the Atlantic

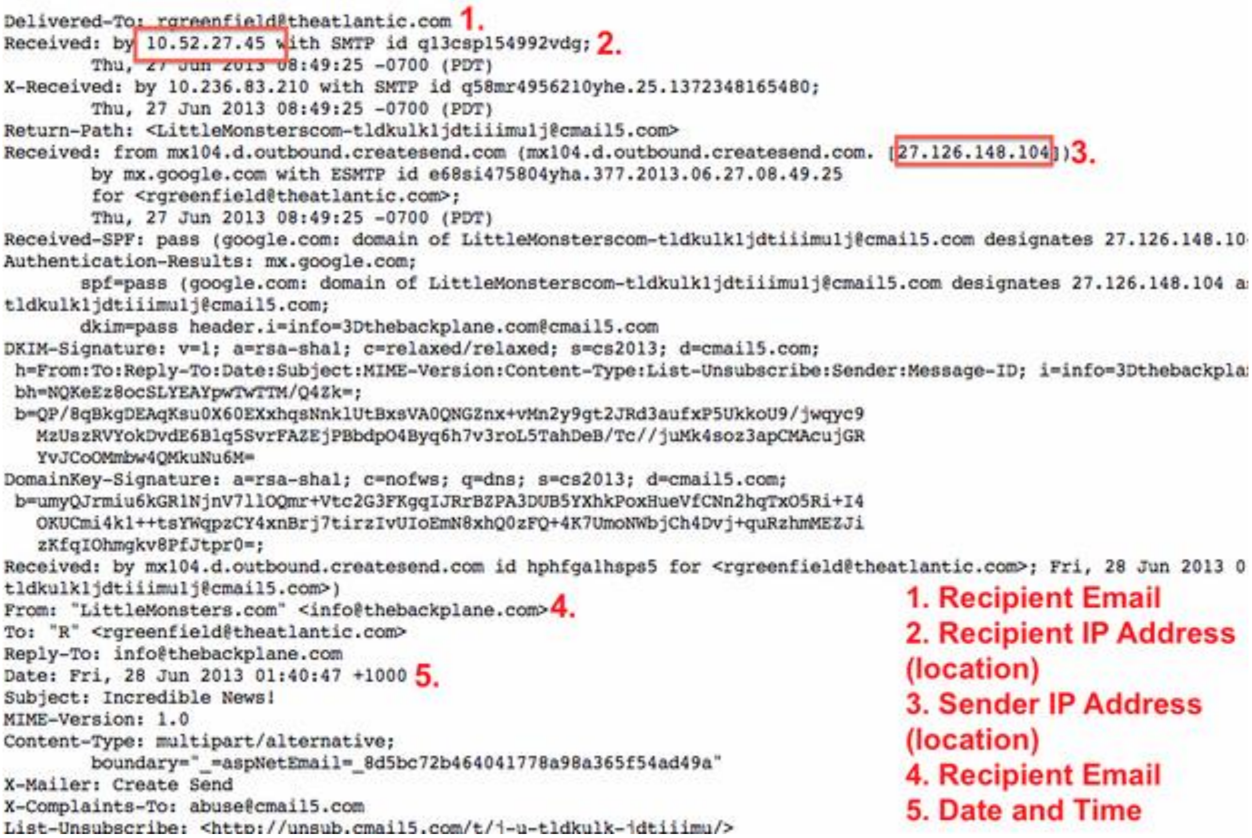
What Your Email Metadata Told the NSA About You

By Rebecca Greenfield – June 27th, 2013

President Obama said "nobody is listening to your telephone calls," even though the National Security Agency could actually track you from cellphone metadata. Well, the latest from the Edward Snowden leaks shows that Obama eventually told the NSA to stop collecting your email communications in 2011, apparently because the so-called StellarWind program "was not yielding much value," even when collected in bulk. But how much could the NSA learn from all that email metadata, really? And was it more invasive than phone data collection? The agency is well beyond its one trillionth metadata record, after all, so they must have gotten pretty good at this.

To offer a basic sense of how StellarWind collection worked — and how much user names and IP addresses can tell a spy about a person, even if he's not reading the contents of your email — we took a look at the raw source code of an everyday email header. It's not the exact kind of information the NSA was pulling, of course, but it shows the type of information attached to every single one of your emails.

