> *The popular Airbnb named for its likeness to the housing in J. R. R. Tolkien's Lord of Rings books went on the hunt for a new name following a threat from Warner Bros. which owns the trademark to the word hobbit. Christine Le Combe and her husband purchased the Halfling Hideaway, located roughly 30 minutes east of Osoyoos, last year and renamed it the Hobbit Mountain Hideaway. It's been a popular vacation destination since it opened in 2019. Earlier this week, Le Combe was contacted by entertainment media company Warner Bros. and was told the word "hobbit" is trademarked and they asked her to take down the listing.*

Unfortunately, the source post doesn't bother to interrogate whether the takedown request from Warner Bros. is remotely valid. I would very much argue that it is not, considering that Warner Bros. use of the term "hobbit" is solely focused on movies and movie merchandise, both of which are a far cry from the hospitality and rental business. But Warner Bros. also has deep pockets and the folks behind this Airbnb listing likely do not, which is why trademark bullying works. The threat of Warner Bros. taking this far enough for it to see the inside of the courtroom is almost certainly an extinction level scenario for the former Hobbit Mountain Hideaway.

So, instead, a movie studio gets a rental property to change its name. And that sucks, no matter how positive the victims of this bullying want to be.

> *"Having to get out of my comfort zone and engage with the community has been a good experience," Le Combe said.*
>
> *"I really didn't think that somebody would copyright the word hobbit and then try to hunt a person down if they use the word hobbit because it's not like I meant any harm. The hobbit house is an homage to the favourite book series of a lot of people."*

It's almost as though at Warner Bros. there is some sort of all-seeing eye that scours the physical and digital worlds for any use of the term "hobbit", all in an effort to track and strike down those that would use it. If only there were some usable analogy I could reference for that without getting sued...

4 Comments »

Content Moderation Case Studies: Twitter Clarifies Hacked Material Policy After Hunter Biden Controversy (2020)

from the *clarification-needed* dept

by Copia Institute - May 26th @ 3:38pm

Summary: Three weeks before the presidential election, the New York Post published an article that supposedly detailed meetings Hunter Biden (son of presidential candidate Joe Biden) had with a Ukrainian energy firm several months before the then-Vice President allegedly pressured Ukraine government officials to fire a prosecutor investigating the company.

The "smoking gun" -- albeit one of very dubious provenance -- provided ammo for Biden opponents, who saw this as evidence of Biden family corruption. The news quickly spread across Twitter. But shortly after the news broke, Twitter began removing links to the article.

Backlash ensued. Conservatives claimed this was more evidence of Twitter's pro-Biden bias. Others went so far as to assert this was Twitter interfering in an election. The reality of the situation was far more mundane.

As Twitter clarified -- largely to no avail -- it was simply enforcing its rules on hacked materials. To protect victims of hacking, Twitter forbids the distribution of information derived from hacking, malicious or otherwise. This policy was first put in place in March 2019, but it took an election season event to draw national attention to it.

The policy was updated after the Hunter Biden story broke, but largely remained unchanged. The updated policy explained in greater detail why Twitter takes down links to hacked material, as well as any exceptions it had to this rule.

Despite many people seeing this policy in action for the first time, this response was nothing new. Twitter had exercised it four months earlier, deleting tweets and suspending accounts linking to information obtained from law enforcement agencies by the Anonymous hacker collective and published by transparency activists Distributed Denial of Secrets. The only major difference was this involved acknowledged hackers and had nothing to do with a very contentious presidential race.

Decisions to be made by Twitter:

- Does the across-the-board blocking of hacked material prevent access to information of public interest?
- Does relying on the input of Twitter users to locate and moderate allegedly hacked materials allow users to bury information they'd rather not seen made public?
- Is this a problem Twitter has handled inadequately in the past? If so, does enforcement of this policy effectively deter hackers from publishing private information that could be damaging to victims?

Questions and policy implications to consider:

- Given the often-heated debates involving releases of information derived from hacking, does leaving decisions to Twitter moderators allow the platform to

decide what is or isn't newsworthy?
- Is the relative "power" (for lack of a better term) of the hacking victim (government agencies vs. private individuals) factored into Twitter's moderation decisions?
- Does any vetting of the hacked content occur before moderation decisions are made to see if released material actually contains violations of policy?

Resolution: The expanded version of Twitter's rules on hacked material remain in force. The additions to the policy in response to questions about its takedown of the Post article more clearly state what is or isn't allowed on the platform. The expanded rules presumably also make it easier for moderators to make informed decisions, rather than simply remove any information that may appear to be the result of hacking.

