

The Background Investigator

Your Information Resource

Happy Holidays



Volume 19 Number 12
December 2019

Since the beginning of our industry.

Ride Share Background Checks

Lyft, Uber are examples of what's wrong with background checks

WE BEAT
any
PRICE
any
DAY
GUARANTEED!

London Criminal \$19.99

London
Daily

Additional service throughout the U.K.

Criminal
Requests

Our Every Day Low Prices
London England
Criminal Record Search
\$19.99

Puerto Rico
More Hits
Straightline
International

Based on figures, Straightline is booming in the UK



Sri Lanka Court



Express Service
Same day service available*

LOWEST PRICES

★
Everyday
★

STRAIGHT
LINE

★
Special
prices on
ALL
Searches

After 20 years I know Straightline gets the job done

Want More Hits?
Fastest Turnaround
call Straightline

Unlimited Possibilities

Puerto Rico
More Hits
Straightline
International

Straightline International - The Best Canadian Searches Available

Ae Hiring Algo-
rithims Fair?

Time is money and, unfortunately for companies, hiring new employees takes significant time -- more than a month on average, research shows.

Hiring decisions are also rife with human bias, leading some organizations to hand off at least part of their employee searches to outside tech companies who screen applicants with machine learning algorithms. If humans have such a hard time finding the best fit for their companies, the thinking goes, maybe a machine can do it better and more efficiently.

But new research from a team of Computing and Information Science scholars at Cornell University raises questions about those algorithms and the tech companies who develop and use them: How unbiased is the automated screening process? How are the algorithms built? And by whom, toward what end, and with what data?

They found companies tend to favor obscurity over transparency in this emerging field, where lack of consensus on fundamental points -- formal definitions of "bias" and "fairness," for starters -- have enabled tech companies to define and address algorithmic bias on their own terms.

"I think we're starting to see a growing recognition among creators of algorithmic decision-making tools that they need to be particularly cognizant of how their tools impact people," said Manish Raghavan, a doctoral student in computer science and first author of "Mitigating Bias in Algorithmic Employment Screening: Evaluating Claims and Practices," to be presented in January at the Association for Computing Machinery Conference on Fairness, Accountability and Transparency.

"Many of the vendors we encountered in our work acknowledge this (impact) and they're taking steps to

address bias and discrimination," Raghavan said. "However, there's a notable lack of consensus or direction on exactly how this should be done."

The researchers scoured available public information to begin to understand these tools and what measures, if any, companies have in place to evaluate and mitigate algorithmic bias. Shielded by intellectual property laws, tech companies don't have to disclose any information about their algorithmic models for pre-employment screenings -- though some companies did choose to offer insight.

The researchers honed in on 19 vendors who specialize in algorithmic pre-employment screenings, which, they found, include questions, video interview analysis and games. They combed company websites, webinars and any available documents for insights into vendor claims and practices.

Very few vendors offer concrete information about how they validate their assessments or disclose specifics on how they mitigate algorithmic bias, researchers found.

"Plenty of vendors make no mention of efforts to combat bias, which is particularly worrying since either they're not thinking about it at all, or they're not being transparent about their practices," Raghavan said.

Even if they use such terms as "bias" and "fairness," these can be vague. A vendor can claim its assessment algorithm is "fair" without revealing how the company defines fairness.

It's like "free-range" eggs, Raghavan said: There is a set of conditions under which eggs can be labeled free range, but our intuitive notion of free range may not line up with those conditions.

"In the same way, calling an algorithm 'fair' appeals to our intuitive understanding of the term while only

accomplishing a much narrower result than we might hope for," he said.

The team hopes the paper will encourage transparency and conversation around what it means to act ethically in this domain of pre-employment assessments through machine learning.

Given the challenges, could it be that algorithms are just not up to the job of screening applicants? Not so fast, Raghavan said.

"We know from years of empirical evidence that humans suffer from a variety of biases when it comes to evaluating employment candidates," he said. "The real question is not whether algorithms can be made perfect; instead, the relevant comparison is whether they can improve over alternative methods, or in this case, the human status quo.

"Despite their many flaws," he said, "algorithms do have the potential to contribute to a more equitable society, and further work is needed to ensure that we can understand and mitigate the biases they bring."

