GlobalResearch
Center for Research on Globalization

Documents Show Undersea Cable Firms Provide Surveillance Access to US Secret State

By Tom Burghardt
Global Research, July 18, 2013
Antifascist Calling...

Theme: Intelligence, Police State & Civil Rights

Documents published last week by the Australian web site Crikey revealed that the US government "compelled Telstra and Hong Kong-based PCCW to give it access to their undersea cables for spying on communications traffic entering and leaving the US."

The significance of the disclosure is obvious; today, more than 99 percent of the world's internet and telephone traffic is now carried by undersea fiber optic cables. An interactive submarine cable map published by the Global Bandwidth Research Service is illustrative in this regard.

Since the late 1960s as part of its ECHELON spy project, the United States has been tapping undersea cables to extract communications and signals intelligence. In fact, projects such as Operation Ivy Bells, a joint Navy-NSA secret intelligence program directed against the former Soviet Union was designed to do just that.

Prefiguring the Bush administration's warrantless wiretapping scandal which broke in 2005, the *Associated Press* reported that a $3.2 billion Navy Seawolf class submarine, a 453-foot behemoth called the USS Jimmy Carter, "has a special capability: it is able to tap undersea cables and eavesdrop on the communications passing through them."

A year later, AT&T whistleblower Mark Klein told *Wired Magazine*that NSA was tapping directly into the world's internet backbone, and was doing so from domestic listening posts the telecommunications' giant jointly built with the agency at corporate switching stations.

Whatever submarine operations NSA still carry out with the US Navy and "Five Eyes" surveillance partners (Australia, Britain, Canada, New Zealand and the US), access to information flowing through undersea cables mean that the US government is well-positioned to scoop-up virtually all global communications.

Since former NSA contractor Edward Snowden began spilling the beans last month, it should be clear that the American government's capabilities in amassing unprecedented volumes of information from cable traffic, also potentially hands the US and their corporate collaborators a treasure trove of sensitive economic secrets from competitors.

Economic Espionage

Reporting by Australian journalists confirm information published July 6 by *The Washington Post*. There we learned that overseas submarine cable companies doing business in the United States must maintain "an internal corporate cell of American citizens with government clearances," a cadre of personnel whose job is to ensure that "when US

government agencies seek access to the massive amounts of data flowing through their networks, the companies have systems in place to provide it securely."

Inked just weeks after the 9/11 provocation, the 23-page Telstradocument specifies that access to undersea cable traffic by the FBI and "any US governmental authorities entitled to effect Electronic Surveillance," is an explicit condition for doing business in the United States.

Similar agreements were signed between 1999 and 2011 with telecommunication companies, satellite firms, submarine cable operators and the US government and were published earlier this month by the Public Intelligence web site.

It has long been known that the Australian secret state agency, the Defence Security Directorate (DSD), is a key participant in US global surveillance projects. Classified NSA maps provided by Snowden and subsequently published by Brazil's *O Globo*newspaper, revealed the locations of dozens of US and allied signals intelligence sites worldwide. DSD currently operates four military installations involved in a top secret NSA program called X-Keyscore.

Snowden described X-Keyscore and other programs to *Der Spiegel* as "the intelligence community's first 'full-take' Internet buffer that doesn't care about content type . . . 'Full take' means it doesn't miss anything, and ingests the entirety of each circuit's capacity."

According to *The Sydney Morning Herald*, along with the "US Australian Joint Defence Facility at Pine Gap near Alice Springs," three other DSD facilities, "the Shoal Bay Receiving Station near Darwin, the Australian Defence Satellite Communications Facility at Geraldton and the naval communications station HMAS Harman outside Canberra," were identified as X-Keyscore "contributors." The paper also reported that "a new state-of-the-art data storage facility at HMAS Harman to support the Australian signals directorate and other Australian intelligence agencies" is currently under construction.

The *Herald* described the project as "an intelligence collection program" that "processes all signals before they are shunted off to various 'production lines' that deal with specific issues and the exploitation of different data types for analysis–variously code-named Nucleon (voice), Pinwale (video), Mainway (call records) and Marina (internet records). US intelligence expert William Arkin describes X-Keyscore as a 'national Intelligence collection mission system'."

