Threat Level
Privacy, Crime and Security Online

Newly Declassified Files Detail Massive FBI Data-Mining Project

By Ryan Singel  September 23, 2009  |  7:00 am  |  Categories: Sunshine and Secrecy, Threats, Watchlists

A fast-growing FBI data-mining system billed as a tool for hunting terrorists is being used in hacker and domestic criminal investigations, and now contains tens of thousands of records from private corporate databases, including car-rental companies, large hotel chains and at least one national department store, declassified documents obtained by Wired.com show.

Headquartered in Crystal City, Virginia, just outside Washington, the FBI’s National Security Branch Analysis Center (NSAC) maintains a hodgepodge of data sets packed with more than 1.5 billion government and private-sector records about citizens and foreigners, the documents show, bringing the government closer than ever to implementing the “Total Information Awareness” system first dreamed up by the Pentagon in the days following the Sept. 11 attacks.

Such a system, if successful, would correlate data from scores of different sources to automatically identify terrorists and other threats before they could strike. The FBI is seeking to quadruple the known staff of the program.

But the proposal has long been criticized by privacy groups as ineffective and invasive. Critics say the new documents show that the government is proceeding with the plan in private, and without sufficient oversight.
The FBI’s Data-Mining Ore

Composed of government information, commercial databases and records acquired in criminal and terrorism probes, the FBI’s National Security Branch Analysis Center is too broad to be considered mission-focused, but still too patchy to be Orwellian. Here’s the data we know about.

• **International travel records of citizens and foreigners**

• **Financial forms filed with the Treasury by banks and casinos**

• **55,000 entries on customers of Wyndham Worldwide, which includes Ramada Inn, Days Inn, Super 8, Howard Johnson and Hawthorn Suites**

• **730 records from rental-car company Avis**

• **165 credit card transaction histories from Sears**

• **Nearly 200 million records transferred from private data brokers such Accurint, Acxiom and Choicepoint**

• **A reverse White Pages with 696 million names and addresses tied to U.S. phone numbers**

• **Log data on all calls made by federal prison inmates**

• **A list of all active pilots**

• **500,000 names of suspected terrorists from the Unified Terrorist Watch List**

• **Nearly 3 million records on people cleared to drive hazardous materials on the nation’s highways**

• **Telephone records and wiretapped conversations captured by FBI investigations**

• **17,000 traveler itineraries from the Airlines Reporting Corporation**

“We have a situation where the government is spending fairly large sums of money to use an unproven technology that has a possibility of false positives that would subject innocent Americans to unnecessary scrutiny and impinge on their freedom,” said Kurt Opsahl, a lawyer with the Electronic Frontier Foundation. “Before the NSAC expands its mission, there must be strict oversight from Congress and the public.”
The FBI declined to comment on the program.

Among the data in its archive, the NSAC houses more than 55,000 entries on customers of the Cendant Hotel chain, now known as Wyndham Worldwide, which includes Ramada Inn, Days Inn, Super 8, Howard Johnson and Hawthorn Suites. The entries are for hotel customers whose names matched those on a long list the FBI provided to the company.

Another 730 records come from the rental car company Avis, which used to be owned by Cendant. Those records were derived from a one-time search of Avis’s database against the State Department’s old terrorist watch list. An additional 165 entries are credit card transaction histories from the Sears department store chain. Like much of the data used by NSAC, the records were likely retained at the conclusion of an investigation, and added to NSAC for future data mining.

It’s unclear how the FBI got the records. In the past, companies have been known to voluntarily hand over customer data to government data-mining experiments — notably, in 2002, JetBlue secretly provided a Pentagon contractor with 5 million passenger itineraries, for which it later apologized. But the FBI also has broad authority to demand records under the Patriot Act, using so-called “national security letters” — a kind of self-issued subpoena that’s led to repeated abuses being uncovered by the Justice Department’s inspector general.

Wyndham Worldwide did not respond to repeated requests for comment. Sears declined comment.

