STOP AND FRISK STOPPED! [UPDATED]

[Note **Update** below]

In a rather remarkable decision just handed down by Judge Shira Scheindlin in the Southern District of New York (SDNY), has found New York City's insidious stop and frisk policy violative of citizen's basic Constitutional rights. From the NYT:

> In a decision issued on Monday, the judge, Shira A. Scheindlin, ruled that police officers have for years been systematically stopping innocent people in the street without any objective reason to suspect them of wrongdoing. Officers often frisked these people, usually young minority men, for weapons or searched their pockets for contraband, like drugs, before letting them go, according to the 195-page decision.
>
> These stop-and-frisk episodes, which soared in number over the last decade as crime continued to decline, demonstrated a widespread disregard for the Fourth Amendment, which protects against unreasonable searches and seizures by the government, according to the ruling. It also found violations with the 14th Amendment.
>
> To fix the constitutional violations, Judge Scheindlin of Federal District Court in Manhattan said she intended to designate an outside lawyer, Peter L. Zimroth, to monitor the Police Department's compliance with the Constitution.

The full decision and order is here.

This is a very strong decision, and it is based

on trial evidence and specific findings of fact and conclusions of law that should give it some extra protection, compared to a straight legal decision alone, should the city appeal to the 2nd Circuit.

The court found that the practice violated both the 4th and 14th Amendments and denied equal protection. In so doing, the court basically confirmed that New York City had a standing policy that constituted blatant racial profiling. The court noted, in reference to the City's belligerent defense of such an unconstitutional policy:

> City acted w/deliberate indifference toward NYPD's practice of making unconstitutional stops and conducting unconstitutional frisks.

The "Applicable Law" portion contained in pages 15-30 (by the court's page numbering) is a hornbook primer on *Terry* stops and reasonable suspicion.

A few words from the court will close out this post:

> New Yorkers are rightly proud of their city and seek to make it as safe as the largest city in America can be. New Yorkers also treasure their liberty. Countless individuals have come to New York in pursuit of that liberty. The goals of liberty and safety may be in tension, but they can coexist – indeed the Constitution mandates it.
>
> ….
>
> In conclusion, I find that the City is liable for violating plaintiffs' Fourth and Fourteenth Amendment rights. The City acted with deliberate indifference toward the NYPD's practice of making unconstitutional stops and conducting unconstitutional frisks. Even if the City had not been deliberately

> indifferent, the NYPD's unconstitutional practices were sufficiently widespread as to have the force of law. In addition, the City adopted a policy of indirect racial profiling by targeting racially defined groups for stops based on local crime suspect data. This has resulted in the disproportionate and discriminatory stopping of blacks and Hispanics in violation of the Equal Protection Clause. Both statistical and anecdotal evidence showed that minorities are indeed treated differently than whites. For example, once a stop is made, blacks and Hispanics are more likely to be subjected to the use of force than whites, despite the fact that whites are more likely to be found with weapons or contraband. I also conclude that the City's highest officials have turned a blind eye to the evidence that officers are conducting stops in a racially discriminatory manner. In their zeal to defend a policy that they believe to be effective, they have willfully ignored overwhelming proof that the policy of targeting "the right people" is racially discriminatory and therefore violates the United States Constitution. One NYPD official has even suggested that it is permissible to stop racially defined groups just to instill fear in them that they are subject to being stopped at any time for any reason – in the hope that this fear will deter them from carrying guns in the streets. The goal of deterring crime is laudable, but this method of doing so is unconstitutional.

Bravo Judge Scheindlin, and thank you.

More like this please; the federal courts of America owe the citizens the duty of reeling in 4th Amendment abuses by governmental entities. This is a start, but the Obama Administration's

surveillance programs demonstrate there is a very long way to go.

UPDATE: I neglected to include the separate "Remedies Opinion" issued by Judge Scheindlin, here is the link for that.

A few words from the court about the intransigence of NYC and NYPD:

> I have always recognized the need for caution in ordering remedies that affect the internal operations of the NYPD, the nation's largest municipal police force and an organization with over 35,000 members. I would have preferred that the City cooperate in a joint undertaking to develop some of the remedies ordered in this Opinion. Instead, the City declined to participate, and argued that "the NYPD systems already in place" – perhaps with unspecified "minor adjustments" – would suffice to address any constitutional wrongs that might be found. I note that the City's refusal to engage in a joint attempt to craft remedies contrasts with the many municipalities that have reached settlement agreements or consent decrees when confronted with evidence of police misconduct. (footnotes omitted)

The defendant NYC and NYPD are very much not going to like Judge Scheindlin's remedies and, thus, likely will appeal on that basis. As I said above, the decision itself looks pretty solid for appeal, the remedies may be another matter. Professor Orin Kerr thinks the court may have gone too far in broad scope based on this paper he previously authored on 4th Amendment remedies in 2009.