Credit: <https://www.sciencedaily.com/releases/2019/11/191120175616.htm>

CALL
to ADVERTISE
1-866-909-6678
BackGround Investigator

Straightline



1-866-909-6678

Virginia Courts
Online

Virginia's court system made it a lot easier to find online court records, quietly rolling out a statewide search function on its website that allows users to search by a defendant's name to find docket information about criminal and traffic charges back to 1990 or earlier in most jurisdictions.

Previously, the records were available online, but searches were limited to specific courthouses, meaning a user had to either know where charges were filed to find them or conduct hundreds of individual searches.

The General Assembly required the Supreme Court's Office of the Executive Secretary to provide the new function as part of legislation passed in March 2018, which mandated the new system to go live by the beginning of this month.

There was little discussion at the time. Lawmakers rolled the bill, proposed by Sen. Monty Mason, D-Williamsburg, into a broader (and more widely reported) open records law championed by the Daily Press in Newport News that requires the court system to provide bulk data to those who request it.

The newspaper's advocacy was bolstered by open government advocates, who

used time-consuming scraping techniques to provide both bulk data and a rudimentary statewide search function beginning in 2014.

Ben Schoeneld, who created VirginiaCourtData.org to provide the data free of charge, said he would cease operating the statewide search he created and cease scraping data now that both functions are available through official channels.

While the new system will make it easier for journalists to, say, vet a candidate for public office or cover breaking news, it remains unclear how it will be received by the wider public, particularly as momentum grows to limit the role of criminal record searches in employment screenings.

Website: <https://eapps.courts.state.va.us/ocis/landing/false>

Contact:
Steven Brownstein
Box 10001
Saipan, MP 96950

+1-670-256-7000
findcrime@thebackgroundinvestigator.com



Meet Steven Brownstein
On LinkedIn

Did LexisNexis Sell Private Data Or Not?

LexisNexis states, “depending on how you interact with us and the service, we use your personal information to” and then gives a laundry list of uses.

These include custom content, targeted ads, promotional messages, even sweepstakes invitations.

It also says LexisNexis may study usage trends, develop data analysis and also may trade your data with parent company RELX, which as the New York Times reported in 2016, collects police information, sells it to insurance companies and kicks back a cut to cities.

LexisNexis has even been sued by states like Illinois and Massachusetts, for allegedly withholding portions of those fees from law enforcement agencies.

The company disputes those claims, but settled with the states for millions of dollars.

Confused About Canada Criminal Record Checks?

From Canadian HR Reporter > Canadian Employment Law Today

Outside of a few defined industries, most organizations are not obligated to obtain police record checks when screening employment candidates.

The court records are also available as an alternative.

Confused About Canada Criminal Record Checks (PartII)?

What comes back from a CPIC search?

CONFIRMATION OF A CRIMINAL RECORD - Standard Response

13.10 When the CNI/CRS query identifies a criminal record that matches to the criminal record information declared by the Applicant: "Based solely on the name (s) and date of birth provided and the criminal record information declared by the applicant, a search of the RCMP National Repository of Criminal Records has resulted in a possible match to a registered criminal record. Positive identification that a criminal record does or does not exist at the RCMP National Repository of Criminal Records can only be confirmed by fingerprint comparison. As such, the criminal record information declared by the applicant does not constitute a Certified Criminal Record by the RCMP. Delays do exist between a conviction being rendered in court, and the details being accessible on the RCMP National Repository of Criminal Records. Not all offences are reported to the RCMP National Repository of Criminal Records."

What comes back from a court search?

Case number, Name found on index, Identifiers on record, Date files, charges, date of disposition, disposition, sentence.

Is Renting A Virtual Office Duping The Customer?

Recently it was found that a Canadian based company advertised a new business in the USA, but it turned out to be a vir-

**STRAIGHT
LINE**

The new business' advertised phone number was for their Canadian physical location.

Is this fraud or duping an unsuspecting public? Read on about these Virtual Office Companies and make up your own mind up.

Time to shut these dodgy offices for the dodgy dealers

by Patrick Collinson

It's the prestigious address that gives an air of authenticity...

It only costs a few hundred pounds to rent a “virtual office” that redirects mail and phone calls. What could be more respectable than, say, an office in Tower 42, still better known as the former NatWest Tower and an icon of the London skyline?

One (person), though, had her suspicions. She decided to do a bit of her own investigating, and rang the number in Tower 42.