Two of the Australian bases illustrated on the X-Keyscore map sit adjacent to major undersea cable sites transiting the Pacific and Indian Oceans.

Cozy arrangements with Telstra and other firms however, hardly represent mere passive acceptance of terms and conditions laid out by the US government. On the contrary, these, and dozens of other agreements which have come to light, are emblematic of decades-long US corporate-state "public-private partnerships."

As *Bloomberg* reported last month, "thousands of technology, finance and manufacturing companies are working closely with US national security agencies, providing sensitive information and in return receiving benefits that include access to classified intelligence."

It's a two-way street, Bloomberg noted. Firms providing "US intelligence organizations with additional data, such as equipment specifications" use it "to help infiltrate computers of its

adversaries." In return, "companies are given quick warnings about threats that could affect their bottom line." Such sensitive data can also be used to undermine the position of their foreign competitors.

We now know, based on documents provided by Snowden, that the "infiltration" of computer networks by US secret state agencies are useful not only for filching military secrets and mass spying but also for economic and industrial espionage.

That point was driven home more than a decade ago in a paperprepared by journalist Duncan Campbell for the European Parliament.

"By the end of the 1990s," Campbell wrote, "the US administration claimed that intelligence activity against foreign companies had gained the US nearly $150 billion in exports."

"Although US intelligence officials and spokespeople have admitted using Comint [communications intelligence] against European companies . . . documents show that the CIA has been directly involved in obtaining competitor intelligence for business purposes."

At the time the Telstra pact was signed, the Australian telecommunications and internet giant was "50.1% owned" by the Australian government. Reach Global Services, is described in the document as "a joint venture indirectly owned 50% by Telstra" and "50% owned" by Hong Kong's Pacific Century CyberWorks Limited (PCCW).

With controlling interest in more than 40 undersea fiber optic cables, and with landing rights in global markets that include Hong Kong, Japan, Korea, Taiwan, Singapore, Australia, North America and Europe, the joint venture was then the largest commercial telecommunications carrier in Asia with some 82,000 kilometers of undersea cables. Reach also operates international satellite systems that cover two-third's of the planet's surface.

Such assets would be prime targets of "Five Eyes" spy agencies under terms of the UKUSA Communications Intelligence Agreement.

Telstra and PCCW restructured their partnership in 2011, with the Australian firm now controlling the lion's share of an undersea cable network that stretches "more than 364,000 kilometres and connects more than 240 markets worldwide," the*South Morning China Post* reported. Inevitably, the restructuring will afford the US government an even greater opportunity for spying.

Network security agreements hammered out among undersea cable firms and the US government have profound implications for global commerce. Their geopolitical significance hasn't been lost on America's closet "allies."

The Guardian revealed last month that the US is "spying on the European Union mission in New York and its embassy in Washington." In addition to the EU mission, target lists include "the French, Italian and Greek embassies, as well as a number of other American allies, including Japan, Mexico, South Korea, India and Turkey."

That list has since been supplemented by further disclosures.

Snowden told the *South China Morning Post* that NSA hacked into the "computers at the Hong Kong headquarters of Pacnet, which owns one of the most extensive fibre optic

submarine cable networks in the region."

Recently, the firm signed major deals with the Chinese mainland's "top mobile phone companies" and "owns more than 46,000 kilometres of fibre-optic cables."

According to the paper, Pacnet "cables connect its regional data centres across the Asia-Pacific region, including Hong Kong, the mainland, Japan, South Korea, Singapore and Taiwan. It also has offices in the US."

The *South Morning China Post* also disclosed that Tsinghua University, "China's premier seat of learning" has sustained extensive attacks on the school's "network backbones."

Available documents based on Snowden disclosures and other sources seem to suggest that President Obama's militaristic "pivot to Asia" is also an aggressive campaign to steal commercial and trade secrets from US imperialism's Asian rivals.

Whether or not these revelations will effect negotiations over the proposed Trans-Pacific Partnership (TPP), a NAFTA-style "free trade" agreement between the US and ten Pacific Rim nations, including Chile, Japan, Malaysia, Mexico, Peru and Singapore–all prime US-UK targets of PRISM, TEMPORA and X-Keyscore–remains to be seen.