I am a big fan of Professor Kerr's 4th Amendment analysis, but we occasionally differ. And we differ here. My review of Judge Scheindlin's remedies and order reflects a set of cures targeted and appropriate in purpose, and broad

only where necessary to effect said purpose (with possible exception of order to wear cameras). We shall see how they hold up on appeal, but the remedies look proper and necessary to me.

CHUCK SCHUMER MUST WANT ALL AMERICAN BROWN YOUTH STOP AND FRISKED

I thought Chuck Todd was speculating in that beltway fashion when he said he had heard people suggest Ray Kelly should replace Janet Napolitano as Department of Homeland Security Secretary.

But apparently, Chuck Schumer actually thinks it's a good idea.

> It's leader needs to be someone who knows law enforcement, understands anti-terrorism efforts, and is a top-notch administrator, and at the NYPD, Ray Kelly has proven that he excels in all three. As a former head of the Customs and Border patrol, he has top-level federal management experience. There is no doubt Ray Kelly would be a great DHS Secretary, and I have urged the White House to very seriously consider his candidacy.

Not only is this a batshit crazy idea because of all the authoritarian things Ray Kelly has done in NYC, from harassing hundreds of thousands of African American and Latino youths to spying on Muslims.

But note how Schumer doesn't mention the other,

equally important part of Homeland Security: keeping the country safe from things like Chinese hackers and natural disasters.

How’d Kelly do at organizing a response to Hurricane Sandy? Maybe we should ask Occupy Sandy about that?

TONY BOLOGNA, JOHN PIKE, AND STOP AND FRISK: A BAD COUPLE OF DAYS FOR ABUSIVE COPS

In a move that might make cops think twice before they go nuts on kettled protestors, NYC has decided not to defend Anthony Bologna, the officer filmed spraying defenseless protestors with pepper spray in NY.

> New York City has distanced itself from a high-ranking police official accused of firing pepper spray at Occupy Wall Street protesters, taking the unusual step of declining to defend him in a civil lawsuit over the incident.
>
> The decision means Deputy Inspector Anthony Bologna also could be personally liable for financial damages that may arise out of the suit, said lawyers familiar with similar civil-rights claims.

Because Bologna accepted the findings of an internal investigation finding him in violation of department guidelines, it appears, the city has space to say pepper-spraying docile protestors is not his job.

In even better news, John Pike—the UC Davis cop filmed spraying peaceful protestors with pepper spray—got fired, in spite of an internal review finding he acted reasonably.

> The police chief at the University of California, Davis overruled an internal affairs panel's recommendation and fired a lieutenant who soaked demonstrators with pepper spray – an incident that sparked protests after it was recorded and posted online, according to documents obtained by a McClatchy-Tribune newspaper.
>
> The Sacramento Bee (http://sacb.ee/MABZrq) reports that investigators concluded Lt. John Pike acted reasonably during the Nov. 18 campus protest and should face demotion or suspension at worst.
>
> But police Chief Matthew Carmichael rejected those findings and wrote Pike on April 27 that he planned to fire him. Pike, 39, was fired Tuesday, according to the Bee.
>
> "The needs of the department do not justify your continued employment," Carmichael wrote in a letter to Pike, according to the documents, which included the internal affairs investigation report.

I'm curious about the delay between the time Carmichael decided to fire Pike and the time it was official, Tuesday. Hopefully, that time was spent insulating the university against suit.

Finally, there are preliminary reports that the number of stop and frisks in NYC have dropped significantly as the sheer scale of the abusive practice has become clear.

> Officers conducted about 134,000 stop-and-frisks between April 1 and June 30, down from more than 200,000 during the

> first three months of the year.

That’s still too many. But sunshine and embarrassment seems to be making progress there, too.

Update: In related news, the 2004 RNC protestors suing for false arrest and other abuses just won class action status.

THE INTRANSITIVE CORRUPTION OF THE OATH KEEPERS

In a ruling affirming DOJ’s application of “obstruction” to the January 6 riot, Judge Amit Mehta ruled that “corruptly” in 18 USC 1512(c)(2) is intransitive, meaning defendants themselves must have had the intent of acting corruptly.