Originally posted to the Trust & Safety Foundation website.

6 Comments »

Upload Filters Will Always Be A Bad Idea, But Germany's New Implementation Of Article 17 Is An Attempt To Provide Some Protection For Users, Which Others May Follow

from the *but-what-will-the-CJEU-say?* dept

by Glyn Moody - May 26th @ 1:37pm

The EU's Copyright Directive was passed back in 2019, and the two-year period for implementing the law in national legislation is almost up. The text's contradictory requirements to stop infringing material from being posted online without imposing a general requirement to monitor users, which is not permitted under EU law, has proved difficult for governments to deal with. France aims to solve this by ignoring even the limited user protections laid down by the Directive. Germany has been having a rather fraught debate about how exactly Article 17, which implicitly requires upload filters, should be implemented. One good idea to allow users to "pre-flag" as legal the material they upload was jettisoned. That led to fears that the country's implementation of Article 17 would be as bad as France's. But the final version of the law does attempt to ensure that automated filters -- now admitted as indispensable, despite earlier assurances they were optional -- do not block user uploads that are not infringing on copyright. Communia explains:

> *the German implementation relies on the concept of "uses presumably authorised by law", which must not be blocked automatically. For an upload to qualify as "presumably authorised by law", it needs to fulfil the following cumulative criteria:*

> *The use must consist of less than 50% of the original protected work, The use must combine the parts of the work with other content, and The use must be minor (a non-commercial use of less than 15 seconds of audio or video, 160 characters of text or 125 kB of graphics) or, if it generates significant revenues or exceeds these thresholds, the user must flag it as being covered by an exception.*

Although it's good that this "presumably authorised by law" use is enshrined in law, the actual limits are absurd. For example, the name alone of the EU Copyright Directive in German is longer than 160 characters. Copyright holders can still challenge the legality of material, but platforms have to keep the uploads online until the complaints have been reviewed by a human. As former Pirate Party MEP Julia Reda writes on the Gesellschaft für Freiheitsrechte (Society for Civil Liberties) site, there's another feature of the new German law that might help keep upload filters in check, at least a little (original in German, translation via DeepL):

> *In order to enforce freedom of expression and artistic freedom against upload filters gone wild, the draft law provides for a right of association action for non-commercial associations dedicated to protecting the interests of users. These associations can take legal action against platforms that repeatedly block legal content. In addition, users will be able to claim damages against false copyright claims. The Society for Civil Liberties will use these possibilities if it becomes necessary.*

Those are important new options for getting material back online, and discouraging over-blocking. Reda notes that there is also good news for popular online activities such as caricature, parody and pastiche, which will be permitted without restrictions:

> *This copyright exception includes memes, remixes, mashups, fan fiction and fan art. The German government's draft proposal was to restrict this right to remix in the German copyright reform, although it was adopted as mandatory at the EU level as part of Article 17. The German government's proposal that these uses should only be allowed "provided that the extent of the use is justified by the specific purpose" generated an outcry in the fan fiction community. This has apparently had an effect, because the [German parliament's] legal committee has removed this restriction. Fans in Germany can now look forward to a solid legal basis for fan art and remix culture.*

The new German copyright law also brings in copyright exceptions for online teaching, and text and data mining. Cultural institutions such as libraries or archives will be permitted to make their collections available online if these works are no longer

commercially available. Those are all welcome, but it is the implementation of Article 17 that is likely to have the most impact. As the Communia blog post notes:

> *the German implementation law sets a new standard for the implementation of the [Digital Single Market] directive. This is especially true for the implementation of Article 17. With the Commission having missed the chance to issue guidance for the member states in a timely manner [discussed previously on Techdirt], other member states who seek to implement Article 17 in a fundamental rights-compliant way should look at the German law for guidance.*

Since the new Germany copyright law could become the model for other EU nations as they implement Article 17 -- except for France, of course -- it's good news that it has a number of positive elements. Those are likely to prove crucial if -- or rather when -- the EU Copyright Directive faces another legal challenge at the CJEU, the Court of Justice of the European Union (Poland has already lodged one). The complaint is likely to be that Article 17 cannot be implemented without violating the fundamental rights of users. In that case, the CJEU will have to decide whether Germany's innovative approach goes far enough in preserving them.

Follow me @glynmoody on Twitter, Diaspora, or Mastodon.