'Legal' License to Spy

If we have learned anything since Snowden's revelations began surfacing last month, it is that the US secret state relies on a body of "secret laws" overseen by a Star Chamber-like FISA court described in the polite language *The New York Times* as a "parallel Supreme Court," to do its dirty work.

Along with leaked NSA documents, published agreements between telecommunications firms, internet service providers and the US government should demolish the fiction that blanket surveillance is "legal," "limited in scope" or chiefly concerned with fighting "crime" and "terrorism."

Proclaiming that "US communications systems are essential to the ability of the US government to fulfill its responsibilities to the public to preserve the national security of the United States, to enforce the laws, and to maintain the safety of the public," the Telstra summary posted by *Crikey* should dispel any illusions on that score.

On the contrary, the agreement reveals the existence of a vast surveillance web linking private companies to the government's relentless drive, as *The Washington Post* explained, to "collect it all."

> ● All customer billing data to be stored for two years;
> ● Ability to provide to agencies any stored telecommunications or internet communications and comply with preservation requests;
> ● Ability to provide any stored metadata, billing data or subscriber information about US customers;
> ● They are not to comply with any foreign privacy laws that might lead to mandatory destruction of stored data;
> ● Plans and infrastructure to demonstrate other states cannot spy on US customers;
> ● They are not to comply with information requests from other countries without DoJ permission;

● A requirement to:

> . . . designate points of contact within the United States with the authority and responsibility for accepting and overseeing the carrying out of Lawful US Process to conduct Electronic Surveillance of or relating to Domestic Communications carried by or through Domestic Communications Infrastructure; or relating to customers or subscribers of Domestic Communications Companies. The points of contact shall be assigned to Domestic Communications Companies security office(s) in the United States, shall be available twenty-four (24) hours per day, seven (7) days per week and shall be responsible for accepting service and maintaining the security of Classified Information and any Lawful US Process for Electronic Surveillance . . . The Points of contact shall be resident US citizens who are eligible for US security clearances.

In other words, an "internal corporate cell of American citizens," charged with providing confidential customer data to the secret state, as *The Washington Post* first reported.

Additional demands include:

● A requirement to keep such surveillance confidential, and to use US citizens "who meet high standards of trustworthiness for maintaining the confidentiality of Sensitive Information" to handle requests;
● A right for the FBI and the DoJ to conduct inspection visits of the companies' infrastructure and offices; and
● An annual compliance report, to be protected from Freedom of Information requests.

This is not a one-off as the other 27 Agreements published by Public Intelligence readily attest.

For example, the 31-page 2011 Agreement between the US government and Level 3 Communications, which operates in North America, Europe, Latin America and the Asia-Pacific, which acquired Global Crossing from from the Hong Kong-based Hutchison Whampoa and Singapore Technologies Telemedia (the focus of *The Washington Post's* July 6 report), was expanded beyond the FBI and Department of Justice to include the Department of Homeland Security and the Department of Defense, NSA's "parent" agency.

As with the 2001 Telstra agreement, "Access" to Level 3's systems by governmental entities is defined as "the ability to physically or logically undertake any of the following actions: (a) read, divert, or otherwise obtain non-public information or technology from or about software, hardware, a system or a network; (b) add, edit or alter information or technology stored on or by software, hardware, a system or a network; and (c) alter the physical or logical state of software, hardware, a system or a network (e.g., turning it on or off, changing configuration, removing or adding components or connections)."

NSA, the principle US spy agency charged with obtaining, storing and analyzing COMINT/SIGINT "products, i.e., user data, has been handed virtually unlimited access to information flowing through Level 3 fiber optic cables as it enters the US.

This includes what is described as "Domestic Communications," content, not simply the metadata, of any phone call or email that transit Level 3 systems: "'Domestic Communications' means: (a) Wire Communications or Electronic Communications (whether

stored or not) from one US location to another US location; and (b) the US portion of a Wire Communication or Electronic Communication (whether stored or not) that originates or terminates in the United States."

So much for President Obama's mendacious claim that "nobody is listening to your phone calls"!

Access to the entirety of customer records and communications is clearly spelled out in the section entitled "Electronic Surveillance."