DABNEY FRIEDRICH REJECTS CHALLENGE TO JANUARY 6 OBSTRUCTION APPLICATION

In the first opinion assessing DOJ’s novel application of obstruction in January 6 prosecutions, Trump appointee Dabney Friedrich upheld DOJ’s approach.

WILL THE DRAGNET REFORM CRIMINALIZE ORDERING PIZZA?

There are two major problems with the phone dragnet, as it currently exists.

First, the government has a database of all the phone-based relationships in the United States, one they currently (as far as we know) do not abuse, but one that is ripe for unbelievable abuse.

But there is current abuse going on. The dragnet takes completely innocent people who are three (now two) degrees of separation from someone subjected to a digital stop-and-frisk, a very low standard, and puts them (by dint of at least one communication with someone who communicated with someone who might be suspicious) into the NSA's analytical maw. Permanently. Those people can have their multiple IDs connected, including any online searches NSA happened to injest, they can be subjected to data mining, by dint of those conversations, they apparently can even have the content of their communications accessed without a warrant, they might even be targeted to become informants using the data available to NSA.

This may well be the digital equivalent of J Edgar Hoover's subversives list, a collection of people who will always be subject to heightened scrutiny, including unbelievably invasive digital analysis, because of a three degree association years in the past.

According to PCLOB's estimate, as many as 120 million people may have been — may still be! — subjected for this treatment.

Discussions of whether the House Judiciary and Intelligence Committee bills "reforming" the

dragnet really fix it have almost entirely ignored this second abuse, the innocent people who will be subjected to the "full range of NSA's analytical tradecraft" merely because of a potentially completely innocent association.

There are things that should be done — whether in the current dragnet or the "reformed" one — to mitigate this abuse. Those data ought to age off, which they currently don't (and won't, under the new program, as currently described). That analysis ought to be subject to audits, which they're not currently. The FISC ought to get some sense of what happens in this corporate store, which it's not clear it currently has. Criminal defendants ought to have some visibility into whether their prosecutions stemmed from such analysis.

But there are also things — as Congress crafts a dragnet replacement — that can affect the sheer number of new people who will be thrown into the corporate store, into NSA's analytical pool. And those things have a lot to do with how this new scheme deals with what is called "data integrity."

As I have written repeatedly, the number of results NSA (or the telecoms, under the new system) will get under a particular query depends on how many noisy numbers — things like telemarketers, voice mail numbers, and pizza joints — remain in the collection. As Jonathan Mayer showed, even in his 300 person dataset that included just 2 people who had ever called each other, 17% were connected at the second hop through T-Mobile's voice mail number.

> In spite of the fact that just 2 of its participants had called each other, the fact that so many people had called T-Mobile's voicemail number connected 17% of participants at two hops.
>
> > Already 17.5% of participants are linked. That makes intuitive sense—many Americans use T-Mobile for mobile phone service,

> > and many call into voicemail. Now think through the magnitude of the privacy impact: T-Mobile has *over 45 million subscribers in the United States*. That's potentially tens of millions of Americans connected by just two phone hops, solely because of how their carrier happens to configure voicemail.
>
> And from this, the piece concludes that NSA could get access to a huge number of numbers with just one seed.
>
> > But our measurements are highly suggestive that many previous estimates of the NSA's three-hop authority were conservative. Under current FISA Court orders, the NSA may be able to analyze the phone records of a sizable proportion of the United States population with just one seed number.

We know NSA currently does significant work to pull those noisy numbers via a "data integrity" process both before new data is used for contact chaining and as new numbers are identified as "high volume numbers." While we don't get to assess the efficacy of that process, it can make the difference between hundreds of millions of Americans getting thrown into the NSA's analytical pool, or just tens of thousands. But as the contact-chaining process gets outsourced to the telecoms, the question becomes more pressing.

As I see it, there are three possible ways this function might be done going forward:

1. The telecoms do an initial sort of high volume numbers, taking out voice mail box

and telemarketer calls, then pass the data onto NSA, which does a secondary sort to pull out things like pizza joints (which NSA might want to keep in the data set, but suppress in contact chaining until they have evidence a pizza joint might be a key hub in a terrorist attack). This plays to existing telecom strengths (most likely do similar analysis on their own use of the data now), but doesn't require they make what are analytical intelligence decisions. Even though this is likely the best solution, it still means many completely innocent Americans may be subject to NSA's analysis because they ordered pizza.

2. The telecom does all the data integrity analysis, identifying all the high volume numbers. This would result in the fewest number (but still intolerably too many) of innocent Americans being dumped into NSA's pot. But it would also turn the telecoms into an arm of US intelligence (well, even more than they already are!), because they'd be in

the position of making analytical judgments about what data is useful for NSA's intelligence purposes. Which may be one of the reasons the telecoms seem to be demanding immunity, again.