4 Comments »

EFF Tells Court Defendants Must Be Allowed To Examine The DNA Software Used To Convict Them

from the *rolling-dice-with-more-sides-but-they're-still-just-dice* dept

by Tim Cushing - May 26th @ 12:11pm

A proper adversarial system means the accused can confront the accuser. But that's rarely the case when crime solving software is involved. The FBI doesn't allow accused child porn downloaders to examine the malicious software it used to identify their computers. Multiple law enforcement agencies have dropped cases rather than discuss Stingray devices in open court.

All DNA analysis is handled by software. Most DNA analysis utilizes proprietary code created by private companies which license it to government agencies. The analysis may be performed by government agencies and employees, but when it comes to giving defense lawyers and their clients a chance to examine the software used to generate evidence, it suddenly becomes a very private matter.

Companies routinely intercede in criminal cases, telling judges that handing over source code or other information about their algorithms would somehow make it impossible for them to compete in the crime solving market. In most cases, judges are

sympathetic to claims about trade secrets and proprietary code, allowing the accused to only confront their accuser by proxy, via a government expert or an employee of the software company.

In rare cases, the court actually finds in favor of the defendant. Earlier this year, a case involving third-party DNA software and the EFF's intercession went the defendant's way with a federal judge in Pennsylvania telling the government it couldn't hide behind third-party trade secret assertions to keep this code out of the accused's hands. As the court reasoned then, if DNA evidence is central to the case against the defendant, the defendant should have access to the evidence and the software that created it.

The EFF is hoping for a similar outcome in a case being handled in California. It deals with the possibly wrongful conviction of a 70-year-old man for rape. And it involves a DNA software company whose algorithm was the only one that tied the suspect to the crime.

> *An elderly woman was sexually assaulted and murdered in her home and two witnesses described seeing a black man in his 50s on the property on the day of the murder. Dozens of people had passed through the victim's home in the few months leading up to the murder, including Mr. Davis and another individual. Mr. Davis is an African American man who was in his 70s at the time of the murder and suffers from Parkinson's disease. Another individual who met the witnesses' description had a history of sex crimes including sexual assault with a foreign object.*
>
> *DNA samples were taken from dozens of locations and items at the crime scene. Mr. Davis's DNA was not found on many of those, including a cane that was allegedly used to sexually assault the victim. Traditional DNA software was not able to match Mr. Davis to the DNA sample from a shoelace that was likely used to tie up the victim—but STRMix did, and the prosecution relied heavily on the latter before the jury.*

As the EFF points out in its brief [PDF], DNA software is anything but infallible. STRMix was caught a half-decade ago when a bug in its code possibly led to dozens of false arrests and convictions. Presumably that bug has been patched, but if no one outside of STRMix is allowed to examine the code, it's impossible to see if it might be leading prosecutors and government experts to overstate the certainty of DNA matches.

> *The necessity of independent source code review for probabilistic DNA programs was starkly demonstrated when FST (a counterpart to STRmix that was used in New York crime labs) was finally provided to a defense team for analysis. According to a defense expert, the undisclosed portion of the code could incorrectly tip the scales in favor of the prosecution's hypothesis that a defendant's DNA was present in a mixture. Reply Mem.*

> *of Law in Supp. as to Kevin Johnson at 19-21, United States v. Kevin Johnson, (S.D.N.Y. Feb. 27, 2017) (No. 15-CR-565 (VEC), D.I. 110). In fact, STRmix8 has suffered from programming errors that created false results in 60 cases in Queensland, Australia.*
>
> *The problems caused by nondisclosure are especially acute in the context of the latest generation of probabilistic DNA analysis because there is no objective baseline truth against which the output from the program may be evaluated—and thus it is impossible to gauge the accuracy of these programs by examining their results.*

If there's no objective baseline, every DNA analysis program is allowed to grade on its own curve. DNA matches aren't actually matches. They just reflect the likelihood of a match. With no baseline, the probability of it being an actual match is left to the discernment of prosecutors and their expert witnesses -- all of whom come out looking better if they can secure a conviction.

> *Unlike breathalyzers, the latest generation of complex DNA analysis tools cannot be measured against an objective truth. Instead, these DNA programs are more akin to probabilistic election forecasting models, such as those designed by FiveThirtyEight and The Economist. The outputted results are based on the calculation of the probability of events—that the defendant, rather than a random person, contributed to the DNA mixture or that person X will win an election—a value that is not an objectively measurable fact. This is why different DNA programs, and even different laboratories using the same program, will generate substantially different results for the same sample.*

This is why courts should allow defendants to examine the software that has, for the most part, accused them of committing crimes. If different algorithms produce different outcomes using the same inputs, none are to be trusted until they're independently examined. And DNA software companies aren't interested in that happening -- not solely because of any trade secrets but because any defendant who successfully casts doubt on the accuracy of test results undermines their business model.