The office was managed by Regus, the self-styled “world’s largest provider of flexible workspace”. By doing her research, she found they had a mail forwarding facility and not a physical presence in the skyscraper. But the Regus person answering the phone gave her the impression that the company had a team of people occupying level seven of the tower.

(But she) persisted. Had there been other calls? Had there been complaints? She was again assured by Regus that there had not been “any sort of complaints”.

But our caller was cruelly deceived. However, and rather brilliantly, she had the sense to tape the conversation – and it has provided vital evidence for prosecution.

(Recently), Regus was found guilty at the City of London magistrates court and fined £11,000 plus £16,600 costs.

But Regus – which made an operating profit of

£104.3m in 2014 – was lucky to get off so lightly.

It turns out that four months earlier, Regus had been contacted by the City of London Corporation's trading standards team, worried that their temporary tenant in Tower 42 had the hallmarks of a typical "boiler room" investment scam, involving the sale of worthless or nonexistent commodities like diamonds and wine, or "carbon credits".

There are rules about mail forwarding services (yes, I'm surprised they exist) and for once they are being enforced. Office providers are required by the London Local Authorities Act 2007 to hold detailed records on their client firms. Regus did not – and was found guilty of four breaches of the act.

Servcorp, another multinational provider of temporary offices, has been little better. In December last year the City of London police and trading standards offices called in at its “stunning skyscraper” Dashwood House, just minutes from Liverpool Street station in the heart of the City. They asked to inspect the records Servcorp held on clients, a significant number of whom were suspected of fraudulent activity.

The act required Servcorp to keep records open for inspection at all reasonable times. But it couldn't comply with the request for another two months – and, when it did, its records were inadequate. A fortnight ago it was ordered to pay £21,000 in fines and £11,500 in costs after pleading guilty to seven

offences under the act. Of course, not every occupant of Servcorp's space in Dashwood House or Regus's offices in Tower 42 are crooks. But in both instances Servcorp and Regus were the enablers to fraudsters hoping to dupe the public with prestige office addresses. A quick search of the Financial Conduct Authority's database unearths seven official warnings about dodgy firms in Dashwood House, and 14 in Tower 42. We can't say if every one of them were Regus or Servcorp clients, but it's not a happy record.

The City of London trading standards has said it will “not tolerate office providers which allow suspected boiler room operations to develop in their sites”. In a statement, Regus said these were “isolated incidents” and “enhanced safeguards have been put in place to prevent any future repetition”.

So, why would a foreign background check company put a new company in a virtual office?



PUBLISHER
Steven Brownstein

CONTRIBUTORS:
Les Rosen, Dennis Brownstein, Phyllis Nadel

COVER PHOTOGRAPH: Baltimore, Maryland Courthouse

COVER PHOTOGRAPHER:
Steven Brownstein

PURPOSE: “Dedicated to pre-employment screenings everywhere”

The Background Investigator is published by Steven Brownstein, LLC, PMB 1007, Box 10001, Saipan, MP 96950. Phone: 670-256-7000. Copyright 2018 by Steven Brownstein. Some material in this publication must not be reproduced by any method without the written permission of the copyright holder.

SUBSCRIPTIONS: Toll free USA 1-866-909-6678

Senator Says Checkr Background Checks Not Good Enough

Sen. Richard Blumenthal (D-Conn.) said that Uber and Lyft provided “ambiguous” answers to his recent inquiries about safety measures in the ride-hailing industry and called on both companies to institute fingerprint background checks for drivers.

Blumenthal said the two companies should also exchange data about driver dismissals with each other, which would help keep the entire system more safe.

“The responses to us certainly are lacking in any sense of priority,” he said, referring to responses to his request for background checks or fingerprinting. “They have a real responsibility for taking every possible step to do background checks that are reliable and comprehensive.”

The senator in September asked for more information from Uber and Lyft following a Washington Post article about Uber’s Special Investigations Unit. The Post investigation found that safety investigators are instructed to keep the company’s interests foremost, including through restrictions on their ability to report apparent felonies to police and a ban on sharing information with competitor Lyft about possibly dangerous drivers. That means that drivers who are restricted from Uber or Lyft for violations like poor driving or even assaults on passengers can, with impunity, simply register as a driver for the other company.

“If they ban a driver right now, they have no protocol or procedure for sharing that information with each other,” he said. “I think that’s just central to safety, and yet they have no protocol.”