Below is what the metadata looks like as it travels around with an email — we've annotated the relevant parts, based on what *The Guardian* reported today as the legally allowed (and apparently expanded) powers of the NSA to read without your permission. After all, it's right there behind your words:

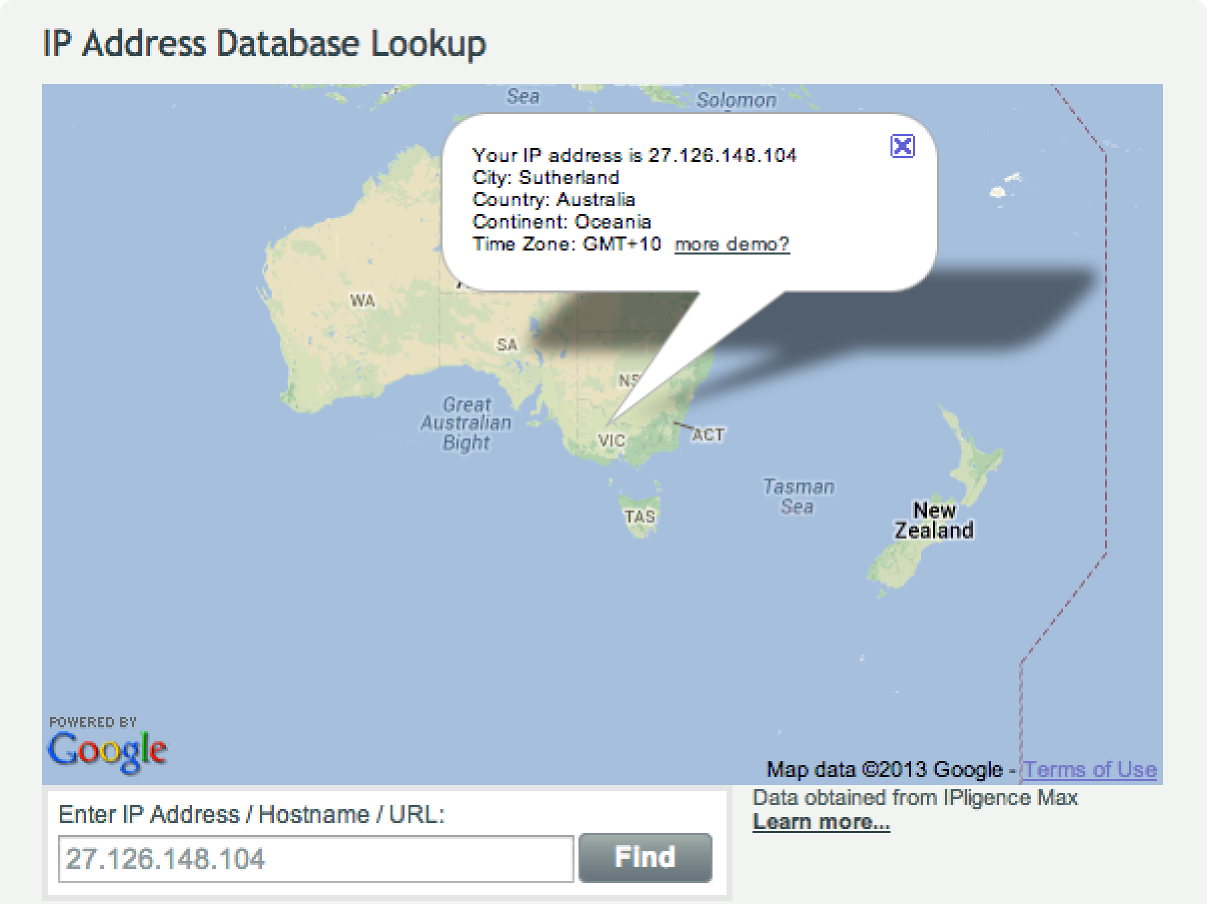


```
Delivered-To: rgreenfield@theatlantic.com 1.
Received: by 10.52.27.45 with SMTP id q13csp154992vdg; 2.
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
X-Received: by 10.236.83.210 with SMTP id q58mr4956210yhe.25.1372348165480;
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
Return-Path: <LittleMonsterscom-tldkulkljdtiiimulj@cmail5.com>
Received: from mx104.d.outbound.createsend.com (mx104.d.outbound.createsend.com. [27.126.148.104]) 3.
        by mx.google.com with ESMTP id e68si475804yha.377.2013.06.27.08.49.25
        for <rgreenfield@theatlantic.com>;
        Thu, 27 Jun 2013 08:49:25 -0700 (PDT)
Received-SPF: pass (google.com: domain of LittleMonsterscom-tldkulkljdtiiimulj@cmail5.com designates 27.126.148.10
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of LittleMonsterscom-tldkulkljdtiiimulj@cmail5.com designates 27.126.148.104 a
tldkulkljdtiiimulj@cmail5.com;
       dkim=pass header.i=info=3Dthebackplane.com@cmail5.com
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=cs2013; d=cmail5.com;
 h=From:To:Reply-To:Date:Subject:MIME-Version:Content-Type:List-Unsubscribe:Sender:Message-ID; i=info=3Dthebackpla
 bh=NQKeEz8ocSLYEAYpwTwTTM/Q4Zk=;
 b=QP/8qBkgDEAqKsu0X60EXxhqsNnklUtBxsVA0QNGZnx+vMn2y9gt2JRd3aufxP5UkkoU9/jwqyc9
   MzUszRVYokDvdE6Blq5SvrFAZEjPBbdpO4Byq6h7v3roL5TahDeB/Tc//juMk4soz3apCMAcujGR
   YvJCoOMmbw4QMkuNu6M=
DomainKey-Signature: a=rsa-sha1; c=nofws; q=dns; s=cs2013; d=cmail5.com;
 b=umyQJrmiu6kGR1NjnV71lOQmr+Vtc2G3FKgqIJRrBZPA3DUB5YXhkPoxHueVfCNn2hqTxO5Ri+I4
   OKUCmi4k1++tsYWqpzCY4xnBrj7tirzIvUIoEmN8xhQ0zFQ+4K7UmoNWbjCh4Dvj+quRzhmMEZJi
   zKfqIOhmgkv8PfJtpr0=;
Received: by mx104.d.outbound.createsend.com id hphfgalhsps5 for <rgreenfield@theatlantic.com>; Fri, 28 Jun 2013 0
tldkulkljdtiiimulj@cmail5.com>)
From: "LittleMonsters.com" <info@thebackplane.com>4.
To: "R" <rgreenfield@theatlantic.com>
Reply-To: info@thebackplane.com
Date: Fri, 28 Jun 2013 01:40:47 +1000 5.
Subject: Incredible News!
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="_=aspNetEmail=_8d5bc72b464041778a98a365f54ad49a"
X-Mailer: Create Send
X-Complaints-To: abuse@cmail5.com
List-Unsubscribe: <http://unsub.cmail5.com/t/i-u-tldkulk-idtiiimu/>
```