But protecting a business model isn't the court's business. The courts are there to serve justice, which means protecting the rights of the accused from accusers utilizing proprietary tech while waving around signed NDAs.

Read More 8 Comments »

Babies & Bathwater: WSJ OpEd Suggests Banning

Cryptocurrency Entirely To Stop Ransomware

from the *good-luck-with-that* dept

by Mike Masnick - May 26th @ 10:44am

The hack of the Colonial Pipeline has already made lots of news, and with that, the government is rushing to come up with new regulations, which will almost certainly be overkill. While the transparency aspect of the expected rules (requiring reporting of "cyber incidents" to the federal government) was more or less expected to come at some point no matter what, the other rules are likely to be fighting the last battle. There are constant changes to these kinds of attacks, and seeking just to prevent them is a fool's errand.

However, we're now seeing some truly silly suggestions. Lee Reiners, who runs Duke Law School's Global Financial Markets Center, has published an op-ed in the WSJ that truly is an astounding example of throwing out all the babies with the bathwater. Reiners says the way to stop these attacks is to just ban all cryptocurrency. This is silly on many levels -- mostly because (1) that's impossible, (2) it wouldn't work, and (3) it would destroy a ton of important and valuable projects. Frankly this op-ed does not speak well to the Global Financial Markets Center and its understanding of anything. Here's the core of the argument:

> *Ransomware can't succeed without cryptocurrency. The pseudonymity that crypto provides has made it the exclusive method of payment for hackers. It makes their job relatively safe and easy. There is even a new business model in which developers sell or lease ransomware, empowering malicious actors who aren't tech-savvy themselves to receive payment quickly and securely. Before cryptocurrency, attackers had to set up shell companies to receive credit-card payments or request ransom payment in prepaid cash cards, leaving a trail in either case. It is no coincidence that ransomware attacks exploded with the emergence of cryptocurrency.*

There is no doubt that cryptocurrency does aid the ability to pass around money without being traced -- and that certainly can (and does) help some criminal enterprises. But, the idea that it makes their job "safe and easy" is simply not true. We've seen plenty of criminal operations that relied on cryptocurrency run into issues, including being taken down by law enforcement. This is for a variety of reasons -- including that in the process of converting cryptocurrency into other forms of money, you often end up introducing friction that may require some identification. Similarly, there are a lot of steps involved in transferring around even large sums of cryptocurrency that can leave trails. Are there ways to hide yourself? Absolutely, but it's not as "easy" as the article makes it out to be.

And the claim that the rise of ransomware is because of cryptocurrency seems like a

"correlation does not mean causation" kind of situation. There are many reasons why ransomware may have increased over the past few years -- including improvements in a variety of hacking tools, the increased online nature of many businesses (especially during the pandemic) and some other factors as well.

> *Banning anything runs counter to the American ethos, but as our experience with social media should teach us, the innovative isn't always an unalloyed good. A sober assessment of cryptocurrency must conclude that the damage wrought by crypto-fueled ransomware vastly outweighs any benefits from cryptocurrency.*

I mean... what? No one has ever argued that any innovation is "an unalloyed good." Basically everyone recognizes that innovation has a variety of different impacts -- some good, some bad, some indifferent. They're tools. Some people use them for good things. Some people use them for bad things. That's true of social media. And it's true of cryptocurrency. But Reiner then takes the leap from saying it's not an "unalloyed good" to insist that, actually, cryptocurrency is all bad. Why? Because he says so.

> *It isn't obvious that cryptocurrency provides any benefit at all beyond the chance to make a quick buck. I have been studying the crypto market since its inception, and I have yet to identify a single task or process that crypto makes easier, better, cheaper or faster. Don't take my word for it. Ask any friend why he owns cryptocurrency, and the answer will invariably be "to make money." In other words, speculation. (The blockchain technology that underpins crypto does have promising applications in supply-chain management and other areas.)*

This paragraph is the kind that should be remembered in the future. I know that many people probably do agree with this assessment, but it shows a real lack of imagination about how cryptocurrency could be useful, as well as a real lack of understanding of the nature of innovations and how they progress over time. We certainly heard similar statements regarding home computers, the internet itself, mobile phones and many other things as well. It may be true that the killer apps for cryptocurrencies are not well recognized now, but that hardly means they don't exist, and it really isn't an excuse for trying to **ban** the entire concept.