Wired.com’s analysis of more than 800 pages of documents obtained under our Freedom of Information Act request show the FBI has been continuously expanding the NSAC system and its goals since 2004. By 2008, NSAC comprised 103 full-time employees and contractors, and the FBI was seeking budget approval for another 71 employees, plus more than $8 million for outside contractors to help analyze its growing pool of private and public data.

A long-term planning document from the same year shows the bureau ultimately wants to expand the center to 439 people.

As described in the documents, the system is both a meta-search engine — querying many data sources at once — and a tool that performs pattern and link analysis. The NSAC is an analytic Swiss army knife.

The FBI used the system to locate a suspected Al Qaeda operative with expertise in biological agents who was hiding out in Houston. And when law
enforcement officials got information suggesting members of a Pakistani terrorist group had obtained jobs as Philadelphia taxi drivers, the NSAC was tapped to help the city’s police force run background checks on Philadelphia cabbies.

(A Jordanian-born Philly cab driver was convicted in 2008 for his part in a plot to attack the Fort Dix army base in New Jersey, but there’s no evidence of a connection between the investigations.)

And when the FBI lost track of terrorism suspects swept in the evacuation from Hurricane Katrina in 2005, it created a standing order in the system to flag any activity by the missing targets.

Additionally, the FBI shared NSAC data with the Pentagon’s controversial Counter-Intelligence Field Activity office, a secretive domestic-spying unit which collected data on peace groups, including the Quakers, until it was shut down in 2008. But the FBI told lawmakers it would be careful in its interactions with that group.

Conventional criminal cases have also benefited. In a 2004 case against a telemarketing company called Gecko Communications, NSAC used its batch-searching capability to provide prosecutors with detailed information on 192,000 alleged victims of a credit scam.

The feds suspected that Gecko had promised to help the victims improve their credit scores, and then failed to produce results. NSAC automatically analyzed the victims’ credit records to prove their scores hadn’t improved, a task that took two days instead of the four-and-a-half years that the U.S. Attorney’s Office had expected to sink into the job. In December 2006, the owners and seven office managers at the company were sentenced to prison.

The NSAC was born as two separate systems designed to improve information-sharing between government agencies following the Sept. 11 attacks. The Foreign Terrorist Tracking Task Force database has been used to screen flight-school candidates and assist anti-terror investigations. The Investigative Data Warehouse is the more general system, and is the principal element now under expansion.

“The IDW objective was to create a data warehouse that uses certain data elements to provide a single-access repository for information related to issues beyond counterterrorism to include counterintelligence, criminal and cyber investigations,” stated a formerly secret fiscal year 2008 budget request document. “These missions will be refined and expanded as these capabilities are folded into the NSAC.”

When the bureau unified the systems under the NSAC banner in 2007, the move set off alarm bells with lawmakers, who thought it sounded a lot like the Pentagon’s widely-criticized Total Information Awareness project, which had sought to identify terrorist sleeper cells by linking up and searching through U.S. credit card, health and communication databases. The TIA program had
moved into the shadows of the intelligence world after Congress voted to revoke most of its funding.

In 2007, Republican congressman James Sensenbrenner asked the Government Accountability Office to look into the NSAC. No report has been made public yet. But the documents obtained by Wired.com show that the FBI has repeatedly downplayed the databases’s capabilities when addressing critics in Congress, while simultaneously talking up — in budget documents — the system’s power to spit out the names of newly suspicious persons.

The FBI deflected criticism from a House committee on June 29, 2007, by pointing out a major difference between the NSAC and the shuttered TIA program: The NSAC, the bureau said, is not as open-ended. “A mission is usually begun with a list of names or personal identifiers that have arisen during a threat assessment, preliminary or full investigation,” the unsigned response read. “Those people under investigation are then assessed to determine if they have any association with terrorism or foreign espionage.”

But a formerly secret 2008 funding justification document among the newly released documents suggests the FBI’s pre-crime intentions are much wider that the bureau acknowledged.

The NSAC will also pursue “pattern analysis” as part of its service to the [National Security Branch]. Pattern analysis queries take a predictive model or pattern of behavior and search for that pattern in data sets. The FBI’s efforts to define predictive models ... should improve efforts to identify “sleeper cells.”