1. Recipient Email
2. Recipient IP Address (location)
3. Sender IP Address (location)
4. Recipient Email
5. Date and Time

As you can see, at the bare minimum, your average email metadata offers location (through the IPs), plus names (or at least email addresses), and dates (down to the second). *The Guardian*'s Glenn Greenwald and Spencer Ackerman report that Attorney General Michael Mukasey and Defense Secretary Bob Gates signed a document that OK'd the collection and mining of "the information appearing on the 'to,' 'from' or 'bcc' lines of a standard email or other electronic communication" from, well, you and your friends and maybe some terrorists.

But email metadata is more revealing than that — even more revealing than what the NSA could do with just the time of your last phone call and the nearest cell tower. For operation StellarWind, it must have been all about that IP, or Internet protocol, address. Hell, it'd be easy enough for your grandma to geolocate both parties from a couple of IPs: there are countless free services on Google that turn those numbers you give to the IT guy into your exact location. For example, using the two IP addresses in the email sent to me above, we can easily determine that it was sent from Victoria, Australia:



IP Address Database Lookup

Your IP address is 27.126.148.104
City: Sutherland
Country: Australia
Continent: Oceania
Time Zone: GMT+10 more demo?

Map data ©2013 Google - Terms of Use

Enter IP Address / Hostname / URL:
27.126.148.104

Data obtained from IPligence Max
Learn more...

The IP address is like a homing pigeon, and that's why the revelations of email metadata being authorized under the Bush and Obama administrations amounts to a seriously revealing breach of personal security in the name of terror-hunting. "Seeing your IP logs — and especially feeding them through sophisticated analytic tools — is a way of getting inside your head that's in many ways on par with reading your diary," Julian Sanchez of the Cato Institute told *The Guardian*. Of course, the administration has another party line, telling the *Los Angeles Times* that operation StellarWind was discontinued because it wasn't adding up to enough good intelligence of "value." But with one of the many "sophisticated analytic tool" sets developed by the NSA over the last decade or so and leaked during the last month — like, say, EvilOlive, "a near-real-time metadata analyzer" described in yet another *Guardian* scoop today — America's intelligence operation certainly can zero in on exactly where Americans are. Even if you're just emailing your hip grandma.