As for that closing sentence about blockchain, the paragraph totally misses that the underpinnings of what makes a blockchain effective is the integration with cryptocurrency. Yes, you can create cryptocurrency-less blockchains, but they tend to be significantly less interesting, and almost certainly need to create some other incentive system. That generally means that they only work when controlled by a few centralized players, dropping the benefits of a more truly decentralized system with cryptocurrency.

And, the line that most people investing in cryptocurrency are doing so to make money is... meaningless. Yes, that's one of the important functions of money. It acts as an incentive system. But some of the clever aspects of how cryptocurrency and blockchain work together is that built-in incentive structure that makes the distributed/trustless system function. Yes, the fact that many people are in cryptocurrency to make money does open it up to speculation (and scams). But that incentive is a feature, not a bug.

Most importantly, this ignores that there are interesting ideas and innovations that are just starting to come out of the cryptocurrency world. Obvious, we've talked a lot on Techdirt about dealing with other issues -- competition, privacy, free speech, content moderation, etc. -- with a more distributed internet. And one way to help make that a reality is using cryptocurrency. We're already seeing some interesting elements of that start to play out with things like FileCoin and the projects that are just starting to show up around that space. To claim that there's nothing valuable at all is to show a near total ignorance of the more interesting elements of what's happening. Yes, there are plenty of silly scams and headline grabbing nonsense, but to insist that means there's no redeeming value is missing the point. Entirely.

Reiner then includes a paragraph that basically says people will mock him for these claims, and insisting that because people will attack him for his short-sighted ideas, it proves that "the emperor has no clothes." Huh?

> *A day after the Colonial Pipeline shutdown, cryptocurrency champion and self-proclaimed "Dogefather" Elon Musk went on "Saturday Night Live" and admitted the obvious: The dogecoin cryptocurrency is a "hustle." He then performed an encore by tweeting that Tesla was suspending the use of bitcoin for vehicle purchases due to the coin's carbon footprint.*

Tarring all cryptocurrency because Elon Musk's random flights of fancy -- and focusing on Dogecoin of all the cryptocurrencies out there -- does not make the argument more compelling. It screams out that Reiner is cherry picking examples. Yes, there are silly cryptocurrencies. Yes, there are scams. Yes there is ransomware and yes sometimes cryptocurrencies can make some aspects of criminal behavior easier. But this article fails to tackle any of that in a meaningful way, simply pulling some edge cases and tapdancing around the rest.

And, of course, as we noted above, the idea that you could even ban cryptocurrency is ludicrous. The entire idea behind them was that there is no central node that you can shut off. Reiner tries to get around this by noting the government could put in place a whole bunch of annoying hurdles, but that's not going to stop cryptocurrencies at all.

> *Any solution must at least reduce the use of cryptocurrency. Governments and retailers should be encouraged not to accept payment in it. An outright ban could get the job done, but if it would be too*

> *difficult to enforce or get through Congress, regulators could crack down on the off-ramps and on-ramps, the points at which crypto is converted into fiat currency and vice versa.*
>
> *Cryptocurrency firms serving U.S. customers are supposed to be subject to the same anti-money-laundering requirements as traditional financial institutions, but more can be done. Late last year, the Treasury Department's Financial Crimes Enforcement Network proposed a rule to establish new reporting, verification and record-keeping requirements for certain cryptocurrency transactions. Last week Treasury proposed granting more resources to the Internal Revenue Service to address crypto and called on businesses to report receipts of more than $10,000 in cryptocurrency. Both proposals should be adopted, but they will be effective only if other countries follow suit.*

I mean, it's kinda funny, because up top I noted that the idea that criminals can easily get away with ransomware because of cryptocurrency wasn't always true because of regulations at the "on-ramps" and "off-ramps" and then later in the article he more or less admits that's true.

Of course, there are other risks associated with heavily regulating cryptocurrency -- again in potentially throwing out babies with the bathwater. Putting too many restrictions on the usage of cryptocurrency could hinder adoption of the *actual* useful elements of it.