Note: the "USC." provisions refer to (18) the Stored Communications Act which compels disclosure to the government of stored wire, electronic and transactional data; a provision that greatly weakened the Fourth Amendment right to privacy. 50 USC outlines the role of War and National Defense in the United States Code and includes "foreign intelligence," "electronic surveillance authorization without court order," "internal security," including the "control of subversive activities" and the "exercise of emergency powers and authorities" by the Executive Branch.

> 'Electronic Surveillance,' for the purposes of this Agreement, includes: (a) the interception of wire, oral, or electronic communications as defined in 18 U.S.C. §§ 2510(1), (2), (4) and (12), respectively, and electronic surveillance as defined in 50 U.S.C. § 1801(f); (b) Access to stored wire or electronic communications, as referred to in 18 U.S.C. § 2701 et seq.; (c) acquisition of dialing, routing, addressing, or signaling information through pen register or trap and trace devices or other devices or features capable of acquiring such information pursuant to law as defined in 18 U.S.C. § 3121 et seq. and 50 U.S.C. § 1841 et seq.; (d) acquisition of location-related information concerning a service subscriber or facility; (e) preservation of any of the above information pursuant to 18 U.S.C.§ 2703(f); and (f) Access to, or acquisition, interception, or preservation of, wire, oral, or electronic communications or information as described in (a) through (e) above and comparable state laws.

Level 3 is further enjoined from disclosing what is described as "Sensitive Information," that is, "information that is not Classified Information regarding: (a) the persons or facilities that are the subjects of Lawful US Process; (b) the identity of the Government Authority or Government Authorities serving such Lawful US Process; (c) the location or identity of the line, circuit, transmission path, or other facilities or equipment used to conduct Electronic Surveillance; (d) the means of carrying out Electronic Surveillance."

In other words, *we* do the spying; *you* hand over it over and keep your mouths shut.

The electronic driftnet thrown over global communications is expedited by *direct access* to Level 3's equipment by the US government.

> 'Principal Equipment' means the primary electronic components of a submarine cable system, to include the hardware used at the NOC(s) [Network Operations Center], landing station(s) and the cable itself, such as servers, repeaters, submarine line terminal equipment (SLTE), system supervisory equipment (SSE), power feed equipment (PFE), tilt and shape equalizer units (TEQ/SEQ), optical distribution frames (ODF), and synchronous optical network (SONET), synchronous digital hierarchy (SDH), wave division multiplexing (WDM), dense wave division multiplexing (DWDM), coarse wave division multiplexing (CWDM) or optical carrier network (OCx) equipment, as

applicable.

Who oversees the set-up? On paper it appears that Level 3 control their operations. However, the Agreement specifies that the firm must utilize “primary US NOCs for any Domestic Communications Infrastructure” and it “shall be maintained and remain within the United States and US territories, to be operated by Level 3, exclusively using Screened Personnel.”

Who signs off on “screened personnel”? Why the US government of course, which raises the suspicion that corporate employees are little more than spook assets.

But here’s where it gets interesting. “Level 3 may nonetheless use the United Kingdom NOC for routine day-to-day management of any of the Cable Systems as such management is in existence as of the Effective Date.”

Why might that be the case, pray tell?

Could it be that fiber optic cables transiting the UK are *already*lovingly scrutinized by NSA’s kissin’ cousins across the pond? GCHQ, as *The Guardian* disclosed, is merrily ingesting “vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them” with the American agency.

Therefore, since UK undersea cable traffic is already under close “management” via the British agency’s TEMPORA program, described as having the “‘biggest internet access’ of any member of the Five Eyes electronic eavesdropping alliance,” it makes sense that Level 3 is allowed to “use the United Kingdom NOC” as a hub for its “Domestic Communications Infrastructure”!

In conclusion, these publicly available documents provide additional confirmation of how major corporations are empowering the US surveillance octopus.

By entering into devil’s pacts with the world’s “sole superpower,” giant telcos and internet firms view the destruction of privacy rights as just another item on the balance sheet, a necessary cost of doing business in America.

And business is *very* good.

Articles by: **Tom Burghardt**
http://antifascist-calling.blogspot.com/