As an example, the FBI said its sophisticated data queries allowed it to identify 165 licensed helicopter pilots who came from countries of interest, and found that six of those had “derogatory” information about them in the NSAC computers. It sent the leads to FBI field agents in Los Angeles.

The FBI also has ambitious plans to expand its data set, the budget request shows. Among the items on its wish list is the database of the Airlines Reporting Corporation — a company that runs a backend system for travel agencies and airlines. A complete database would include billions of American’s itineraries, as well as the information they give to travel agencies, such as date of birth, credit card numbers, names of friends and family, e-mail addresses, meal preferences and health information.

So far, the company has given the FBI nearly 17,000 records, which are now part of NSAC. Spokesman Allan Mutén said the company gives the FBI records only when presented with a subpoena or a national security letter — which, he adds, has happened quite a bit. “Nine-eleven was a time and event that piqued the interest of the authorities in airline passenger data,” Mutén said.

The ever-growing size of the database concerns EFF’s Opsahl, who has pieced together the best picture of the FBI’s data mining system through other government FOIA requests.

Opsahl cites a October 2008 National Research Council paper that concluded
that data mining is a dangerous and ineffective way to identify potential terrorists, which will inevitably generate false positives that subject innocent citizens to invasive scrutiny by their government.

At the same time, Opsahl admits the NSAC is not at the moment the Orwellian system that TIA would have been.

“This is too massive to be based on a particular query, but too narrow to reflect a policy that they are going to out and collect this kind of data systematically,” Opsahl said.

That could change if the FBI gets it hands on the data sources on its 2008 wish list. That list includes airline manifests sent to the Department of Homeland Security, the national Social Security number database, and the Postal Service’s change-of-address database. There are also 24 additional databases the FBI is seeking, but those names were blacked out in the released data.

Graphic: Wired.com/Dennis Crothers

Story updated September 23, 2009 | 2:00 pm

See Also:

- [Data-Mining for Terrorists Not ‘Feasible,’ DHS-Funded Study Finds](http://www.wired.com/threatlevel/2009/09/fbi-nsac/)
- [Inside DCSNet, the FBI’s Nationwide Eavesdropping Network](http://www.wired.com/threatlevel/2009/09/fbi-nsac/)
- [Documents: FBI Spyware Has Been Sharing Extortionists, Hackers for Years](http://www.wired.com/threatlevel/2009/09/fbi-nsac/)
- [Funding for TIA All But Dead](http://www.wired.com/threatlevel/2009/09/fbi-nsac/)

Tags: data mining, FBI, nsac, terrorist watch list, tia

Post Comment  |  Permalink

Comments (44)

Posted by: galarant | 09/23/09 | 8:46 am

Oh no you guys, they have 165 credit card transaction histories from Sears! Imagine what they could do with that!

Posted by: DUSTOFF_CE | 09/23/09 | 9:04 am

You know who this will affect? No one you know. If you think this will affect you, or a family member, your wrong. I don’t care the gov’t in sifting through my hotel records, or CC charges because I have nothing to hide. I’m not renting a truck, buying 800lbs of fertilizer from four different sources and staying in a Hotel 8 for a week while renting a large storage space.
However, you know what does affect more people that no one seems to care about, and which does report personal information directly to the govt? Any state with a prescription monitoring program for controlled substances. I know more people who are hooked on prescription drugs than I do who want to blow up something.

Did anyone really think this wasn’t going on?

Gotta laugh at the slippery slope...things like this were implemented for terrorism, and already are being used in domestic cases. And of course we get the chorus of idiots: “Hey, as long as I am not doing something wrong, I don’t care if the government knows I ordered a butt plug from adult toys.com!” Yeah, until some bible thumper gets in office and declares all such things satan’s toys and lock you up as a sexual predator or some nonsense.