> *We can live in a world with cryptocurrency or a world without ransomware, but we can't have both. It is time for the adults to tell the children: Party's over.*

That's nonsense. There's no way to get rid of cryptocurrency, and if we just overly burden it with excess regulations as he proposes, that will just lead to more creative workarounds, that will get even more adoption among criminal elements, rather than for more socially useful activities. Second, there is no such thing as "a world without ransomware." This is just wishful thinking based on the false premise that ransomware only exists because of cryptocurrencies.

And, yes, clearly there's a real risk with ransomware and attacks like the Colonial Pipeline that the end result could be quite problematic. However, the fact is the real cybersecurity risks from ransomware are monetary risks. The risks associated with taking down or breaking critical infrastructure tends to come from nation-state attacks, not ransomware attacks for money. The whole op-ed is a silly, nonsensical attack on cryptocurrency that doesn't seem based in reality. If that's the level of the work that comes out of the Global Financial Markets Center, it does not speak highly of Duke's ability to produce good scholarship on this subject.

Of course, I will note that Reiner's hatred of cryptocurrency has not stopped his own center from asking the public to donate cryptocurrency to support the center. How curious.

42 Comments »

Daily Deal: The Ultimate 2021 White Hat Hacker Bundle

from the *good-deals-on-cool-stuff* dept

by Daily Deal - May 26th @ 10:39am

The Ultimate 2021 White Hat Hacker Bundle has 10 courses to teach you how to defend any system from digital attacks. You'll develop an understanding of the threat and vulnerability landscape through threat modeling and risk assessments, and build a foundation for which to expand your security knowledge. It's on sale for $39.90.

source: imgur.com

Note: The Techdirt Deals Store is powered and curated by StackCommerce. A portion of all sales from Techdirt Deals helps support Techdirt. The products featured do not reflect endorsements by our editorial team.

Comment »

DC Court Says Recordings Of Capitol Rioters Must Be Made Public, But Only On A Case-By-Case Basis

from the *getting-prejudiced-by-your-own-livestream* dept

by Tim Cushing - May 26th @ 9:34am

Here's a small victory for the First Amendment and presumption of openness that's supposed to apply to court proceedings. A recent opinion [PDF] by the DC Circuit Court will give everyone more access to recordings covering the dozens of prosecutions of insurrectionist cosplayers who raided the Capitol on January 6th. The court comes down firmly on the side of openness and transparency, but has hung a rather large asterisk on that statement.

ProPublica is the entity that made the request for an administrative order, but it's the in-court figurehead for a group of fourteen journalistic concerns. The US Attorney's Office hasn't exactly been proactive when releasing recordings entered as evidence in the Capitol raid cases. It has even (temporarily) withheld recordings that were pulled from social media services and YouTube -- something that indicates these recordings were public before the government made them private.

While these recordings are viewable during court proceedings, limited access has prevented some journalists from accessing them. And once the proceedings are over, they're no longer viewable. The DC Circuit Court has made some permanently accessible but only on a case-by-case basis. Considering the volume of criminal cases being handled by the court -- combined with limited access prompted in part by the COVID pandemic -- this no longer appears to be acceptable.

> *In the pending petition, the group of fourteen media organizations express frustration with the case-by-case approach to providing media access to video exhibits, explaining that petitioning for the release of video exhibits in individual cases has led to delayed release of those exhibits, and objecting to the absence of a platform to provide broad and convenient public access to video exhibits in the numerous Capitol Cases in which such exhibits have been presented to the court but are not available to the public. Consequently, they seek a standing order directing the government to contemporaneously release copies of video exhibits admitted in pretrial proceedings in the Capitol Cases to a designated press representative, ProPublica, for further distribution to news organizations and to the public at large.*

The government doesn't necessarily disagree. It would prefer to handle things its way -- giving press members access through a shared "drop box." Recordings would be placed there after being reviewed for any necessary redactions. But that would mean a 72-hour delay between their presentation in court and their accessibility by outsiders.

On the other side, the defendants' legal reps are arguing that releasing recordings during the pre-trial phase would potentially prejudice their clients, decreasing their chances of receiving a fair trial. This includes possibly tainting jury pools or giving the government the upper hand with edited footage that might mislead members of the public.

Given these three conflicting interests, the court decides the records are definitely public. But how public and how quickly can't necessarily be resolved with a broad order. It's not that anyone isn't aware of the January 6th Capitol raid or the arrests stemming from this. But there's still a small chance defendants might lose access to a fair trial if selectively edited recordings are released.

