The New York Times | http://nyti.ms/1dwTMjh

U.S.

Spying by N.S.A. Ally Entangled U.S. Law Firm

By JAMES RISEN and LAURA POITRAS FEB. 15, 2014

The list of those caught up in the global surveillance net cast by the National Security Agency and its overseas partners, from social media users to foreign heads of state, now includes another entry: American lawyers.

A top-secret document, obtained by the former N.S.A. contractor Edward J. Snowden, shows that an American law firm was monitored while representing a foreign government in trade disputes with the United States. The disclosure offers a rare glimpse of a specific instance in which Americans were ensnared by the eavesdroppers, and is of particular interest because lawyers in the United States with clients overseas have expressed growing concern that their confidential communications could be compromised by such surveillance.

The government of Indonesia had retained the law firm for help in trade talks, according to the February 2013 document. It reports that the N.S.A.'s Australian counterpart, the Australian Signals Directorate, notified the agency that it was conducting surveillance of the talks, including communications between Indonesian officials and the American law firm, and offered to share the information.

The Australians told officials at an N.S.A. liaison office in Canberra, Australia, that "information covered by attorney-client privilege may be included" in the intelligence gathering, according to the document, a monthly bulletin from the Canberra office. The law firm was not identified, but Mayer Brown, a Chicago-based firm with a global practice, was then advising the Indonesian government on trade issues.

On behalf of the Australians, the liaison officials asked the N.S.A. general counsel's office for guidance about the spying. The bulletin notes only that the counsel's office "provided clear guidance" and that the Australian agency "has been able to continue to cover the talks, providing highly useful intelligence for interested US customers."

The N.S.A. declined to answer questions about the reported surveillance, including whether information involving the American law firm was shared with United States trade officials or negotiators.

Duane Layton, a Mayer Brown lawyer involved in the trade talks, said he did not have any evidence that he or his firm had been under scrutiny by Australian or American intelligence agencies. "I always wonder if someone is listening, because you would have to be an idiot not to wonder in this day and age," he said in an interview. "But I've never really thought I was being spied on."

A Rising Concern for Lawyers

Most attorney-client conversations do not get special protections under American law from N.S.A. eavesdropping. Amid growing concerns about surveillance and hacking, the American Bar Association in 2012 revised its ethics rules to explicitly require lawyers to "make reasonable efforts" to protect confidential information from unauthorized disclosure to outsiders.

Last year, the Supreme Court, in a 5-to-4 decision, rebuffed a legal challenge to a 2008 law allowing warrantless wiretapping that was brought in part by lawyers with foreign clients they believed were likely targets of N.S.A. monitoring. The lawyers contended that the law raised risks that required them to take costly measures, like traveling overseas to meet clients, to protect sensitive communications. But the Supreme Court dismissed their fears as "speculative."

The N.S.A. is prohibited from targeting Americans, including businesses, law firms and other organizations based in the United States, for surveillance without warrants, and intelligence officials have repeatedly said the N.S.A. does not use the spy services of its partners in the so-called Five Eyes alliance — Australia, Britain, Canada and New Zealand — to skirt the law.

Still, the N.S.A. can intercept the communications of Americans if they are in contact with a foreign intelligence target abroad, such as Indonesian officials. The

N.S.A. is then required to follow so-called minimization rules to protect their privacy, such as deleting the identity of Americans or information that is not deemed necessary to understand or assess the foreign intelligence, before sharing it with other agencies.

An N.S.A. spokeswoman said the agency's Office of the General Counsel was consulted when issues of potential attorney-client privilege arose and could recommend steps to protect such information.

"Such steps could include requesting that collection or reporting by a foreign partner be limited, that intelligence reports be written so as to limit the inclusion of privileged material and to exclude U.S. identities, and that dissemination of such reports be limited and subject to appropriate warnings or restrictions on their use," said Vanee M. Vines, the spokeswoman.

The Australian government declined to comment about the surveillance. In a statement, the Australian Defense Force public affairs office said that in gathering information to support Australia's national interests, its intelligence agencies adhered strictly to their legal obligations, including when they engaged with foreign counterparts.Several newly disclosed documents provide details of the cooperation between the United States and Australia, which share facilities and highly sensitive intelligence, including efforts to break encryption and collect phone call data in Indonesia. Both nations have trade and security interests in Indonesia, where Islamic terrorist groups that threaten the West have bases.

The 2013 N.S.A. bulletin did not identify which trade case was being monitored by Australian intelligence, but Indonesia has been embroiled in several disputes with the United States in recent years. One involves clove cigarettes, an Indonesian export. The Indonesian government has protested to the World Trade Organization a United States ban on their sale, arguing that similar menthol cigarettes have not been subject to the same restrictions under American antismoking laws. The trade organization, ruling that the United States prohibition violated international trade laws, referred the case to arbitration to determine potential remedies for Indonesia.

Another dispute involved Indonesia's exports of shrimp, which the United States claimed were being sold at below-market prices.

The Indonesian government retained Mayer Brown to help in the cases concerning cigarettes and shrimp, said Ni Made Ayu Marthini, attaché for trade and industry at the Indonesian Embassy in Washington. She said no American law firm had been formally retained yet to help in a third case, involving horticultural and animal products.

Mr. Layton, a lawyer in the Washington office of Mayer Brown, said that since 2010 he had led a team from the firm in the clove cigarette dispute. He said Matthew McConkey, another lawyer in the firm's Washington office, had taken the lead on the shrimp issue until the United States dropped its claims in August. Both cases were underway a year ago when the Australians reported that their surveillance included an American law firm.