It’s a stretch to go from “I have nothing to hide so go ahead and read my credit card bills” to just throwing up your hands and relinquishing your right to privacy under the fourth amendment. Maybe you think your spending habits are no cause for alarm, but once you give up these rights, you no longer get to make that decision. What was once your private business is now the government’s business. And once they start connecting the dots — based on the system they designed and what behaviors they determine are dangerous — who really knows what kind of people may start getting locked up on the other end. Watch out rednecks, you might just get what you ask for.

Excellent bit of investigative journalism, Wired. Keep it up. Someone has to keep an eye on the people who are keeping an eye on us.

While I have the utmost respect for our law enforcement agencies, they consist
of fallible individuals like you and me. While I don’t think my name, which is pretty plainly the result of WASP-y heritage, is going to get mixed up with a Person of Interest with a “furriner” sounding name in the NSAC or that the research I do for my job, which often relates to transporting/disposing of regulated chemicals is going to raise a flag, it could. I’d just as soon not have to explain to my state’s Bar Association Ethics Board why the FBI investigated me for inquiring into 10,000 gallon LP tanks or have some poorly written piece of code flag my actions as “derogatory” to national security interests thus spurring a real invasion into my privacy as one group of law enforcement or another starts issuing national security letters to get access to my medical records, educational transcripts and buying habits. If the NSAC is as necessary as the FBI maintains, I’ll grudgingly accept that if, and only if, that information is acquired and collected through proper judicial channels. I’m a natural born US citizen who pays his taxes, votes and stays out of trouble...but in return, I expect that the protections afforded me by the framework of our government be respected even if it means some extra work drafting an affidavit of probable cause and presenting it to a FISA judge to request a warrant. That the government shall be limited in its reach into the private lives of the citizenry is a long-honored concept going back nearly a millenium to our British forebears; it is a concept I refuse to surrender.

---

Posted by: pilnomi | 09/23/09 | 11:49 am

This really doesn’t raise any alarms with the “I don’t mind, I’m not doing anything wrong” crowd? hrmnnn k. The obvious course of action is to boycott the companies on this list — there’s a line between cooperating with government and assisting it in illegal surveillance.

---

Posted by: jeiwest | 09/23/09 | 12:11 pm

<<<Misses the days for a court issued warrant/subpoena’s....

---

Posted by: piddlyd | 09/23/09 | 12:14 pm

Gifftor, it is just as likely that a giant NSA scrubbing web-crawler has collected your repeated, anti-patriotic posts of this nature, coallated the information in those posts to match your multiple different handles and nicks to your most likely real identity, and put that all on file to identify you as a possible subversive. Fortunately in the near future the FBI plans on implementing a system of 3 albino precogs in vats of water determining criminal activity.
before it happens - and they’re bound to bust you before you do anything.

I’ll see you in re-education camp... Cheers. 😑

---

Posted by: NoahB416 | 09/23/09 | 12:17 pm

The most serious danger with this system is that corrupt FBI agents or contractors abuse this system for personal profit. The opportunities to dig up dirt on political candidates, celebrities, well connected corporate insiders, or anyone else they could possibly think of a way to extort money from are ENDLESS.

Any system like this is going to be a gold mine for potential blackmailers, and it probably already is. They can extort money from just about anyone. For a cash payment, they can dig up dirt on high profile individuals and leak it to the press. They can use it to blackmail corporate insiders into revealing inside information. And that’s just scratching the surface.

---

Posted by: Giftor | 09/23/09 | 12:20 pm

@piddlyd - Ha! Want me to bring you a water-board? I figured I’d just bring my own. 😁

---

Posted by: rgb3 | 09/23/09 | 12:31 pm

Yes, this doesn’t affect us law-abiding citizens today. However history shows us that governments eventually abuse the power they are given. That is why privacy advocates cry fowl at every seemingly small intrusion on privacy. The Bush administration was known for using it’s power against its political opponents, although in a much simpler way. Now extrapolate out a few dozen years, and imagine the concerns.

---

Posted by: technophile | 09/23/09 | 12:36 pm

people worry about privacy but the fact that the records exist at all proves that
they are not private. If you want privacy then you go to use cash. The issue is fear of all the records being in just one groups hands (the government).

