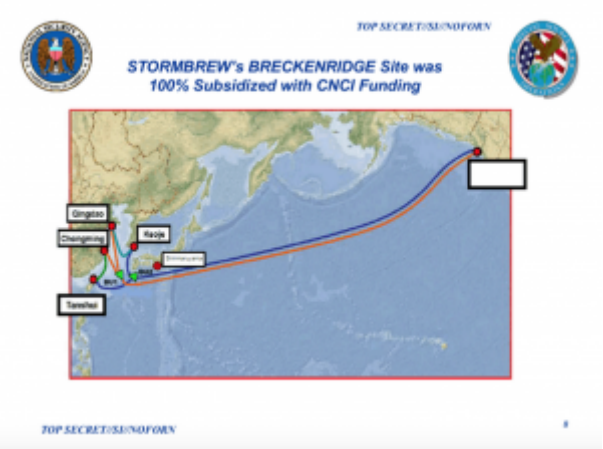
WHAT'S A LITTLE (OR A LOT) COOPERATION AMONG SPIES?

A key point in the ProPublica/NYT piece on AT&T's close cooperation with the NSA (and, though not stated explicitly, other agencies) on spying is that AT&T was the telecom that helped NSA spy on the UN.



> It provided technical assistance in carrying out a secret court order permitting the wiretapping of all Internet communications at the United Nations headquarters, a customer of AT&T.

If you read the underlying document, it actually shows that NSA had a traditional FISA order requiring the cooperation (remember, "agents of foreign powers," as diplomats are, are among the legal wiretap targets under FISA, no matter what we might think about NSA spying on UN in our own country) — meaning whatever telecom serviced the UN legally had to turn over the data. And a big part of AT&T's cooperation, in addition to technically improving data quality, involved filtering the data to help NSA avoid overload.

> BLARNEY began intermittent enablement of DNI traffic for TOPI assessment and feedback. This feedback is being used by the BLARNEY target development team to support an ongoing filtering and

> throttling of data volumes. While BLARNEY is authorized full-take access under the NSA FISA, collected data volumes would flood PINWALE allocations within hours without a robust filtering mechanism.

In other words, AT&T helped NSA, ironically, by helping it limit what data it took in. Arguably, that's an analytical role (who builds the algorithms in the filter?), but it's one that limits how much actually gets turned over to the government.

That doesn't mean the cooperation was any less valued, nor does it mean it didn't go beyond what AT&T was legally obliged to do under the FISA order. But it's not evidence AT&T would wiretap a non-legal (private corporation) target as a favor for NSA. That evidence may exist, somewhere, but it's not in this story, except insofar as it mentions Stellar Wind, where AT&T *was* doing such things.

To be fair, AT&T's UN cooperation is actually emphasized in this story because it was a key data point in the worthwhile ProPublica piece explaining how they proved Fairview was AT&T.

> In April 2012, an internal NSA newsletter boasted about a successful operation in which NSA spied on the United Nations headquarters in New York City with the help of its Fairview and Blarney programs. Blarney is a program that undertakes surveillance that is authorized by the Foreign Intelligence Surveillance Court.
>
> > FAIRVIEW and BLARNEY engineers collaborated to enable the delivery of 700Mbps of paired packet switched traffic (DNI) traffic from access to an OC192 ring serving the United Nations mission in New York … FAIRVIEW

> > engineers and the partner worked to provide the correct mapping, and BLARNEY worked with the partner to correct data quality issues so the data could be handed off to BLARNEY engineers to enable processing of the DNI traffic.
>
> We found historical records showing that AT&T was paid $1 million a year to operate the U.N.'s fiber optic provider in 2011 and 2012. A spokesman for the U.N. secretary general confirmed that the organization "has a current contract with AT&T" to operate the fiber optic network at the U.N. headquarters in New York.

That is, the UN story is important largely because there are public records proving that AT&T was the provider in question, not because it's the most egregious example of AT&T's solicitous relationship with the nation's spies.

Also in that story proving how they determined Fairview was AT&T and Stormbrew included Verizon was the slide above, bragging that the Comprehensive National Cybersecurity Initiative 100% subsidized Verizon's Breckenridge site at a new cable landing carrying traffic from China.

It's not entirely clear what that means — it might just refer to the SCIF, power supply, and servers needed to run the TURMOIL (that is, passive filtering) deployments the NSA wanted to track international traffic with China. But as ProPublica lays out, the NSA was involved the entire time Verizon was planning this cable landing. Another document on CNCI shows that in FY2010 — while significantly less than AT&T's Fairview — NSA was dumping over $100M into Stormbrew and five times as much money into "cyber" than on FISA (in spite of the fact that they admit they're really doing all this cybering to catch attacks on the US, meaning it

has to ostensibly be conducted under FISA, even if FISC had not yet and may never have approved a cyber certificate for upstream 702). And those numbers date to the year after the Breckenridge project was put on line, and at a time when Verizon was backing off an earlier closer relationship with the Feds.

How much did Verizon really get for that cable landing, what did they provide in exchange, and given that this was purpose-built to focus on Chinese hacking 6 years ago, why is China still eating our lunch via hacking? And if taxpayers are already subsidizing Verizon 100% for capital investments, why are we still paying our cell phone bills?

Particularly given the clear focus on cyber at this cable landing, I recall the emphasis on Department of Commerce when discussing the government's partnership with industry in PPD-20, covering authorizations for various cyber activities, including offensive cyberwar (note the warning I gave for how Americans would start to care about this Snowden disclosure once our rivals, like China, retaliate). That is, the government has Commerce use carrots and sticks to get cooperation from corporations, especially on cybersecurity.

None of this changes the fact that AT&T has long been all too happy to spy on its customers for the government. It just points to how little we know about these relationships, and how much quid pro quo there really is. We know from PRISM discussions that the providers could negotiate how they accomplished an order (as AT&T likely could with the order to wiretap the UN), and that's one measure of "cooperation." But there's a whole lot else to this kind of cooperation.

Update: Credo released a statement in response to the story.

> As a telecom that can be compelled to participate in unconstitutional surveillance, we know how important it is to fight for our customers' privacy

> and only hand over information related to private communications when required by law," said CREDO Mobile Vice President Becky Bond. "It's beyond disturbing though sadly not surprising what's being reported about a secret government relationship with AT&T that NSA documents describe as 'highly collaborative' and a 'partnership, not a contractual relationship,'
>
> CREDO Mobile supports full repeal of the illegal surveillance state as the only way to protect Americans from illegal government spying," Bond continued, "and we challenge AT&T to demonstrate concern for its customers' constitutional rights by joining us in public support of repealing both the Patriot Act and FISA Amendments Act.