3. NSA does the data integrity analysis at the telecoms, as seems to be envisioned by the HPSCI bill. This might achieve the current status quo, borrowing on 8 years of experience to strike the right balance. But it would also present the intolerable condition of NSA employees or contractors accessing and analyzing the raw data of private communications providers at the providers' locales.

When I asked a White House Senior Administration Official back in March how this function would be done, she had no answer (though it sounded like the government might ask the telecoms to do all of this).

> Under the President's proposal, the government would seek court orders compelling the companies to provide technical assistance to ensure the information can be queried, to run the queries, and to give the records back to the government in a usable format and on a timely basis. As additional questions arise with respect to the proposal, we look forward to working through them with Congress and relevant

> stakeholders to craft legislation that embodies the key attributes of this new approach.

That is, the White House is leaving it to Congress to deal with this, but thus far this is the extent of the discussion of its resolution in the two bills:

HPSCI

> [T]he Attorney General and the Director of National Intelligence may direct, in writing, an electronic communications service provider to –
>
> (A) immediately provide the Government with records, whether existing or created in the future, in the format specified by the Government and in a manner that will protect the secrecy of the acquisition;
>
> [snip]
>
> The Government may provide any information, facilities, or assistance necessary to aid the electronic communications service provider in complying with a directive issued pursuant to paragraph (1).

HJC

> [Orders will] direct each person the Government directs to produce call detail records under the order to furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production;

While there are hints of this question in this language (and the SAO I asked about it seemed aware the issue existed), no one is explicitly discussing who will ensure that hundreds of millions of completely innocent Americans aren't sucked up because they checked their voice mail or ordered a pizza.

And with language like this (from the HJC bill), it leaves open the possibility the numbers of innocent people who have their data handed to NSA — because they are, by definition, relevant to an investigation — will be kept and analyzed forever.

> (v) direct the Government to destroy all call detail records produced under the order not later than 5 years after the date of the production of such records, except for records that are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism.

There are many things that need to be fixed in these bills — including the language on how long the NSA can keep and analyze potentially innocent data handed over because of query noise.

But Congress needs to be cognizant that this very basic question — who cleans up the data — will have a potentially enormous impact on how abusive this program will be going forward. Because if they're not, it is easily conceivable that **more** completely innocent people will be subjected to NSA's analytical might than currently happens under the dragnet.

Update: Interesting. HPSCI just released a managers amendment that adds language on providing facilities:

> '(ii) information, facilities, or assistance necessary to provide the records described in clause (i);

That seems to be a change from the government providing assistance, above.

"FACTS MATTER" SAID NSA YAY-MAN MICHAEL HAYDEN WHO TOLD SERIAL LIES ABOUT THE PHONE DRAGNET

I'm not sure if you saw last night's Munk Debate pitting Glenn Greenwald and Alexis Ohanian against Michael Hayden and Alan Dershowitz. I did a whole slew of fact checking and mockery on twitter last night.

But I wanted to pay particular attention to a string of false claims Hayden made about the phone dragnet program.

First, my hobbyhorse, he claimed the database can only be used for terror. (After 1:08)

> If this program — and here we're talking about the metadata program — which is about terrorism, because the only reason you can use the metadata is to stop terrorism. No other purpose.

Actually, terrorism and … Iranian "terrorism." It's unclear when or why or how Iran got included in database access (though it is considered a state sponsor of terror). But according to Dianne Feinstein and Keith Alexander, analysts can also access the database for Iran-related information. Now, maybe they can only access the Iran data if they claim terror. But that's a very different thing than claiming a tie to al Qaeda.

The real doozies come later (my transcription;

after 1:20:40; I've numbered the false claims and provided the "facts matter" below).

> I started out with facts matter. So I assume on the metadata issue we're talking about the 215 program. About the phone records, alright? Because frankly, that's the only bulk metadata NSA has on American citizens. **(1)**
>
> [cross talk]
>
> Accusations fit on a bumper sticker. The truth takes longer. NSA gets from American telephone providers the billing records of American citizens. **(2)** What happens to the billing records is actually really important. I didn't make this phrase up but I'm gonna use it. They put it in a lock box, alright? They put it in a lock box at NSA. **(3)** 22 people at NSA are allowed to access that lockbox. **(4)** The only thing NSA is allowed to do with that truly gajillion record field sitting there is that when they have what's called a seed number, a seed number about which they have reasonable articulable suspicion that that seed number is affiliated with al Qaeda – you roll up a safe house in Yay-Man, he's got pocket litter, that says here's his al Qaeda membership card, he's got a phone you've never seen before. Gee, I wonder how this phone might be associated with any threats in the United States. **(5)** So, I'll be a little cartoonish about this, NSA gets to walk up to the transom and yell through the transom and say hey, anybody talk to this number I just found in Yay-Man? And then, this number, say in Buffalo, says well, yeah, I call him about every Thursday. NSA then gets to say okay Buffalo number – by the way, number, not name – Buffalo number, who did you call. At which point, by description the 215 metadata program