When rides go wrong: How Uber’s investigations

unit works to limit the company’s liability

Blumenthal said he plans to arrange to meet with representatives of the two companies privately and that he believed Congress should hold hearings on ride-hailing safety. Representatives from neither Uber nor Lyft appeared at a recent House Transportation subcommittee hearing aimed at examining safety and labor practices.

Uber and Lyft have both faced multiple lawsuits over their background checking policy and responses to assaults and sexual misconduct during rides. Earlier this year, 14 women sued Lyft alleging it didn’t adequately respond to their allegations of sexual assaults during rides.

The companies have added new features like panic buttons in the app and additional background checks for existing drivers. Lyft recently updated its protocols for driver bans, The Post reported, issuing new guidelines that could result in bringing some previously banned drivers back onto the platform.

“Uber is deeply committed to the safety of riders and drivers, and our actions show it,” Uber spokeswoman Susan Hendrick said in a statement. “We look forward to meeting with the Senator soon.” Lyft spokesman Adrian Durbin said Lyft “has worked hard to design innovative policies and features focused on the safety of both passengers and drivers” and that the company has hundreds of staff working on safety initiatives.

In their responses to Blumenthal, both Uber and Lyft said fingerprinting may bias against minorities who are more likely to be arrested but not necessarily convicted. That is why, they said, they rely on their own background check systems and those provided by a tech company called Checkr.

“That’s the reason for belt and suspenders — for using both Checkr and finger-

print,” said Blumenthal. “The only reason they can possibly give [for not using fingerprinting] is additional cost — it should be the cost of engaging in their business.”

Uber and Lyft are required to use fingerprint background checks in New York City and previously were required to in Houston. Rather than face voter-approved fingerprint background checks, the companies in 2016 suspended operations in Austin for more than a year before the governor overturned the rules statewide.

“While no background check is perfect, our process is thorough, fair and relevant to the work in question,” Justin Kintz, Uber vice president of global public policy, wrote in his letter to Blumenthal.

Lyft’s director of federal public policy, Lauren Belive, said in her letter to Blumenthal that the company is “constantly developing new ways to enhance ride safety.”

Blumenthal said he supports Uber’s policy that survivors of sexual assault should be allowed to decide if they want to go public with their stories, but he noted that law enforcement can keep victims anonymous. Uber and Lyft “have an independent responsibility to at least alert law enforcement even if the wish of the survivor is respected — and it should be — that they want to avoid being part of some public proceeding,” he said. “Lyft or Uber drivers are in positions of trust. Once somebody gets into their car, the rider is vulnerable.”

Uber and Lyft both said they have 24-hour support for riders and suspend or ban drivers when their investigations warrant.



CA DMV Makes \$50M Selling Personal Data, Report Says

The California Department of Motor Vehicles is selling customers’ personal information for millions of dollars, according to a report from VICE released this week.

The report cites a CA DMV document that shows the “total annual revenue” from commercial requesters of data.

The state has collected about \$50 million a year since 2015 providing registration and license data to various businesses, according to that document.

“[I’m] really irritated that they make that much money selling our personal information,” said Julian resident Dale Watterson while in line at the Hillcrest DMV Tuesday. “In this day of protecting your information, that’s just inexcusable.”

But the DMV is pushing back.

“The VICE headline is inaccurate,” said DMV Public Affairs Deputy Director Anita Gore.

Gore explained only certain groups, like insurance companies, background check businesses or car manufacturers, can seek the data.

The spokesperson said the \$50 million a year is not profit, but rather just the cost of processing the requests for data.

“We do not put information up for sale,” Gore continued in a phone call with NBC 7.

However, the DMV did not provide a specific list of those businesses or companies who have paid for data.

And when asked if DMV customers are made aware their data may be sold, Gore asked, wouldn’t [NBC 7] want to know if a

car manufacturer had a recall, and used the information to get in touch?

“We don’t want it to be just open sourced, where anybody who wants it can obtain our data for a fee,” said Identity Theft Resource Center CEO Eva Velasquez.

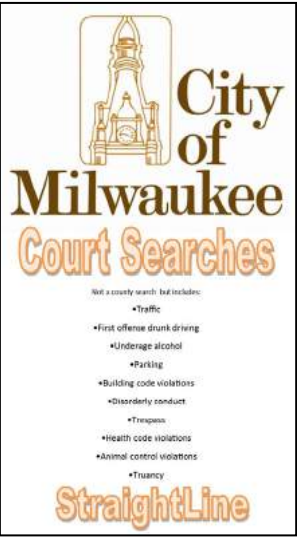
The data and privacy expert said companies buying data is not necessarily a bad thing, emphasizing this issue is nuanced.

