Word Games

Government officials have made many statements about the warrantless surveillance since it became public in 2005. They've done so in court, in Congress, and in the media. Unfortunately, their words have too often served to evade or obscure, rather than clarify, their actions.

A close reading of the government's statements, along with other publicly available materials, sheds some light on at least some of their word games. Here are some words or phrases to watch closely:

- Terrorist Surveillance Program or TSP
- Surveillance
- Targeted
- Collection or Collect
- Content
- Conversations and Communications

This list likely isn't complete, but with the specific definitional games in mind, the government's public statements about the warrantless surveillance become both much less clear and much more troubling. Here's a detailed look:

"Terrorist Surveillance Program"

Government officials have generally cabined their discussions of the warrantless surveillance program to one aspect of the Program: the "Terrorist Surveillance Program" (TSP). Yet they have now admitted, and the Inspector General has confirmed, that the so-called TSP is not everything that they are doing.

As President Bush's then-Press Secretary Tony Snow explained when warrantless wiretapping was first revealed (http://georgewbush-whitehouse.archives.gov/news/releases/2007/08/20070801-3.html), TSP was simply a marketing term, "a label attached after the original stories appeared about the program." More critically, the phrase "Terrorist Surveillance Program" does not describe the entire warrantless wiretapping program or even an independent program, but, as the former Director of National of Intelligence Mike McConnell put it (http://www.washingtonpost.com/wp-dyn/content/article/2007/07/31/AR2007073102137.html), "one particular *aspect* of these activities" that President Bush publicly disclosed in 2005—it references, by definition, only intercepts where one end of the communication was affiliated with al Qaeda.

The Inspectors General Report (https://www.eff.org/deeplinks/2009/07/unclassified-version), brings some needed clarity, acknowledging that "several different intelligences activities were authorized," and adopting the broader term "President's Surveillance Program."

Officials nevertheless persist in using the TSP phrase in an effort to assert that the broader program is limited, justified, or is no longer in operation—which is not the case. For example, in the *Jewel v. NSA* case, the government wrote (https://www.eff.org/node/71868):

> Plaintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false.

A first glance, this seems like a rather strong denial of warrantless spying.

But the statement only refers to activities "under the TSP," meaning that it is only a denial of the *aspect* of intelligence activities labeled the Terrorist Surveillance Program. So if the collections occurred under another aspect of the government spying, the denial would not apply.

Moreover, the statement also uses "collected" and "content" in ways you might not expect. As described further below, under the government's definition, "collected" means "reviewed by a live person" and "content" excludes metadata like phone numbers and email addresses.

Thus, under the government's misleading use of terms,

the statement above would still be true if the NSA obtained copies of millions of communications, placed them all in a massive database, searched through their metadata using algorithms, and had agents review the communications found to be suspicious.

"Surveillance"

In public discussions of the Program, the government appears to exclude from the term "surveillance" instances where communications are acquired but subsequently "minimized," despite the broader legal definition of "electronic surveillance" under applicable law. For example, a statement by then White House press secretary Tony Snow (http://georgewbush-whitehouse.archives.gov/news/releases/2007/08/20070808-4.html) displays this irregular usage:

> MR. SNOW:...the target in these conversations: a foreign individual not on US soil. If that person is talking to a US citizen, it does not mean that you're sitting around doing surveillance on the US citizen. Furthermore, if it is a—
>
> Q: But if you're surveilling a phone call, you're not just listening to the foreigner's side of the call, right?
>
> MR. SNOW: Well, yes, but on the other hand, if—you probably understand that if somebody is just calling in and asking how his socks are at the dry

> cleaners, all of that personal information is combed out and, in fact, the US citizen basically —you're not conducting surveillance.

"Targeted"

The government defends its online surveillance programs under Section 702 of FISA as "targeted" and not mass surveillance, but don't be fooled. Programs like Upstream —which taps directly into U.S. fiber-optic Internet backbone cables and then copied and retains hundreds of millions of communications—are far from targeted.

Under Upstream and PRISM—which involves the government working with companies like Google, Facebook, or Yahoo to get users' communications—the so-called "targeted" surveillance sweeps so broadly that communications of innocent third parties are inevitably and intentionally vacuumed up.

According to The Washington Post's analysis (https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html) of documents obtained by former NSA contractor Edward Snowden, nine out of 10 account holders whose communications were collected by the NSA "were not the intended surveillance targets but were caught in a net the agency had case for someone

else." The Post estimated that the government would collect communications from more than 900,000 user accounts annually under its "targeted" 702 programs.

"Targeted" fails to describe how wide a net the NSA casts both when it comes to whose communications they look at and what they look for. Through Upstream, the NSA retains communications that are "about" – rather than to or from – a surveillance target. To collect those communications, the NSA conducts a content search of all, or substantially all, international Internet communications travelling through U.S. Internet cables.