> is over. That's all NSA is allowed to do with the data. There is no data mining, there's no powerful algorithms chugging through it, trying to imagine relationships. **(6)** It's did that dirty number call someone in the United States. The last year for which NSA had full records is 2012 — I'll get the 13 numbers shortly **(7)** — but in 2012, NSA walked up to that transom and yelled "hey! anybody talk to this number?" 288 times. **(8)**

(1) Under the SPCMA authority, NSA can include US persons in contact-chaining of both phone and Internet metadata collected overseas. SPCMA has far fewer of the dissemination and subject matter limitations that the Section 215 dragnet has.

(2) NSA doesn't get the "billing records." It gets routing information, which includes a great deal of data (such as the cell phone and SIM card ID and telecom routing information) that wouldn't be included on a phone bill, even assuming a bill was itemized at all (most local landline calls are not). It also gets the data every day, not every month, like a billing record.

(3) Starting in early January 2008, NSA made a copy of the dragnet data and "for the purposes of analytical efficiency" dumped it in with all their other metadata. That allows them to conduct "federated queries," which is contact chaining across authorities (so chains including both foreign collected EO12333 data and domestic Section 215 data). The NSA coaches its analysts to rerun queries that are replicable in EO12333 alone because of the greater dissemination that permits.

(4) The 22 number refers to the people who can approve an identifier for Reasonable Articulable Suspicion, not the people who can conduct queries. Those 22 are:

> the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate.

While we don't know how many analysts are trained on Section 215 dragnet right now, the number was 125 in August 2010.

But even those analysts are not the only people who can access the database. "Technicians" may do so too.

> Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, but the results of any such queries ill not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes.

And this access — which requires access to the raw metadata — is not audited.

(5) Note, in the past, the government has also accessed the database with "correlated" identifiers — phone numbers and SIM cards associated with the same person. It's unclear what the current status of querying on correlated identifiers is, but that is likely the topic of one of the FISC opinions the government is withholding, and the government is withholding the opinion in question in the name of protecting an ongoing functionality.

(6) Hayden pretends there's a clear boundary to this program, but even the FISC minimization procedures for it approve the corporate store, where these query results — people 2 degrees from someone subjected to a digital stop-and-frisk — may be subjected to "the full range of [NSA's] analytic tradecraft." So when Hayden says there's no data mining and no powerful algorithms, he's lying about the data mining and powerful algorithms (and content access) that are permitted for identifiers in the corporate store.

(7) Given that DOJ has already released their numbers for FISA use in 2013, I presume it also has the number of identifiers that have been queried.

(8) The 288 number refers to the number of identifiers queried, not the number of queries run. Given that the dragnet serves as a kind of alert system — to see who has had contracts with a certain number over time — the number of actual queries is likely significantly higher, as most of the identifiers were likely run multiple times.

DOJ SAYS YOU CAN'T KNOW IF THEY'VE USED

THE DRAGNET AGAINST YOU … BUT FISC SAYS THEY'RE WRONG

As I noted the other day in yet another post showing why investigations into intelligence failures leading up to the Boston Marathon attack must include NSA, the government outright refuses to tell Dzhokhar Tsarnaev whether it will introduce evidence obtained using Section 215 at trial.

> Tsarnaev's further request that this Court order the government to provide notice of its intent to use information regarding the ". . . collection and examination of telephone and computer records pursuant to Section 215 . . ." that he speculates was obtained pursuant to FISA should also be rejected. Section 215 of Pub. L. 107-56, conventionally known as the USA PATRIOT Act of 2001, is codified in 50 U.S.C. § 1861, and controls the acquisition of certain business records by the government for foreign intelligence and international terrorism investigations. It does not contain a provision that requires notice to a defendant of the use of information obtained pursuant to that section or derived therefrom. Nor do the notice provisions of 50 U.S.C. §§ 1806(c), 1825(d), and 1881e apply to 50 U.S.C § 1861. Therefore, even assuming for the sake of argument that the government possesses such evidence and intends to use it at trial, Tsarnaev is not entitled to receive the notice he requests.