“Often other organizations use that data in their fraud analytics, in their authentication process... however we need to be more transparent about it,” said Velasquez.

“People need to know if their data is being sold and to whom it is being sold and for what purpose,” she said.

“It is important to note DMV does not sell driver information for marketing purposes, or to generate revenue outside of the administrative cost of the program,” read a statement from the DMV.

“The DMV takes its obligation to protect personal information very seriously. Information is only released according to California law, and the DMV continues to review its release practices to ensure information is only released to authorized persons/entities and only for authorized purposes,” the statement continued.



Les Rosen's Corner

A monthly column
By Lester Rosen,
Attorney at Law



Written By ESR News Blog Editor
Thomas Ahearn

On November 18, 2019, the U.S. Equal Employment Opportunity Commission (EEOC) – which advances opportunity in the workplace by enforcing the federal laws prohibiting employment discrimination – announced that a major retail chain has agreed to pay \$6 million to settle a discrimination lawsuit filed by the EEOC that claimed the retailer's criminal background check process discriminated on the basis of race.

According to the lawsuit filed by the EEOC in U.S. District Court for the Northern District of Illinois in Chicago, Dollar General – the largest small-box discount retailer in the United States – violated Title VII of the Civil Rights Act of 1964 by denying employment to African American applicants at a significantly higher rate than white applicants for failing the company's broad criminal background check.

The three-year consent decree settling the lawsuit requires Dollar General to pay \$6 million into a settlement fund which will be distributed to African Americans who lost their chance at employment at the company between 2004 and 2019. Employment screens that have a disparate impact on the basis of race violate Title VII unless an employer can show the screen is job-related and is

a business necessity.

"Because of the racial disparities in the American criminal justice system, use of criminal background checks often has a disparate impact on African Americans. This consent decree reminds employers that criminal background checks must have some demonstrable business necessity and connection to the job at issue," EEOC Chicago District Director Julianne Bowman stated in a press release about the settlement.

If Dollar General uses a criminal background check during the three year consent decree, they must hire a criminology consultant to develop a new criminal background check based on time since conviction, number of offenses, nature and gravity of the offense, and risk of recidivism. Once a recommendation is given, the decree enjoins Dollar General from using any other criminal background check when hiring.

"This case is important because Dollar General is not just providing relief for a past practice but for the future as well. Unlike other background checks based on unproven myths and biases about people with criminal backgrounds, Dollar General's new approach will be informed by experts with knowledge of actual risk," Gregory Gochanour, regional attorney for EEOC's Chicago District, stated in the press release.

In April of 2012, the EEOC issued "Enforcement Guidance on the Consideration of Arrest and Conviction Records in Employment Decisions Under Title VII of the Civil Rights Act of 1964" that recommended if employers ask about criminal convictions that the "inquiries be limited to convictions for which exclusion would be job-related for the position in question and consistent with business necessity."

The EEOC enforces Title VII, which makes it illegal to discriminate against a person on the basis of race, color, religion, sex, or na-

tional origin. An employer may violate Title VII if its policy has a "disparate impact" of disproportionately screening out a Title VII-protected group without demonstrating the policy is job related for the position in question and consistent with "business necessity."

In cases involving a criminal history exclusion, the ruling in *Green v. Missouri Pacific Railroad* held that the three "Green factors" relevant to assessing whether an exclusion was job related for the position in question and consistent with business necessity were the nature and gravity of the offense, the time passed since the offense or completion of the sentence, and the nature of the job held or sought.


In 2013, a group of national civil and workers' rights organizations released a report entitled "Best Practice Standards: The Proper Use of Criminal Records in Hiring" that addressed the use of criminal records by employers during background checks. At-

torney Lester Rosen, founder and chief executive officer (CEO) of Employment Screening Resources® (ESR), helped develop these best practice standards.

Rosen also wrote a complimentary white paper entitled "Practical Steps Employers Can Take to Comply with the EEOC Criminal Record Guidance" that gives examples on what employers should do to remain in compliance with

EEOC Guidance when performing criminal background checks. ESR also offers a proprietary EEOC Compliance Toolkit that provides a set of software tools available only to ESR clients.