> *Certainly, the events at the U.S. Capitol on January 6, 2021, generally, and the Capitol Cases in particular, have already been the subject of extraordinary attention both nationally and even globally. Given this context, disclosure of video exhibits in individual Capitol Cases may not generate any more prejudicial attention than already attaches to this event. Nevertheless, disclosure of particularly egregious or inflammatory*

> *conduct associated with an individual defendant or a particular video clip that "does not contain the whole event but rather a deliberately chosen or edited clip to support a certain argument or narrative," FPD Resp. at 3, may present sufficient unfair prejudice at this stage that the presiding judge may decide to delay or limit access in some way. Evaluation of such risks must be carried out on a case-by case basis.*

For the first time in a long time, the government agrees with the press. It argues the risk of prejudice is so low as to be speculative and supports ProPublica's request for a blanket order affecting all recordings entered as evidence. Of course, this has nothing to do with supporting free speech protections and everything to do with getting as much damaging info about the Capitol raid suspects out there as possible, even if it means utilizing the Fourth Estate.

In the end, the press (and its new buddy, the government) wins. But only barely. And with a handful of stipulations.

> *For these reasons, petitioners' request for issuance of a standing order to provide a streamlined means in this Court for making video exhibits in Capitol Cases accessible to the media will be granted but, in accordance with applicable law and rules, access to these video exhibits may be authorized after the presiding judge has the opportunity to consider the positions of the parties.*

Yes, with a but. That's probably all we can expect at this point in the judicial process. But it's good to see the DC Circuit reiterate its belief in the presumption of openness. This is the circuit that hosts the highest percentage of sealed cases and dockets -- something that has earned it a lot of justified criticism over the years. Hopefully it will maintain its support of this presumption when it's the government arguing that filings and evidence should be withheld from the public.

Read More | 1 Comment »

27 'Right To Repair' Laws Proposed This Year. Giants Like Apple Have Ensured None Have Passed So Far.

from the *this-isn't-going-away* dept

by Karl Bode - May 26th @ 6:12am

We've repeatedly noted how the "right to repair" movement has been gaining a full head of steam as consumers, independent repair shops, schools, farmers, and countless others grow tired of corporations' attempts to monopolize repair. Whether it's Sony and Microsoft creating repair monopolies for their game consoles, Apple bullying independent repair shops, or John Deere making it a costly hassle just to fix a

tractor, the more companies restrict access to cheap repair, parts, tools, and documentation, the more this movement seems to grow. Especially in the COVID era where the problem has also hindered health care.

Bloomberg notes that 27 states have considered right to repair legislation so far this year, making access to essential tools and less expensive repair options a legal right. But corporations have shot down all of them so far, in part thanks to a misleading, coordinated lobbying campaign falsely claiming that reform on this front poses dramatic privacy and security harms:

> *"One reason these legislative efforts have failed is the opposition, which happens to sell boatloads of new devices every year. Microsoft's top lawyer advocated against a repair bill in its home state. Lobbyists for Google and Amazon.com Inc. swooped into Colorado this year to help quash a proposal. Trade groups representing Apple Inc. successfully buried a version in Nevada. Telecoms, home appliance firms and medical companies also opposed the measures, but few have the lobbying muscle and cash of these technology giants. While tech companies face high-profile scrutiny in Washington, they quietly wield power in statehouses to shape public policy and stamp out unwelcome laws."*

Bloomberg doesn't even get into many of the sleazier efforts on this front, like the auto industry's false claims that right to repair reform would be of great benefit to stalkers and sexual predators. Or Apple's false claim that giving consumers more rights over things they own would turn states into dangerous meccas for hackers. Despite the fact the FTC recently released a report making it clear the vast majority of these claims aren't substantiated, the scare mongering has been extremely effective at befuddling confused or financially-conflicted lawmakers.

The existing broken, wasteful system is hugely lucrative for major companies, even if it harms the planet, annoys countless consumers, and makes everyday life more expensive for school districts:

> *"Around 10 to 15% of a district's devices end up needing repairs during a typical school year, according to Millman. One Long Island district he works with has over 13,000 iPads in circulation. He estimates that they have around $130,000 a year in repair costs. If the district had to replace all the broken iPads, rather than fix them, that cost jumps up a quarter of a million dollars.*
>
> *"That's why Apple doesn't answer my emails," Millman said. "For them, it's just dollars and cents. They don't think about the person on the other side of the iPad."*

It's tough to pass reform when you've got a vast coalition of extremely wealthy and

powerful corporations all working in concert to fight it (see: the long uphill climb on passing even a very basic US privacy law). But with right to repair, there's a massive, bipartisan coalition of folks whose ranks only grow bigger the more these companies press their luck.