This should concern every American whose call records are likely to be in that database, because the government can derive prosecutions — which may not even directly relate to terrorism

– using the digital stop-and-frisk standard used in the dragnet, and never tell you they did so.

Note, too, Dzhokhar's lawyers are not just asking for phone records, but also computer records collected using Section 215, something Zoe Lofgren has made clear can be obtained under the provision.

And in the case in which Dzhokhar's college buddies are accused of trying to hide his computer and some firecracker explosives, prosecutors profess to be unable to provide any of the text messages Dzhokhar sent after his last text to them. That stance seems to pretend they couldn't get at least the metadata from those texts from the phone dragnet.

The government, then, claims that defendants can't have access to data collected using Section 215. They base that claim on the absence of any language in the Section 215 statute, akin to that found in FISA content collection statutes, providing for formal notice to defendants.

But at least in the case of the phone dragnet, that stance appears to put them in violation of the dragnet minimization procedures. That's because since at least September 3, 2009 and continuing through the last dragnet order released (note, ODNI seems to be taking their time on releasing the March 28 order), the minimization procedures have explicitly provided a way to make the query results available for discovery. Here's the language from 2009.

> Notwithstanding the above requirements, NSA may share information derived from the BR metadata, including U.S. person identifying information, with Executive Branch personnel in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings.

The government routinely points to these very

same minimization procedures to explain why it can't provide information to Congress or other entities. But if the minimization procedures trump other statutes to justify withholding information, surely they must have the weight of law for disclosure to criminal defendants. And all that's before you consider the Brady and Constitutional reasons that should trump the government's interpretation as well.

Using the formulation the government always uses when making claims about the dragnet's legality, on at least 21 occasions, FISC judges have envisioned discovery to be part of the minimization procedures with which the government must comply. At least 7 judges have premised their approval of the dragnet, in part, on the possibility exculpatory information may be shared in discovery.

Now, there is a limit to the discovery envisioned by these 21 FISA orders; this discovery language, in the most recently published order, reads:

> Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings …

That is, this discovery language only includes the "results from intelligence analysis queries." It doesn't permit new queries of the entire database, a point the government makes over and over. But in the case of the Marathon bombing, we know the queries have been run, because Executive Branch officials have been bragging about the queries they did after the bombing that gave them "peace of mind."

Those query results are there, and the FISC

judges explicitly envisioned the queries to be discoverable. And yet the government, in defiance of the minimization procedures they claim are sacred, refuse to comply.

FINGERPRINTS AND THE PHONE DRAGNET'S SECRET "CORRELATIONS" ORDER

Yesterday, I noted that ODNI is withholding a supplemental opinion approved on August 20, 2008 that almost certainly approved the tracking of "correlations" among the phone dragnet (though this surely extends to the Internet dragnet as well).

I pointed out that documents released by Edward Snowden suggest the use of correlations extends well beyond the search for "burner" phones.

At almost precisely the same time, Snowden was testifying to the EU. The first question he answered served to clarify what "fingerprints" are and how XKeyscore uses them to track a range of innocent activities. (This starts after 11:16, transcription mine.)

> It has been reported that the NSA's XKeyscore for interacting with the raw signals intercepted by mass surveillance programs allow for the creation of something that is called "fingerprints."
>
> I'd like to explain what that really means. The answer will be somewhat technical for a parliamentary setting, but these fingerprints can be used to construct **a kind of unique signature** for

> any individual or group's communications which are often **comprised of a collection of "selectors" such as email addresses, phone numbers, or user names**.
>
> This allows State Security Bureaus to instantly identify the movements and activities of you, your computers, or other devices, your personal Internet accounts, or even key words or other uncommon strings that indicate an individual or group, out of all the communications they intercept in the world are associated with that particular communication. Much like a fingerprint that you would leave on a handle of your door or your steering wheel for your car and so on.
>
> However, though that has been reported, that is the smallest part of the NSA's fingerprinting capability. You must first understand that any kind of Internet traffic that passes before these mass surveillance sensors can be analyzed in a protocol agnostic manner – metadata and content, both. And it can be today, right now, searched not only with very little effort, via a complex regular expression, which is a type of shorthand programming. But also via any algorithm an analyst can implement in popular high level programming languages. Now, this is very common for technicians. It not a significant work load, it's quite easy.
>
> This provides a capability for analysts to do things like associate unique identifiers assigned to untargeted individuals via unencrypted commercial advertising networks through cookies or other trackers – common tracking means used by businesses everyday on the Internet – with personal details, such as individuals' precise identity, personal identity, their geographic