**criminal research
& investigation**

"My 'Go To' Vendor"

"supportive no matter what the request"

"completes the impossible"

"CRI is committed and extremely responsive to all my needs"

"My 'Yes' man" *"the staff is knowledgeable and resourceful"*

"pulling it all together so it makes sense" **"experts!"**

"when everyone else said No, CRI said Yes"

WHOLESALE BACKGROUND SCREENING WITH HIGHER STANDARDS
www.criscreening.com

In-Court Searches Done Right!

- > Top Provider for DC, DE, MA, NH, NJ, PA & RI
- > World-Class Customer Service, Cutting-Edge Technology, and Exceptional Attention to Detail
- > Trained, Knowledgeable Staff Available 24/7
- > Volume Discounts

County House Research, Inc.

A Public Information Research Company

County House Family of Companies...

County House Research, Inc.,
NH Background Investigations,
Security Consultants

Phone (215) 717-7433

Fax (215) 220-3476

www.CountyHouseResearch.com



What Gives, Appriss? The True Motivation Behind The Opioid Crisis- Profit Off PDMPs And Profiling, Private Data Theft

Part II of Profiling & Data Theft — Our “Clueless” Elected Officials are Filling Their Pockets at The Expense Of Patient Misery

WRITTEN BY Heather Wargo

Those Pesky States and their Statutes... That NO ONE Enforces Their Parameters...

If one stops to peruse the state laws on the books regarding PDMPs (prescription drug monitoring programs), there is an abundance of fascinating language buried in our very own state statutes.

For example, many states have what is called “Compacts” with other states.

These are statutes made in state law, usually over roadway or bridge construction, over licensure in nursing or medicine, with other states. They encompass an agreed upon number of states, have rules set governing etc..., have legal language with terms and so forth.

However, in regards to the Opioid Crisis... why would there even need to be a “Compact”?

And furthermore, why would this “Compact” be written like the one in Kentucky legislation has been?

Yes, here we are, back in Kentucky again- the land of Appriss, Inc., and their House of Rep. champion, Hal Rogers, of the “Hal Rogers PDMP programs”.

What a fascinating coincidence.

When I stumbled across this statute it was 2:30 am,

and I was in the throes of a horrendous pancreatic flare. Maybe these people will realize some will stop researching and chasing after their stupid machinations when they are not being harmed directly by them.

If I wasn’t being supposedly punished for idiotic actions of another, I would be able to sleep through a night.

I would have access to the medication appropriate for my condition, at the dose required and not have to worry about this ridiculous, evil, self serving propaganda play.

This crisis is really no more than a cleansing of America, as well as a dressed up profiteering of those in position to do so, at the expense of the seriously ill.

My sense of fury and outrage mounted as I read every sentence of the Kentucky Statute 218A.390 establishing the Prescription Monitoring Program Compact — not program. (This is a crucial difference).

I encourage every single person to read it, twice.

If you have any doubts about what the real motivation of the opioid crisis is after reading it; read it again.

It appears that stakeholder interests have more to do with this crisis than anything else, whoever plays the game the right way will make the most money.

No patients or their privacy was considered, unless it would “embarrass” a member state.

When HR 6, the expansive “Opioid Bill”, the Support for Patients and Communities Act, was signed by Pres. Trump on October 24, 2018, few people actually knew its entire contents.

Few realized it actually underfunded addiction treatment, yet again.

It put into place strict

and how it was to be carried out.

It granted extension of the “bupe” waiver and more freedoms for the drug Suboxone to be used in substance abuse treatment for Medicaid patients, a huge win for the pharmaceutical company Indivior.

As of this writing, there is still no generic for Suboxone (bupe).

It also expanded funding for PDMP (Prescription Drug Monitoring Program) databases.

A very few people understood that last bit.

Here Comes The Appriss Bit

Appriss Has Been Played

With the passing of HR 6, the company Appriss, Inc., began to feel a little concerned.

This little company, based in Louisville, KY, has enjoyed a secretive monopoly on PDMP algorithm programs utilized in every state system since their inceptions into the state systems.

Beginning in mid 1990’s with the Clinton White House, but helped along by the first Bush White House, with their encouragement of EHRs.

In the first of hundreds of non coincidental coincidences, push turned into hard shove right after President Clinton signed HIPAA into law.