"Collection" or "Collect"

Normally, one would think that a communication that has been intercepted and stored in a government database as "collected." But the government's definition of what it means to "collect" intelligence information is quite different from its plain meaning.

Under Department of Defense regulations (http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf), information is considered to be "collected" only after it has been "received for use by an employee of a DoD intelligence component," and "data acquired by electronic means is 'collected' only when it has been processed into intelligible form."

In other words, the NSA can intercept and store communications in its data base and have an algorithm

search them for key words and analyze the meta data without ever considering the communications "collected."

"Content"

For purposes of national security surveillance at issue in *Jewel v. NSA*, under the Foreign Intelligence Surveillance Act (FISA), the term "content" is defined very broadly, "any *information concerning the identity of the parties to such communication or the existence,* substance, purport, or meaning of that communication."

This is in contrast to the federal Wiretap Act, where "content" is defined as the "substance, meaning or purport of a communication."

But despite the broad, applicable definition of "content" used in FISA, the government often excludes all communications records (or "metadata") from its definition of the term in discussing the NSA's warrantless surveillance, as demonstrated by this statement from then Director of National Intelligence J. Michael McConnell:

> Mr. HOLT. Do you need to be able to conduct bulk collection of call detail records, metadata for domestic-to-domestic phone calls by Americans?
>
> Director MCCONNELL. *Metadata, we think of it as not content* but a process for how you would find something you might be looking for. Think of it

as a roadmap.

Even in the Wiretap Act, as in FISA, "content" includes email subject lines and URLs. The government has admitted as much in its own internal manuals (http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pd But, when describing the Program, the government appears to exclude both subject lines and URLs from its definition of "content."

For example, Gen. Hayden, former Director of the NSA, testified that (http://www.washingtonpost.com/wp-dyn/content/article/2006/05/18/AR2006051800823.html) "we do not use the content of communications to decide which communications we want to study the content of." However, in the next sentence, Hayden shows he was using a crabbed definition of "content" that excludes the subject lines of email and the URLs of web links: "in other words, when we look at the content of the communications, everything between 'hello' and 'good bye'...."

"Conversations" and "Communications"

The government has also used the terms "conversations" and "communications" in ways that obscure the Program's scope. For example, in a January 2006 speech at the National Press Club (https://www.fas.org/irp/news/2006/01/hayden012306.html), Gen. Hayden, as the former Director of the NSA, attempted

to downplay fears after the Program's initial disclosure by the *New York Times.* Hayden said:

> Let me talk for a few minutes also about what this program is not. It is not a driftnet over Dearborn or Lackawanna or Freemont grabbing conversations that we then sort out by these alleged keyword searches or data-mining tools or other devices that so-called experts keep talking about.

Later, however, after the May 11, 2006 *USA Today* story (http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm) brought the government's creation of a vast database of domestic calls to the attention of the American public, Hayden's story became hard to believe. Called to account for this before Congress, Hayden testified (http://www.washingtonpost.com/wp-dyn/content/article/2006/05/18/AR2006051800823.html):

> [A]t key points, key points in my remarks, I pointedly and consciously downshifted the language I was using. When I was talking about a drift net over Lackawanna or Freemont or other cities, I switched from the word "communications" to the much more specific and unarguably accurate conversation.

So as you can see, officials regularly "downshift" their

language when talking about the NSA warrantless surveillance program, or in other words, “purposefully obscure the truth.”

ELECTRONIC FRONTIER FOUNDATION

(https://www.eff.org)
The leading nonprofit defending digital privacy, free speech, and innovation.

FOLLOW EFF:

CONTACT

General (/about/contact)

Legal (/pages/legal-assistance)

Security (/security)

Membership (/about/contact)

Press (/press/contact)

ABOUT

Calendar (/event)

Volunteer (/about/opportunities/volunteer)

Victories (/victories)

History (/about/history)

Internships (/about/opportunities/interns)

Jobs (/about/opportunities/jobs)

Staff (/about/staff)

ISSUES

Free Speech (/issues/free-speech)

Privacy (/issues/privacy)

Creativity & Innovation (/issues/innovation)

Transparency (/issues/transparency)

International (/issues/international)

Security (/issues/security)

UPDATES

Blog (/updates?type=blog)

Events (/updates?type=event)

Press Releases (/updates?type=press_release)

White Papers (/updates?type=whitepaper)

PRESS

Press Contact (/press/contact)

Press Materials (/press/logos)

DONATE

Join or Renew Membership Online (https://supporters.eff.org/donate)

One-Time Donation Online (https://supporters.eff.org/donate)

Shop (https://supporters.eff.org/shop)

Other Ways to Give (/helpout)

COPYRIGHT (CC BY) (/COPYRIGHT)

TRADEMARK (/PAGES/TRADEMARK-AND-BRAND-USAGE-POLICY)

PRIVACY POLICY (/POLICY)

THANKS (/THANKS)