> location, their political affiliations, their place of work, their computer operating system and other technical details, their sexual orientation, their personal interests, and so on and so forth. There are very few practical limitations to the kind of analysis that can be technically performed in this manner, short of the actual imagination of the analysts themselves.
>
> And this kind of complex analysis is in fact performed today using these systems. I can say, with authority, that the US government's claim that "keyword filters," searches, or "about" analysis, had not been performed by its intelligence agencies are, in fact, false. I know this because I have personally executed such searches with the explicit authorization of US government officials. And I can personally attest that these kind of searches may scrutinize communications of both American and European Union citizens without involvement of any judicial warrants or other prior legal review.
>
> What this means in non-technical terms, more generally, is that I, an analyst working at NSA, or, more concerningly, an analyst working for a more authoritarian government elsewhere, can without the issue of any warrant, create an algorithm that for any given time period, with or without human involvement, sets aside the communications of not only targeted individuals, but even a class of individual, and that just indications of an activity – or even just indications of an activity that I as the analyst don't approve of – something that I consider to be nefarious, or to indicate nefarious thoughts, or pre-criminal activity, even if there's no evidence or

> indication that’s in fact what’s happening. that it’s not innocent behavior. The nature of the mass surveillance – of these mass surveillance technologies – create a de facto policy of assigning guilt by association rather than on the basis of specific investigations based on reasonable suspicion.
>
> Specifically, mass surveillance systems like XKeyscore provide organizations such as the NSA with the technical ability to trivially track entire populations of individuals who share any trait that is discoverable from unencrypted communications. For example, these include religious beliefs, political affiliations, sexual orientations, contact with a disfavored individual or group, history of donating to specific or general causes, interactions of transactions with certain private businesses, or even private gun ownership. It is a trivial task, for example, to generate lists of home addresses for people matching the target criteria. Or to collect their phone numbers, to discover their friends, or even, to analyze the proximity and location of their social connections by automating the detection of factors such as who they share pictures of their children with, which is capable of machine analysis.
>
> I would hope that this goes without saying, but let me be clear that the NSA is not engaged in any sort of nightmare scenarios, such as actively compiling lists of homosexual individuals to round them up and send them into camps, or anything of that sort. However, they still deeply implicate our human rights. We have to recognize that the infrastructure for such activities has been built, and is within reach of not

> just the United States and its allies, but of any country today. And that includes even private organizations that are not associated with governments.
>
> Accordingly, we have an obligation to develop international standards, to protect against the routine and substantial abuse of this technology, abuses that are ongoing today. I urge the committee in the strongest terms to bear in mind that this is not just a problem for the United States, or the European Union, but that this is in fact a global problem, not an isolated issue of Europe versus the Five Eyes or any other [unclear]. These technical capabilities don't merely exist, they're already in place and actively being used without the issue of any judicial warrant. I state that these capabilities are not yet being used to create lists of all the Christians in Egypt, but let's talk about what they are used for, at least in a general sense, based on actual real world cases that I can assert are in fact true.
>
> Fingerprints — for example, the kind used of XKeyscore — have been used — I have specific knowledge that they have been used — to track and intercept, to track, intercept, and monitor the travels of innocent citizens, who are not suspected of anything worse than booking a flight. This was done, in Europe, against EU citizens but it is of course not limited to that geographic region, nor that population. Fingerprints have also been used to monitor untold masses of people whose communications transit the entire country of Switzerland over specific routes. They're used to identify people — Fingerprints are used to identify people who have had the bad luck to follow the wrong link on an Internet

> site, on an Internet forum, or even to download the wrong file. They've been used to identify people who simply visit an Internet sex forum. They've also been used to monitor French citizens who have never done anything wrong other than logging into a network that's suspected of activity that's associated with a behavior that the National Security Agency does not approve of.
>
> This mass surveillance network, constructed by the NSA, which, as I pointed out, is an Agency of the US military Department of Defense, not a civilian agency, and is also enabled by agreements with countries such as the United Kingdom, Australia, and even Germany, is not restricted for being used strictly for national security purposes, for the prevention of terrorism, or even for foreign intelligence more broadly.
>
> XKeyscore is today secretly being used for law enforcement purposes, for the detection of even non-violent offenses, and yet this practice has never been declared to any defendant or to any open court.
>
> We need to be clear with our language. These practices are abusive. This is clearly a disproportionate use of an extraordinarily invasive authority, an extraordinarily invasive means of investigation, taken against entire populations, rather than the traditional investigative standard of using the least intrusive means or investigating specifically named targets, individuals, or groups. The screening of trillions — I mean that literally, trillions — of private communications for the vaguest indications of associations or some other nebulous pre-criminal activity is a violation of the human right to be

> free from unwarranted interference, to be secure in our communications and our private affairs, and it must be addressed. These activities — routine, I point out, unexceptional activities that happen every day — are only a tiny portion of what the Five Eyes are secretly doing behind closed doors, without the review, consent, or approval of any public body. This technology represents the most significant — what I consider the most significant.new threat to civil rights in modern times.