Posted by: muD | 09/23/09 | 1:56 pm

Repeat after me... “The FBI is not your friend... The FBI is not your friend..

Posted by: Bahlkris | 09/23/09 | 1:02 pm

Perhaps Wired should insert Bruce Schneier wonderful comparison of “Security v. Privacy” into this story. they should already have a copy of it since its been on wired more then once.

Posted by: tengobotas | 09/23/09 | 1:39 pm

“The FBI is seeking to quadruple the known staff of the program.” What are they going to do with the UNknown staff?

For those who place blame only on Bush for the warrantless wiretapping, Carnivore actually began under Clinton.

Posted by: NoahB416 | 09/23/09 | 1:45 pm

My understanding of Carnivore was that it was overwhelmed and plagued with problems almost from day one, and never did produce results. Still, it’s alarming that they would even be trying something like that, and it’s clear that Carnivore either laid the groundwork for the current NSA program or paralleled the NSA program while it was in development.

24.9.2009 21:00

Posted by: johnleb | 09/23/09 | 12:43 pm

Say you are stalking some nice girl. It takes a lot of work to do that effectively. Now say you have access to this database. While many of your basic stalking issues remain, you can keep an eye on her travel and finances. But you aren’t the stalking type? You just want to get laid? You can use the reverse directory and search it by obviously female names who live near you. Use the Newly Declassified Files Detail Massive FBI Data... http://www.wired.com/threatlevel/2009/09/fbi-nsac/
information from the credit bureaus and the Treasury to find out which ones are single, youngish and in financial trouble. Now that your names are down to a manageable number, start looking at Facebook to see what they look like. With a couple of well written queries you have found all of the financially vulnerable young women in your neighborhood. In the time it takes most people to get a cup of coffee you have just violated the privacy of your neighborhood.

* But say you are old, male and/or fat and don’t care about sexual deviants at the FBI. Those travel and financial datasets are political gold. A couple of queries and you can anonymously feed scandal after scandal to the right-wing or left-wing political group of your choice. While you are not quite a kingmaker, you can switch legislative seats at the local, state and maybe even federal level.

* And of course god forbid you are neighbors with one of these guys and you get into a neighborly dispute. You really better have nothing to hide.

Posted by: Jesus_Jenkins | 09/23/09 | 2:04 pm

In case you’ve been living under a rock, companies ARE allowed to collect personal information with the implied consent of the consumer. After that, they can pretty much do what they want with it, as a (probably unread) contract has been made between the consumer and the company, giving them a certain amount of free reign over what they do with that information (sell it to advertisers, quality control, etc.)

You need to look no further then the Privacy Policy of most major websites (including Wired).

Honestly, you kids are just lucky that the FBI is nice enough to actually disclose this evil Orwellian tyranny to the public. You can’t really be outraged about something you don’t know about, can you?

Posted by: bubbahotep | 09/23/09 | 2:11 pm

Could you please make a page with all the participating companies and their logos so we can start boycotting them?

We should spread that page around so everybody knows who is involved!

Posted by: bobnjersey | 09/23/09 | 2:27 pm

[Honestly, you kids are just lucky that the FBI is nice enough to actually disclose this evil Orwellian tyranny to the public. You can’t really be outraged about something you don’t know about, can you?]

the outrage should be that they’re lying about it ... and many other things as well ... like maybe justifications for starting wars?
Since you liked those quotes from Sunyjim, here’s one of my favs:

“If ye love wealth better than liberty, the tranquility of servitude better than the animating contest of freedom, go home from us in peace. We ask not your...
counsels or your arms. Crouch down and lick the hands which feed you. May your chains set lightly upon you, and may posterity forget that you were our countrymen.” - Samuel Adams

Hey meelk, here’s a novel concept: we could stop letting people who want to kill us immigrate into the country.

NoahB416, that’s exactly what Geronimo said!! 😁

Welcome back Wired! It’s good to see a real story on this site instead of the usual “10 most [blank]” articles that you guys have been churning out recently!