Mr. Layton said that if his emails and calls with Indonesian officials had been monitored, the spies would have been bored. "None of this stuff is very sexy," he said. "It's just run of the mill."

He and the other Mayer Brown lawyers do most of their work on the trade issues from Washington, he said. They also make occasional trips to Jakarta, Indonesia's capital, and Geneva, where the World Trade Organization is based. Mr. Layton said most of his communications with officials in Jakarta had been done through email, while he also talked by phone with officials at the Indonesian Embassy in Washington.

The N.S.A.'s protections for attorney-client conversations are narrowly crafted, said Stephen Gillers, an expert on legal ethics at New York University's School of Law. The agency is barred from sharing with prosecutors intercepted attorney-client communications involving someone under indictment in the United States, according to previously disclosed N.S.A. rules. But the agency may still use or share the information for intelligence purposes.

Andrew M. Perlman, a Suffolk University law professor who specializes in legal ethics and technology issues, said the growth of surveillance was troubling for lawyers. He helped create the bar association's ethics code revisions that require lawyers to try to avoid being overheard by eavesdroppers.

"You run out of options very quickly to communicate with someone overseas," he said. "Given the difficulty of finding anything that is 100 percent

secure, lawyers are in a difficult spot to ensure that all of the information remains in confidence."

In addition to its work on trade issues with the United States, Mr. Layton said, Mayer Brown was representing Indonesia in a dispute with Australia. He said Indonesia had been arguing that Australia's requirements for plain packaging for tobacco products under its antismoking rules were excessive.

Economic Espionage

Even though the Indonesian issues were relatively modest for the United States — about $40 million in annual trade is related to the clove cigarette dispute and $1 billion annually to shrimp — the Australian surveillance of talks underscores the extent to which the N.S.A. and its close partners engage in economic espionage.

In justifying the agency's sweeping powers, the Obama administration often emphasizes the N.S.A.'s role in fighting terrorism and cyberattacks, but disclosures in recent months from the documents leaked by Mr. Snowden show the agency routinely spies on trade negotiations, communications of economic officials in other countries and even foreign corporations.

American intelligence officials do not deny that they collect economic information from overseas, but argue that they do not engage in industrial espionage by sharing that information with American businesses. China, for example, is often accused of stealing business secrets from Western corporations and passing them to Chinese corporations.

The N.S.A. trade document — headlined "SUSLOC (Special US Liaison Office Canberra) Facilitates Sensitive DSD Reporting on Trade Talks"— does not say which "interested US customers" besides the N.S.A. might have received intelligence on the trade dispute.

Other documents obtained from Mr. Snowden reveal that the N.S.A. shares reports from its surveillance widely among civilian agencies. A 2004 N.S.A. document, for example, describes how the agency's intelligence gathering was critical to the Agriculture Department in international trade negotiations.

"The U.S.D.A. is involved in trade operations to protect and secure a large segment of the U.S. economy," that document states. Top agency officials "often

rely on SIGINT" — short for the signals intelligence that the N.S.A. eavesdropping collects — "to support their negotiations."

The Australians reported another instance to the N.S.A. — in addition to the one with the American law firm — in which their spying involved an American, according to the February 2013 document. They were conducting surveillance on a target who turned out to be an American working for the United States government in Afghanistan, the document said. It offered no details about what happened after the N.S.A. learned of the incident, and the agency declined to respond to questions about it.

In a statement, Ms. Vines, the agency spokeswoman, said: "N.S.A. works with a number of partners in meeting its foreign-intelligence mission goals, and those operations comply with U.S. law and with the applicable laws under which those partners operate. A key part of the protections that apply to both U.S. persons and citizens of other countries is the mandate that information be in support of a valid foreign-intelligence requirement, and comply with U.S. attorney general-approved procedures to protect privacy rights."

The documents show that the N.S.A. and the Australians jointly run a large signals intelligence facility in Alice Springs, Australia, with half the personnel from the American agency. The N.S.A. and its Australian counterpart have also cooperated on efforts to defeat encryption. A 2003 memo describes how N.S.A. personnel sought to "mentor" the Australians while they tried to break the encryption used by the armed forces of nearby Papua New Guinea.

Most of the collaboration between the N.S.A. and the Australian eavesdropping service is focused on Asia, with China and Indonesia receiving special attention.

Australian intelligence has focused heavily on Indonesia since the Bali bombing of 2002. The attack, which killed 202 people, including 88 Australians, in a resort area popular with Australians, was blamed on the Southeast Asian Islamist group Jemaah Islamiyah.

The Americans and the Australians secretly share broad access to the Indonesian telecommunications system, the documents show. The N.S.A. has given the Australians access to bulk call data from Indosat, an Indonesian

telecommunications provider, according to a 2012 agency document. That includes data on Indonesian government officials in various ministries, the document states.

The Australians have obtained nearly 1.8 million encrypted master keys, which are used to protect private communications, from the Telkomsel mobile telephone network in Indonesia, and developed a way to decrypt almost all of them, according to a 2013 N.S.A. document.

James Risen reported from Washington, and Laura Poitras from Berlin. Charlie Savage contributed reporting from Washington.

A version of this article appears in print on February 16, 2014, on page A1 of the New York edition with the headline: Spying by N.S.A. Ally Entangled U.S. Law Firm .