Now, this doesn't guarantee that the NSA correlates identifiers to dump them into XKeyscore (which is, as far as I know, used only on data collected outside the US; the "about" 702 collection is a more limited version of what is done in the US, with returned data likely dumped into databases used with XKeyscore). But Snowden makes it clear such fingerprints involve precisely the identifiers, including phone numbers, used in the domestic dragnets.

Moreover, we know that data in the corporate store — all those people who are two or three degrees away from someone who has been digitally stop-and-frisked — is subject to all the analytical authorities the NSA uses, which clearly includes fingerprinting and use in XKeyscore.

"Correlations" — as the NSA uses in language with the FISC and Congress — are almost certainly either fingerprints, or subset of the fingerprinting process.

And this is, almost certainly, what the government is hiding in that August 20, 2008 order.

THE OTHER PROBLEM WITH THE OBAMA PROPOSAL: WHO DOES THE PIZZA JOINT REVIEW?

I'm sure I'll spend all day discussing the various proposals to "fix" the dragnet.

I've already shown why the House Intelligence bill is not an improvement and should not be discussed by credible people as one.

And on Twitter and briefly in that piece, I described two problems that aren't addressed at all in either of these proposals, including President Obama's plan laid out by Charlie Savage.

- The Reasonable Articulable Suspicion standard is still far too lenient, allowing the government to engage in a broad digital stop-and-frisk system
- Once supplied to NSA, it will presumably subject tens or hundreds of thousands of innocent people to the full array of NSA's tradecraft

Finally, though, there's one other problem, which directly affects how many people get subjected to such analytical tradecraft, a problem identified by no other person than … Barack Obama.

> Relying solely on the records of multiple providers, for example, could require companies to alter their procedures in ways that raise new

> privacy concerns.

I suspect one of those privacy concerns, as I laid out in this post, is the necessity to make analytical judgments about what high volume numbers distort the chaining system.

Someone needs to go in and take out such high volume numbers — which include voice mail access numbers, telemarketers, and pizza joints — otherwise almost everyone is two degrees of separation from everyone else.

For two of these functions, I assume the telecoms can do the task as easily as the NSA. (The dirty secret is they conduct the same kind of 3-degrees analysis as the government does!) They know what their own (and reseller phone companies) voice mail access numbers are, after all, and surely they track the telemarketer spam that weighs down their system.

It's the pizza joints that have me — that always have me — worried.

Pizza joints absolutely distort the contact chaining system. Keith Alexander learned this when the contact chaining he was doing — and he used to claim he had mapped out all the evil people tied to Iraq — showed everyone to be guilty because they frequented the same pizza joints.

> When he ran INSCOM and was horning in on the NSA's turf, Alexander was fond of building charts that showed how a suspected terrorist was connected to a much broader network of people via his communications or the contacts in his phone or email account.
>
> "He had all these diagrams showing how this guy was connected to that guy and to that guy," says a former NSA official who heard Alexander give briefings on the floor of the Information Dominance Center. "Some of my colleagues and I were skeptical. Later, we had a chance

> to review the information. It turns out that all [that] those guys were connected to were pizza shops."

Nevertheless, sometimes a cigar is just a cigar, and sometimes a tie through a pizza joint can be a very important tie through a pizza joint, as I believe Gerry's Italian Kitchen was in the case of the Tsarnaev brothers. If NSA purged the pizza joint in that case, they may have eliminated some of the most important evidence tying the brothers (or at least Tamerlan) to the Waltham murder in 2011.

So who, under this new system, will do the pizza joint analysis?

If the phone companies do it (which I doubt, because of cases like the Tsarnaevs), it will mean even more intensive data mining of customer data while it remains in their hands.

If the NSA does it, it means a lot more totally innocent people will have their data turned over to NSA to do as they wish.

Don't get me wrong. The Obama proposal is an improvement off the status quo. But for these reasons, including the pizza joint problem, it still doesn't comply with the Fourth or First Amendments.