I haven’t seen a phrase like “Wired.com’s analysis of more than 800 pages of documents obtained under our Freedom of Information Act request” in your reporting in I don’t know how long.

I’ll put good money down that the first item on the “database wishlist” is the one from the US Census Bureau. It wouldn’t be the first time they tried to violate the Constitution to get information that is specifically forbidden to them. I’ll also hazard a guess that they want access to all immigration records, visas (not the credit card fool), and driver’s license databases right away.

@Dustoff ce: Well guess what. My father is a farmer, and yes we use diesel vehicles, and frequently purchase large amounts of fertilizer, often from different sources because we’re shopping for the best price. You know, to grow crops with. And since we often travel to farm equipment trade shows, etc. we do tend to stay in hotels. And move between states. And enter/exit Canada a LOT. And yes we have a lot of storage space rented in various places because it’s often cheaper to store some equipment there for a month than to build a permanent structure (and reduce space) on a field. If we start getting hassled at the border and bothered by the FBI it’s really going to piss us both off. It’s already pissed off a lot of other farmers who are pretty much the exact opposite of terrorists.

RAU Read And Understand
Amendment IV of the Constitution of the United States of America

The right of the people to be secure on their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath of affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

If you have a difficult time understanding these words and concepts, and why they directly support freedom and democracy in this country, simply imagine if these exact words did not exist. Is even this too difficult? Then using a computer and what is called an internet search engine, spend some time looking into the following: tyranny, fascism, communism, dictatorship, injustice, arbitrary detention, police state. In each of these examples, the 4th Amendment does not exist.

Read the following:

‘As an example, the FBI said its sophisticated data queries allowed it to identify 165 licensed helicopter pilots who came from countries of interest, and found that six of those had “derogatory” information about them in the NSAC computers. It sent the leads to FBI field agents in Los Angeles.’

In a well worded and decisive argument, please explain How In The Fuck subjecting 165 people to a search if only 6 are actually under suspicion is legal under the 4th. Amendment. Will you argue that simply being from “countries of interest” equates to probable cause? Fine, then justify why being Jewish was legitimate probable cause in Nazi Germany. And please keep in mind that in order to get the “165 licensed helicopter pilots from countries of interest”, an even larger pool of licensed helicopter pilots that were and were not from countries of interest had to be subjected to filter and search. What was the probable cause there? Being a helicopter pilot?

No, the following is NOT an argument for anything: “I don’t mind if they search my stuff.” Given what’s at stake, for all those words are worth you might as well have said “I don’t mind if they like my curtains.” If you want a police state, then get off your damn ass and make an argument for it. That’s all I’m asking.

Posted by: technophile | 09/23/09 | 6:24 pm

Add Facebook, You’re toast. 6 degrees is the gold mine.

Posted by: Axio | 09/23/09 | 7:53 pm

The slow creep of government surveillance and control in the name of “security” for citizens is a cancer. It starts slowly, bit by bit, accumulating scope, pervasiveness, and tenacity. At any given point, when properly whitewashed for citizen consumption, any new step towards statism seems
slight compared to the current situation, but when seen from a long view, the
curve of that cancerous growth is alarming. I’m honestly depressed that the
masses don’t realize that excuses such as “its for your safety”, “its to protect
against child pornography”, “its to protect America” are all child-level farces
barely covering the fundamental spread of Control.

---

Posted by: Clarpet | 09/23/09 | 8:42 pm

First I have to point this out:
quote from above:
“• A reverse White Pages with 696 million names and addresses tied to U.S.
phone numbers

• Log data on all calls made by federal prison inmates”

Both of these have been in existence for a very long time. Try anyone of the
phone directories online and use what’s called “Reverse Lookup”. If you have a
listing or have every been listed, even cell phone numbers in some cases, you
can be found, right now, by ANYone who has the internet. Not a big deal. Its
called a phone book.

Logging phone calls in prisons has been done for YEARS and the only
difference is that the info is directly available to the FBI rather than having to
request it from the prison.

