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.