14 Comments »

Crime-Reporting App Citizen Apparently Attempting To Get Into The Law Enforcement Business

from the *bad-ideas-from-worse-people* dept

by Tim Cushing - May 26th @ 3:15am

It looks like app developers want to be cops. Late last week, a Los Angeles resident spotted a Citizen-app branded patrol car roaming the city. Citizen is yet another app that allows residents to send crime alerts and other news to each other, following in the steps of Ring's Neighbors app and Nextdoor, a hyperlocal social media service that only lets actual neighbors connect with each other.

The only thing missing here is the replicant hunters.

> *"Few things make you feel like you live in a bleak dystopian reality like a Citizen App patrol car that looks like a cop car," Brandon Wenerd tweeted, along with a photo of the vehicle, on Wednesday.*
>
> *The all black vehicle with tinted windows has the Citizen logo emblazoned across its side, as well as Citizen's tagline "Making your world a safer place" and the phrase "Private Patrol."*

Also emblazoned on the dystopiamobile was the logo for Los Angeles Professional Security, a private security firm with its own fleet of vehicles. That only added to the list of raised questions about the app and its plans for the future.

Like any other app or service that allows locals to report crime and other suspicious activity, Citizen has proven to be a handy conduit for bigots and racists to expose their biases and, unfortunately, find like-minded "citizens" in their area. This app may have been more empowering than most. It allows users to send crime alerts and Citizen encourages the livestreaming of crimes in progress. While it may not actually encourage users to don their Batsuits and start fighting crime on their own, the app did make its debut under the name "Vigilante." Its booting from Apple's app store resulted in its less-overtly-worrying rebrand.

But here's what's actually going on: Citizen wants to get into the cop business. That's according to internal documents shared with Joseph Cox and Motherboard shortly after residents began reporting the existence of this Citizen-branded mock cop car.

> *Crime and neighborhood watch app Citizen has ambitions to deploy private security workers to the scene of disturbances at the request of app users, according to leaked internal Citizen documents and Citizen sources.*
>
> *[...]*
>
> *"The broad master plan was to create a privatized secondary emergency response network," one former Citizen employee told Motherboard. Motherboard granted multiple sources anonymity to protect them from retaliation from the company.*
>
> *"It's been something discussed for a while but I personally never expected it to make it this far," another Citizen source told Motherboard.*

The car observed on the streets is Citizen's "security response" vehicle. Presumably, Citizen is planning to add more cars to this fleet so it can better serve users who feel they might need some additional security. Whether that includes responding to calls of crimes in progress remains to be seen, but the addition of Los Angeles Professional Security to the mix suggests that it does. This firm offers a "subscription law enforcement service" that includes a "potent combination of technology, K-9 support, and patrol personnel."

That's not the only private security firm in the mix.

> *Citizen has been actively testing the program, with what the company describes as quick response times and instant communication between Citizen and security partners, according to the emails.*
>
> *One of those companies, according to the emails, is well-known private security contractor Securitas. The email about the tests says that Securitas average response times have improved to around 20 minutes.*

It looks like Citizen believes there's a large market for private cops. Unfortunately, it looks like local law enforcement agrees. According to internal emails seen by Motherboard, Citizen approached the Los Angeles Police Department with its proposal to expand into the police business and this was (allegedly -- we are talking about a document that will probably be used to market Citizen to other cop shops) warmly received by LAPD officials, who said it would be a "game changer."

And, to be sure, it might be. Los Angeles has a property crime problem cops can't seem to fix. Adding roving bands of vigilantes would be a "game changer" too, but no one really thinks that's a solution. That's just an additional problem. Citizen's expansion may change the game, but it also encourages Citizen to embrace the ideals that saw it debut as "Vigilante."

We don't need tech companies thinking they're just an extension of the government,

especially the parts of the government allowed to deploy deadly force and deprive people of their freedoms. Blurring the line between public and private tends to work out poorly for those supposedly being served by these partnerships. Members of the public will be expected to treat both as law enforcement, even though only actual cops have the power to enforce the law. Private companies can do things cops can't -- like engage in searches of property ostensibly under their control -- and cops can swoop in and directly benefit from searches they themselves cannot legally engage in. The end result will be more government power -- not derived from laws or Constitutional amendments but from app developers who see themselves as crime fighters.

49 Comments »

Visit Techdirt for today's stories.