Lastly, I’ll just say the same thing I always say to this type of issue: if you look
at the list in gray (the one I quoted from) you’ll see that NONE of that
information has any relevance unless you are suspected of some serious crime,
so unless you’ve done something to cause the FBI to take an interest, who
cares?

And the blow-hards that say “its my private info..” blah blah... its useless
private info that anyone could obtain anyway that you shouldn’t care to hide,
regardless of rights, unless you have a reason to...and if you have a reason,
then it must be criminal.

@Gifftor: frankly, if you or anyone else is purchasing 10,000 LP tanks, then
I’m damn glad someone of authority knows so they don’t end up in the wrong
hands. You should HAVE to explain something like that if asked. If you have a
valid reason, and documentation to back it up, which if legal you would, then
you have nothing to worry about.
As a former Revenue Agent we use to do these things daily back in the 80’s! We even purchased big reel to reel data machines because we had so much data to work with… and we were only looking for people that were not reporting their income selling scrap steel. The feds have been doing this since the beginning of the computer system. I am not supporting it, I am just saying. And you don’t think they are using that data to hold things against a person or

What bothers me is that Americans, my fellow citizens can only say that government widespread surveillance “doesn’t bother them”, that they have nothing to hide. They normally do this using very poor English. There’s a reason for that. It’s only the stupid ones who can’t see the negative possibilities. In these comments, many negative possibilities have been enumerated. The philosophy of why the government watching everyone’s every action is bad has been laid out.

If you have a large amount of transactions from daily life going into a database that is dynamically query able (doesn’t look like the DB is very well fed in this case), how is that any different than having a constant government wiretap on your house? Most of us would see no immediate affect on our lives, granted. That still does not mean that it doesn’t have far-reaching effects on our lives. How could you make sure that a small group of political operatives doesn’t maintain moles in the office with access to the information? How would you know that the scandals coming into the news were even getting information from that DB?

How would you know which side was getting the benefit of those scandals? Do you know what this would mean for you as the voter? You would hear all the negatives of one side, the negatives which you think are morally disgusting, but which don’t affect you financially. Meanwhile, you’re getting fleeced because with this new advantage, the side with the capability to get at all the scandals no longer has to give you as good of a deal. That’s just the more innocent of the possible negative outcomes.

As a former Revenue Agent we use to do these things daily back in the 80’s! We even purchased big reel to reel data machines because we had so much data to work with... and we were only looking for people that were not reporting their income selling scrap steel. The feds have been doing this since the beginning of the computer system. I am not supporting it, I am just saying. And you don’t think they are using that data to hold things against a person or
Dustoff said “You know who this will affect? No one you know. If you think this will affect you, or a family member, your wrong.”

I am sorry to say that you are wrong. This affects everyone with a drivers license.

I was sent a renewal form for my drivers license. I paid the fees but the license never came. I contacted the DMV and they said the license had a hold on it. I asked them why.

The DMV told me that two other states had put a hold on my license. I said “What?” They said that there was a federal database that connected all the states drivers license. You cannot get a drivers license unless all 50 states say you can get one.

I said “I just renewed my license a few years ago and this was not a problem”. They said “Yes. The federal database is new.”. This system Wired is talking about must be the database the DMV people are talking about.

I contacted the other two states. Would you believe one of them said I had a ticket from 15 years ago! I said “Isn’t there a statute of limitations?” They said “No”. I said “If I committed a crime 15 years ago, the statute of limitations would mean I was free of the crime. But you want me to pay this 15 year old ticket?”. They said “Yes”.

The other state, I still cannot believe it, said I owed them $10 from 20 years ago! So if you have ever received any kind of traffic ticket in any of the 50 states in the United States in the past 20 years, you are not going to be able to renew your drivers license the next time until you pay all of those citations.

Anyone who travels knows that small towns set up speed traps and write other unjust tickets to supplement their budgets. It used to be that you could get away from those criminals issuing false tickets for budgetary reasons by leaving their state. Not anymore. Those small towns can now flag your license in your home state so it will not be renewed until you pay the speed trap ticket in the other state.
Dustoff is wrong about this federal database not affecting regular people. This federal database affects everyone in the United States who drives a car.