HIPAA being the smoke and mirrors law that pretends to protect patient privacy.

At the rate of a whopping average of 2 whole convictions per year out of 350 million Americans.

Either the American people are extremely respectful of each other’s privacy in regards to medical information or no one is enforcing HIPAA law in any real way.

As much as I would like to believe the former, the truth is the latter.

No doubt Appriss is helped along by their behind the scenes relationship with Representative Hal Rogers, a House of Representatives official from their state of KY, the “Prince of Pork”, who just so happens to be the face man for their National PDMP grant system.

Did someone say coincidence?

His ‘Hal Rogers’ PDMP grants have been the sole reason most states were even able to implement a PDMP database to enroll patients in the first place.

Now... well... the government is moving in. They are going to fund things.

Rep. Rogers would not be able to wield the power he once did... if this were to come to pass.

Appriss Inc., executives also heard whispers that D.C. was considering making the PDMP a utility.

With the push toward a National PDMP and the certainty it will happen within the next decade, the government focus is now shifting toward whether or not the PDMP should be a public utility.

Still not a peep out of a single government official about privacy, patient consent, if PDMPs even actually work (not one study has shown a definitive yes on this), or if we need a National PDMP.

The CDC isn’t even able to say they work in stopping addiction and overdose.

Likely due to the fact PDMPs track the wrong people and wrong drugs.

A National PDMP utility would spell disaster for Appriss, Inc.

The huge checks would come to an end.

On the verge of receiving the Marconi treatment from

the government, it seems.

Appriss, Inc. is worried they will become a white elephant if the government takes over the PDMP.

The company has launched a media campaign to highlight themselves, because, in reality, they do have a strict monopoly on this trade in America.

I read a fascinating analysis of this from a anon hospital insider blog, though the post itself was written by David Finney, a partner at Leap Orbit- a healthcare consulting firm in Maryland. He writes:

“Appriss has done what monopolists do, bidding up contract prices and seeking to monetize every aspect of the data it controls. Given the commitment by states and the federal government to “do whatever it takes” to address the opioid epidemic—including supporting PDMPs with ever-increasing grant funds—PDMP administrators may grumble, but otherwise few people have stopped and taken much notice.”...

The article speaks of a National PDMP and then goes on to point out:

“By all indications, the federal omnibus spending bill and subsequent signals from federal officials and lobbyists seem poised to deliver on this new model. Not surprisingly, Appriss is worried. In recent weeks, it has launched a marketing campaign of its own to highlight the benefits of the current state-based approach to PDMPs and the interstate gateway it developed in collaboration with the National Association of Boards of Pharmacy....”

That has to sting.

When in doubt call
Straightline
1-866-909-6678

Continues next page ➔

This Appriss Thing, cont.

WRITTEN BY Heather Wargo

This is my take on this.

Basically, the government is giving Appriss the middle finger and a good doggie pat on the head.

Appriss Inc., will be another in a long line who has been played by our dear government, developed a program, only to have it stolen and used with no recourse.

I can't lie and say it isn't personally satisfying to see Appriss being treated... despicably...(like a patient) ... even though it underlines the treachery of our government in spades.

I will waste no more time reflecting on Appriss's potential loss here.

When you deal in deceit- you will have it dealt to you in the future.

When you get too greedy- it never works out.

Since the others in the game, Brandeis and Yale, have day jobs, it shouldn't hit them too hard.

Besides this site and a few other knowledgeable people, no one has said much about their connections to the PDMPs or the Opioid Crisis at all.

They haven't been connected in the public eye.

Furthermore, the Kentucky Compact will be a moot point if a national PDMP is created.

Bye bye to that huge money generator for all the states involved, and stakeholders- of which I am certain Appriss, Inc., is the biggest one.

Of course, the yearly reports that are required by the statute written in Kentucky law are no where to be found.

There is no public list of the members or stakeholders involved in the Ken-

tucky Prescription Monitoring Program Compact or any reports existing for review.

Finally.

Do we, as the patients who exist as members of the very lists involved in these databases, have a right to know who is viewing our protected, sensitive patient information?

What about informed consent?

Who asked us?

Is it right that our information is being traded to other states and stakeholders and profited off of— all without our informed consent?

Make no mistake- this has gone on for years. The Compact was created in 2012.

I wonder how much money has been made off this information in seven years already.

What will become of all the algorithm programs tailored to sell to all the states?

Does the average American understand what has happened in this power play around the Opioid Crisis?

The insurers have copycat algorithm programs now.

Appriss, Inc., has opened Pandora's box.

There are algorithm programs to tell your physician you need to lose weight, based on your BMI- a flawed system that has no clue of your bone density or muscle mass.

A bodybuilder will be flagged for obesity even with a body fat of 8%, if their weight to height ratio is too high.

There is NO INPUT mechanism on these programs.

This is what happens when you allow computers to practice medicine- and allow the companies to use

them without disclosing the fields they use for inputs.

Editor's Note: Appriss has since successfully integrated their PDMP with several States.

Are Hiring Algorithms Fair?

Time is money and, unfortunately for companies, hiring new employees takes significant time -- more than a month on average, research shows.

Hiring decisions are also rife with human bias, leading some organizations to hand off at least part of their employee searches to outside tech companies who screen applicants with machine learning algorithms. If humans have such a hard time finding the best fit for their companies, the thinking goes, maybe a machine can do it better and more efficiently.

But new research from a team of Computing and Information Science scholars at Cornell University raises questions about those algorithms and the tech companies who develop and use them: How unbiased is the automated screening process? How are the algorithms built? And by whom, toward what end, and with what data?

They found companies tend to favor obscurity over transparency in this emerging field, where lack of consensus on fundamental points -- formal definitions of "bias" and "fairness," for starters -- have enabled tech companies to define and address algorithmic bias on their own terms.

"I think we're starting to see a growing recognition among creators of algorithmic decision-making tools that they need to be particularly cognizant of how their tools impact people," said Manish Raghavan, a doctoral student in computer science and first author of "Mitigating Bias in Algorithmic Employment Screening: Evaluating Claims and Practices," to

be presented in January at the Association for Computing Machinery Conference on Fairness, Accountability and Transparency.

"Many of the vendors we encountered in our work acknowledge this (impact) and they're taking steps to address bias and discrimination," Raghavan said. "However, there's a notable lack of consensus or direction on exactly how this should be done."

The researchers scoured available public information to begin to understand these tools and what measures, if any, companies have in place to evaluate and mitigate algorithmic bias. Shielded by intellectual property laws, tech companies don't have to disclose any information about their algorithmic models for pre-employment screenings -- though some companies did choose to offer insight.

The researchers honed in on 19 vendors who specialize in algorithmic pre-employment screenings, which, they found, include questions, video interview analysis and games. They combed company websites, webinars and any available documents for insights into vendor claims and practices.

Very few vendors offer concrete information about how they validate their assessments or disclose specifics on how they mitigate algorithmic bias, researchers found.

"Plenty of vendors make no mention of efforts to combat bias, which is particularly worrying since either they're not thinking about it at all, or they're not being transparent about their practices," Raghavan said.

Even if they use such terms as "bias" and "fairness," these can be vague. A vendor can claim its assessment algorithm is "fair" without

revealing how the company defines fairness.

It's like "free-range" eggs, Raghavan said: There is a set of conditions under which eggs can be labeled free range, but our intuitive notion of free range may not line up with those conditions.

"In the same way, calling an algorithm 'fair' appeals to our intuitive understanding of the term while only accomplishing a much narrower result than we might hope for," he said.

The team hopes the paper will encourage transparency and conversation around what it means to act ethically in this domain of pre-employment assessments through machine learning.

Given the challenges, could it be that algorithms are just not up to the job of screening applicants? Not so fast, Raghavan said.

"We know from years of empirical evidence that humans suffer from a variety of biases when it comes to evaluating employment candidates," he said. "The real question is not whether algorithms can be made perfect; instead, the relevant comparison is whether they can improve over alternative methods, or in this case, the human status quo.

"Despite their many flaws," he said, "algorithms do have the potential to contribute to a more equitable society, and further work is needed to ensure that we can understand and mitigate the biases they bring."

Credit: <https://www.sciencedaily.com/releases->





England

Courthouses



**STRAIGHT
LINE**

More Hits

Whether It's England's Magistrates or Crown Courts Straightline's Got You Covered

For Background Screeners - no need for expensive, long waits, hard to get police or DBS clearances.

DBS clearances are not required for most employment purposes in England and absolutely not needed for employment purposes outside of England.

Court records are public, easy to get, some are even online!



<http://www.straightlineinternational.com/contact-us/>

1-866-909-6678